



11-2002

4th Annual Computer & Technology Law Institute

Office of Continuing Legal Education at the University of Kentucky College of Law

Right click to open a feedback form in a new tab to let us know how this document benefits you.

Follow this and additional works at: https://uknowledge.uky.edu/uky_cle

 Part of the [Computer Law Commons](#), [Contracts Commons](#), [Criminal Law Commons](#), [Intellectual Property Law Commons](#), and the [Privacy Law Commons](#)

Repository Citation

Office of Continuing Legal Education at the University of Kentucky College of Law, "4th Annual Computer & Technology Law Institute" (2002). *Continuing Legal Education Materials*. 70.
https://uknowledge.uky.edu/uky_cle/70

This Book is brought to you for free and open access by the Kentucky Legal History at UKnowledge. It has been accepted for inclusion in Continuing Legal Education Materials by an authorized administrator of UKnowledge. For more information, please contact UKnowledge@sv.uky.edu.

UK
CLE

4th Annual

**Computer &
Technology Law
Institute**

November 2002



UK
CLE

4th Annual

**Computer &
Technology Law
Institute**

November 2002

**Presented by the
OFFICE OF CONTINUING LEGAL EDUCATION
UNIVERSITY OF KENTUCKY COLLEGE OF LAW**

FROM THE LAW LIBRARY OF: _____

Written materials and oral presentations offered through the University of Kentucky College of Law Office of Continuing Legal Education (UK/CLE) are designed to assist lawyers in maintaining their professional competence. The Office of Continuing Legal Education and its volunteer speakers and writers are not rendering legal or other professional services by their participation in continuing legal education activities. Attorneys and others using information obtained from UK/CLE publications or seminars must also fully research original and current sources of authority to properly serve their or their client's legal interests. The forms and sample documents contained in our continuing legal education publications are intended for use only in conjunction with the professional services and advice of licensed attorneys. All parties must cautiously consider whether a particular form or document is suited to specific needs. The legal research presented herein is believed to be accurate, but is not warranted to be so. These written materials and the comments of speakers in presentation of these materials may contain expressions of opinion which do not necessarily reflect the views of the Office of Continuing Legal Education, the University of Kentucky, the Commonwealth of Kentucky, or other governmental authorities. UK/CLE strives to make its written materials and speaker presentations gender-neutral; however, gender-specific references may remain where it would otherwise be awkward or unclear. It should be understood that in such references the female includes the male, and vice-versa.

Copyright 2002 by the University of Kentucky College of Law,
Office of Continuing Legal Education.
All rights reserved.

Printed in the United States of America

UK/CLE: A Self-Supporting Entity

The University of Kentucky Office of Continuing Legal Education (UK/CLE) is an income-based office of the University of Kentucky College of Law. As such, it is separately budgeted and financially self-supporting. UK/CLE operations are similar to not-for-profit organizations, paying all direct expenses, salaries and overhead solely from revenues.

No public funds or tax dollars are allocated to its budget. Revenues are obtained from registrant enrollment fees, and the sale of publications. Our sole function is to provide professional development services. In the event surplus funds become available, they are utilized to offset deficits or retained in our budget to improve the quality and variety of services we provide.

UNIVERSITY OF KENTUCKY
COLLEGE OF LAW

OFFICE OF CONTINUING LEGAL EDUCATION

Suite 260 Law Building
Lexington, Kentucky 40506-0048

Phone
(859) 257-2921

Facsimile
(859) 323-9790

Web Address
www.uky.edu/Law/CLE

PRESIDENT, UNIVERSITY OF KENTUCKY

Lee T. Todd, Jr.

DEAN, COLLEGE OF LAW

Allan W. Vestal

DIRECTOR OF CLE

Kevin P. Bucknam

ASSISTANT DIRECTOR OF CLE

David L. Kinsella

ADMINISTRATIVE/BUSINESS MANAGER

Melinda E. Rawlings

EDITORIAL/MARKETING ASSISTANT

William G. Nims

RESEARCH ASSOCIATES/REGISTRARS

Dennis Flynn
Joe MacLaren
Heather Fryman
Brian Powers

ABOUT...

UK CLE

The University of Kentucky College of Law, Office of Continuing Legal Education (UK/CLE) was organized in 1973 as the first permanently staffed, full-time continuing legal education program in the Commonwealth of Kentucky. It endures with the threefold purpose to: 1) assist lawyers in keeping abreast of changes in the law; 2) develop and sustain practical lawyering skills; and 3) maintain a high degree of professionalism in the practice of law. Revenues from seminar registrations and publication sales allow the Office to operate as a separately budgeted, self-supporting program of the College. No tax dollars, bar dues or public funds are budgeted in the Office's finances.

Courses

UK/CLE provides a variety of workshops, conferences, and institutes to satisfy the continuing education needs of lawyers and other professionals. Courses range from half-day programs in selected areas to in-depth programs extending over several days. While most courses are conducted at the College of Law in Lexington, UK/CLE has a longstanding statewide commitment. Since its first year of operation, beginning with a criminal law program in Madisonville, Kentucky, the Office has continued to bring the highest quality continuing education to attorneys across Kentucky, the Midsouth, the Midwest, and the nation.

Publications

Each course is accompanied by extensive speaker-prepared course materials. These bound materials are offered for sale following courses and are consistently regarded as valuable, affordable references for lawyers. In 1987, UK/CLE began producing a series of publications which now consist of Practice Handbooks, Monographs, and Compendiums. Each Practice Handbook is an extensively referenced, fully indexed practice guide consisting of separately authored chapters, sequenced for the comprehensive coverage of a distinct body of law. Their format allows for updating through supplements and cumulative indexes. Each Monograph is a concisely written practice guide, usually prepared by a single author, designed to cover a topic of narrower scope than Practice Handbooks. Compendiums contain both official forms and sample documents. Designed to assist the lawyer by suggesting specific structures and language to consider in drafting documents, these publications are beneficial in the resolution of legal drafting concerns. The Compendiums are often used most effectively in conjunction with UK/CLE Practice Handbooks and Monographs.

Professional Management

UK/CLE serves the needs of the bar from its offices on the University of Kentucky campus in Lexington. Its staff manages course planning, publication content planning, course registrations, publications sales, course and publication marketing, publication composition and printing, as well as internal budgeting, accounting, and financial reporting. As an "income based" program, UK/CLE's course tuitions and publications sales are designed to generate sufficient revenues for self-support.

Commitment to Quality and Creativity

UK/CLE is a member of the Association for Continuing Legal Education (ACLEA). As such, UK/CLE subscribes to the Standards of Operation for Continuing Legal Education Organizations, and the Standards of Fair Conduct and Voluntary Cooperation administered under the auspices of the American Law Institute-American Bar Association Committee on Continuing Professional Education. Throughout its existence UK/CLE has been actively involved in the activities of and discourse sponsored by ACLEA. UK/CLE's association with national and international CLE professionals has afforded it the opportunity to continually reassess instructional methods, quality in publications, and effective means of delivering CLE services at consistently high levels of quality.

An Integral Part of the Legal Profession's Tradition of Service

An enormous debt is owed to the practitioners, professors, judges and other professionals who generously donate their time and talent to continuing legal education. Their knowledge and experience provide the fundamental components of our seminars and publications. Without their motivation and freely given assistance in dedication to the legal profession, high quality continuing legal education would not exist. As a non-profit organization, UK/CLE relies upon the traditional spirit of service to the profession that attorneys have so long demonstrated. We are constantly striving to increase attorney involvement in the continuing legal education process. If you would like to participate as a volunteer speaker or writer, please contact us and indicate your areas of interest and experience.



-4th Annual -
COMPUTER & TECHNOLOGY LAW INSTITUTE

TABLE OF CONTENTS

DOCUMENTS, DATABASES, DISCOVERY & THE DAMNED SECTION A
Andy Johnson-Laird
Barbara A. Frederiksen

SOFTWARE LICENSES: From Mass Market End User License Agreements
to Mission Critical Development and Installation Agreements SECTION B
William L. Montague, Jr.

PATENT UPDATE: The Patentability of a Business Method, the Survival
and Future of Internet Patents and Other Important Topics SECTION C
Andrew D. Dorisio
Michael S. Hargis

PROTECTING AGAINST AND PROSECUTING CYBERCRIME
(INCLUDING CYBERTERRORISM) SECTION D
Marisa J. Ford
Kenneth J. Tuggle

FINANCING ISSUES & INTELLECTUAL PROPERTY DEVELOPMENT:
The intersection Between Credit and Property Rights SECTION E
Raymond T. Nimmer

THE STATE OF PRIVACY SECTION F
Cynthia L. Stewart

LAW, ETHICS & PUBLIC OPINION REGARDING COMMERCIALIZATION
OF BIOTECHNOLOGY: Pharmacogenomics as an Example SECTION G
Mark A. Rothstein

ETHICS: Taking an Equity Interest in Your Start-Up Client & What
Can Attorneys Do When the Client Fails SECTION H
Grace M. Giesel

DOTGONE - THE DEATH OF DOTCOMS: Why Did it Happen?
Who has Survived? The Next Wave? Bankruptcy Considerations SECTION I
Charles R. Keeton

**GOING GLOBAL: Issues to Consider When Conducting Business
Worldwide Through Cyberspace** SECTION J
Gregory R. Mues

**CYBERLANGUAGE: A Field Guide to the Law of Spiders, Bots,
Netcrawlers and other Cyber Critters** SECTION K
Kurt X. Metzmeier

UPDATE ON DOMAIN NAME DISPUTES AND NEW TLDS SECTION L
Joseph R. Dreitler

**DOCUMENTS, DATABASES, DISCOVERY
AND THE DAMNED**

*Andy Johnson-Laird
and
Barbara A. Frederiksen
Johnson-Laird Inc.
Portland, Oregon*

Copyright 2002, Johnson-Laird Inc.

SECTION A

Computer-Based Evidence: Cutting The Cost Of Discovery

Documents, Databases, Discovery
and
The Damned

Andy Johnson-Laird
Barbara A. Frederiksen
Forensic Software Analysts

Johnson-Laird Inc.
850 Northwest Summit Avenue
Portland, Oregon 97210
Tel: (503) 274-0784 : FAX: (503) 274-0512
andy@jli.com
barb@jli.com
<http://www.jli.com/>

"Technological progress is like an axe in the hands of a pathological criminal." Albert Einstein.

Andy Johnson-Laird: Mr. Johnson-Laird is a forensic software analyst and president of Johnson-Laird Inc., a consulting company specializing in Cyber-Forensics™ (the forensic analysis of computer software and computer-based evidence in the context of copyright and patent infringement, and trade secret misappropriation) and Techno-Archeology™ (the study of disputed software development projects). Mr. Johnson-Laird has 39 years' experience in the computer industry covering computer operations, programming, managing programmers, systems design, systems analysis, and developing software in a "clean room" environment.

Barbara A. Frederiksen: Ms. Frederiksen is a forensic software analyst and the senior managing consultant with Johnson-Laird Inc. of Portland, Oregon. Ms. Frederiksen has 27 years' experience in the computer industry covering software development, systems design, performance engineering, systems analysis, database design, and system administration.

Copyright (C) 2002: Johnson-Laird Inc.
JLI is a Registered Trademark of Johnson-Laird Inc.

COMPUTER-BASED EVIDENCE : CUTTING THE COST OF DISCOVERY
Andy Johnson-Laird and Barbara A. Frederiksen

| | |
|---|-----------|
| INTRODUCTION | 1 |
| DOCUMENTS AND DATABASES..... | 1 |
| WHAT IS DATA?..... | 1 |
| <i>The Difference Between Data and Information</i> | 2 |
| Encoded Information | 4 |
| File Formats | 9 |
| The Need For Common File Formats | 10 |
| DATABASES | 11 |
| The Anatomy Of Databases | 12 |
| DISCOVERY | 17 |
| EVIDENCE PRESERVATION | 17 |
| THE CHALLENGE OF DISCOVERY..... | 18 |
| WHAT DO YOU ASK FOR? | 18 |
| THE DISCOVERY OF META-DATA..... | 20 |
| WE REQUESTED INFORMATION, THE OTHER PARTY PRODUCED DATA!..... | 21 |
| INVENTORY ISSUES | 21 |
| ANCIENT (AND MODERN) GEEK ARCHEOLOGY | 23 |
| PRINTED EVIDENCE IS OFTEN THE MOST MAXIMALLY INCONVENIENT FORM | 24 |
| PRODUCTION COMPLETENESS, QUALITY, AND SCOPE..... | 24 |
| BEYOND BATES - IDENTIFICATION, VALIDATION, AND AUTHENTICATION..... | 26 |
| BATES NUMBER FILES AT YOUR PERIL..... | 27 |
| PRODUCTION PITFALLS | 28 |
| <i>The Trouble With TIFFs</i> | 28 |
| <i>Database Production Issues</i> | 29 |
| <i>Computer Programs</i> | 31 |
| <i>E-mail or E-mangle?</i> | 31 |
| THE DAMNED..... | 31 |
| SO MUCH EVIDENCE, SO LITTLE TIME..... | 32 |
| SAVING THE BEST UNTIL LAST..... | 32 |
| SHOT IN THE FOOT BY YOUR OWN SMOKING GUN | 33 |
| DE-DUPING OR DUPING?..... | 33 |
| CONCLUSION | 34 |
| APPENDIX A : SAMPLE PRODUCTION PROTOCOL AND DISCOVERY LANGUAGE | 35 |

DOCUMENTS, DATABASES, DISCOVERY AND THE DAMNED
Andy Johnson-Laird and Barbara A. Frederiksen

| | |
|------------------------------------|----|
| DEFINITION..... | 35 |
| PRODUCTION PROTOCOL..... | 35 |
| ELECTRONIC DOCUMENTS REQUEST | 38 |

Discovery: The process whereby a requesting party asks for information and the producing party provides only data, thereby increasing the cost of litigation by an order of magnitude.

Introduction

Computer-based evidence is not new to the Law, but its ubiquity and quantity are forcing the Law to contemplate some new challenges. Just about every legal dispute involves data that was created on a computer – even if the final documents appear on dead trees¹. The sheer volume of data produced by litigants is forcing many an attorney to request an extension just to allow it to be reviewed before production and analyzed after receipt.

There are many issues that the Courts still have not resolved when it comes to computer-based evidence – not the least of which being just what *is* a requesting party entitled to, in what form, and what additional explanatory information must be provided?

Documents And Databases

What Is Data?

A computer knows nothing of documents and databases. A computer makes no distinction between the two. It is merely a machine doing precisely what it was told to do by computer programmers who have written a computer program² to process information.

A computer can only store data in the form of 0's and 1's. Everything else, be it a letter, a FAX, an audio recording, a photograph, a video, or a giant corporate database, is an illusion. The illusion requires a conspiracy between the computer hardware (the electronics) and the software (the computer programs). When working properly, the illusion is complete – you think the computer is storing this information in an appropriate form and can redisplay or replay it on demand. However, the savvy counsel never lets go of the idea that it really is an illusion.

¹ The intentionally derogatory terms used by computer geeks for documents created by melting carbon powder onto a matrix of wood chips.

² Thus giving rise to the computer science definition of a computer program as “information about how to process information.”

Those who do let go of that idea run the risk of not requesting information to which they might be entitled, or to produce irrelevant or privileged information.

To many people data and information are essentially synonymous. This is flat wrong. Failure to make this distinction is responsible for many of the discovery and production woes of litigants and their counsel.

Data and information have close-but-no-cigar definitions:

“data (1) A re-interpretable representation of information in a formalized manner suitable for communication, interpretation, or processing.”

“information (1) In information processing, knowledge concerning such things as facts, concepts, object, events, ideas and processes, that with a certain context has a particular meaning.”

IBM Dictionary of Computing, Tenth Edition (1993) (emphasis added).

The subtlety of these definitions bears some consideration: Data is a re-interpretable representation of information. Information is data that has meaning in context. To rephrase this in a more approachable form: Data is what is stored on the computer – information is what you make of it.

The Difference Between Data and Information

Consider this piece of data: 1,000,223,101.

It has no apparent meaning to us yet it represents a number that millions of people will remember until their deaths. To understand the meaning (more properly called the semantics) of this data, one needs only to know what this data is, how it is encoded, and how to interpret it appropriately.

It is the number of seconds that have elapsed since midnight on January 1st, 1970. Using a calculator (or a calendric idiot savant if you have one) this number can be converted into a date: September 11, 2001, 8:46 am³.

³ Technically this time is in UTC (sic), Universal Coordinated Time, not Eastern Standard Time, but the point is made, nevertheless. For those whose cognitive skills have only come on-line since this date, this is the time when the first hijacked aircraft, American Airlines flight 11 from Boston, impacted with the north tower of the World Trade Center. Computers using the UNIX operating system calculate dates as the number of seconds since January 1st, 1970.

Every man, woman and child in North America who is sane and of suitable age, will remember this date, yet were they to be presented with this “raw” data, they would have found it to be completely incomprehensible and devoid of meaning.

That is the difference between data and information. The problem in litigation can be expressed succinctly: What is requested is information. What is produced in response is data. Unless the data produced is accompanied with sufficient additional *information* to allow humans to direct computers to convert the data produced back into information, the data produced and received remains only data and is worth the paper that it is not printed on.

The difference between data and information may seem academic, but it is this difference that, if overlooked, will likely increase the cost of discovery significantly. It is not unusual for the costs of converting data into information during discovery to be one of the most significant costs.

It is not just semantics that we as humans need to fully understand data. For example, the date 9/11/2001 has little meaning to those who live to the East of the U.S.A. Over “there” dates are written differently and September 11, 2001 would be written numerically as 11/9/2001 (notice how North American eyes deal with this date – the meaning fades).

The difference here is that we need to know the *format* of the data in order to interpret it with appropriate semantics.

But, as they say in the Ginsu knife commercials: Wait! There’s more! Consider the following date (in U.S. format): 9/32/2001. Our brains quickly decode that there is a fundamental problem with this date as there is no such thing as the 32nd day of September. What we are now doing is applying rules to the data – technically known as syntax – that control the “grammar” of writing dates. Such syntax determines that it is acceptable to write the month first, followed by a “/”, then the day in the month, a “/” again, and the year. (Notice how before 2000, we rarely wrote the year out as a four digit number? The syntax of date writing has changed.)

Date syntax also determines such things as the validity of writing a date such as 2/29/200x because there can only be a February 29th when there is a leap year. Date syntax also says that it is acceptable to write the date in many other forms: 9-11-01, 11 September, 2001, Sep. 11, 2001, and so on.

The only reason we can all read these dates and know what they mean to us as humans is that we have been “programmed” with an understanding of what it takes to take the *data* and turn it into information. Specifically we have been taught three things: the format, syntax and semantics of North American date representation.

It is these three things that one must have to convert data into useful information. If any of these three things are absent, one has just a pile of binary digits of 0's and 1's.

Encoded Information

Textual Characters

Representing the real world in a computer is a real challenge. Whatever we do must be based on the fact that computers can only represent data using the 0 and 1 of the binary numbering system.

How then can we represent the letters of the alphabet and decimal numbers? The answer is by encoding that data in a binary representation. Of course, it would be distinctly sub-optimal if everyone used their own private way of encoding letters and numbers because it would mean that we could not exchange information⁴.

In North America, most people (apart from IBM) use a system of encoding called quite descriptively, the American Standard Code for Information Interchange (“ASCII”). IBM, for historical and imperial reasons uses a different encoding system on some of its computer systems called the Extended Binary-Coded Decimal Interchange Code (“EBCDIC.”)⁵

Without descending into the complete technical depths, suffice it to say that the letters of the alphabet in ASCII are represented by groups of eight binary digits – such a group is known

⁴ This is not just an academic issue. Even today there are many different alphabets that computers need to represent when one considers all of the different written human languages. In the early days of computing, circa 1960, there were several contending different representations for the current Latin fonts we use in North America.

⁵ Though ASCII and EBCDIC operate in the same fashion, they use different values to represent data. Most PCs require special software to read data encoded in EBCDIC. Special care is therefore required to ensure EBCDIC files are produced in a useable format during discovery

as a "byte" of information⁶. In ASCII, the letter "A" is 01000001, "B" is 01000010 and so on, through all of the upper case letters, the lower case letters, Arabic numeral *characters* (as opposed to numeric values), and the special punctuation marks such as ~!@#\$\$%^&*() etc.

When the "A" key is pressed on a computer's keyboard it is translated by the electronics of the keyboard and the computer into 01000001 when it is placed into the computer's memory. When it is displayed on the computer's screen, the binary value of 01000001 is translated into a pattern of dots that has the appropriate letterform and color for the typeface being used. When it is printed on paper (such as you are reading right now), the hardware and software of the computer and the printer conspire to print small dots of toner or ink on paper for the appropriate letterform. Thus, the illusion is complete. Whenever it matters, the letter "A" can be typed, displayed, and printed, even though internally it is 01000001.

Textual documents can be searched only because they *are* textual and the computer can scan the underlying binary patterns that represent each character for an exact match with a keyword (also represented in ASCII). The computer can do this *precisely* only because the letter "A" is represented as 01000001 regardless of what typeface it might be displayed or printed in. ASCII text such as this is the most basic form of textual information on a computer.

Numbers

The illusion of numbers is effected in a similar way, but using a different *encoding*. A byte of information contains numeric values using the binary numbering system where each binary digit is ascribed a decimal value. In the conventional decimal system, the "columns" of a number are ascribed powers of ten. A number with four digits would have column headings of: 1000 100 10 1, so that we can write 1,234 and know it is one 1000, two 100's, three 10's and four 1's that are then added together to form the final number.

Binary works with the same rules except that, by definition the "columns" are powers of two (hence the name binary). For example:

⁶ "Byte" is a term coined by IBM to denote a group of adjacent binary digits. These days, convention has it that the byte, unless otherwise specified is eight binary digits.

| | | | | | | | | |
|---------------|-----|----|----|----|---|---|---|---|
| Decimal value | 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |
| | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 1 |

The binary number 10110011 shown in the example above really means a value of : one 128, one 32, one 16, one 2 and one 1. Adding these together (as one does for decimal arithmetic), means that 10110011 is equivalent to 179 in decimal.

Computers use binary because it is simpler and easier. There is no measuring of *magnitude* of numbers in each digit position – either it is a 0 or a 1, and the computer will use the presence or absence of voltage, or the polarity of a magnetic field to represent a 0 or a 1 internally⁷.

Is It A Textual Character Or Is It A Number?


This is the first hint of the quagmire that lies ahead and it is the source of much confusion for non-computer people.

Given that the letter “A” is 01000001, and that this also represents the decimal value of 65 (there is a one in the 64 column and a one in the 1 column, added together these are 65), then how does the computer “know” whether or not 01000001 should be a textual character or a decimal number represented in binary?

The answer is that the computer does not need to know. It is entirely up to the computer programmer to ensure all instances of bytes containing textual characters are treated like text, and those instances that represent decimal numbers are properly handled as numeric information. If a computer programmer ever makes a mistake and inadvertently treats numeric information as text then all +FpPÿvpj□èÄüf breaks loose (this being an example of some non-textual information that was misinterpreted as text by forcing Microsoft Word to open an executable program called ghost.exe).

⁷ Paradoxically, all digital computers work by using analog electronic circuitry. This causes considerable confusion when patents speak of digital signals versus analog signals. Internally a computer might, for example, use voltages between 0 volts and +5 volts and adopt the convention that a voltage greater than 3.4 volts is a 1, an lower than 2.0 volts is a zero. With this convention, the signals are “binary,” but they are so, only because an analog voltage is subjected to threshold measurements.

This "context-sensitive" interpretation of binary digits, while it may seem confusing or arbitrary to start with, is not uncommon in everyday life. We are all used to dealing with the problem of context-sensitive encoding; a red light on the instrument panel of your car does not have the same meaning as the red light on the rear-end of a bus, or a red light hanging above an intersection, or outside a building on certain streets in Amsterdam. The semantics are different; but all typically mean some variant of stop or "you have, or will have, a problem" (including the reference to Amsterdam).

Life would become quite confusing if the semantics of the color red were to mean, "it's OK to proceed." Indeed, more than one person has been confused by Microsoft's decision to require us to click on the  button when we wish to stop the computer.

Graphical Images

That small graphical image of the start button is not text even though it looks like text when it is displayed on the screen. Instead it is a small graphical image of an icon and letters. One only need look at the screen close up to see the individual graphic elements and the dots that make up the letters.



Each dot on the screen is represented as a combination of the three primary colors; red, green, and blue. The specific color obtained depends upon the intensity of these values much like mixing light of these primary colors, with black being represented as: Red: 00000000, Green: 00000000, Blue: 00000000 (no light would therefore be black). A dim yellow might be represented as: Red: 00000000, Green: 01011111, Blue: 0101000 (this would have a greenish tinge as there is more green than blue). At the other end of the spectrum (so to speak), white is represented as: Red: 11111111, Green: 11111111, Blue: 11111111.

In this graphic representation above, note that the computer is not storing text as text, but as groups of colored dots that, when displayed (or printed), happen to look like text to a human reader.

This difference between text and a graphical *representation* of text is fundamental and further serves to confuse many a lawyer when dealing with document production.

Scanned Documents

Printed documents can be scanned in and converted to graphic images by document scanners — a FAX machine is an example of this. Horizontal slices (called raster scan lines) of the document are sensed as the document moves past the scan head in a FAX machine. Equipped with hundreds of light sensors, the FAX machine senses those places on the paper that have been darkened with ink or toner, and converts each raster scan into 0's and 1's for transmission to the remote FAX machine. A document scanner works the same way. Color scanners have three sensors for each "dot" position in the scan head, and can sense the amount of red, green, and blue light being reflected back from the document.

Inside the computer (or the receiving FAX machine) these raster scan lines are re-assembled to form an image of the original document.

However, the "digitization" of the document, as this process is more properly called, is imperfect. The sensors in the FAX machine or the document scanner will not line up precisely the same way as each page passes by it — more correctly, the paper will not be aligned precisely the same way, but the effect is the same.

For example, the two images below show two words from the same document, printed on different printers but scanned in on the same document scanner and the difference between the two is quite marked in terms of the convexities and concavities on the letter forms:



For a computer to be able to search graphical images, a computer program would need to be written that was "smart" enough to be able to recognize each of the letters in the document, even though some letterforms are badly mutilated (for example, compare the "r" in both samples).

Such optical character recognition ("OCR") programs do exist, but they rarely attain more than a 98% accuracy and even that level of accuracy is sufficient to obfuscate the original text so badly that it is impossible to search accurately and reliably.

File Formats

Whether particular binary data is textual or graphical in nature is a choice made, in part, by the individual controlling the creation of the computer file. The specific internal file format is something controlled by the choice of software used to create and maintain the file. There are therefore two hurdles by the recipient of produced data: Knowledge of what format in which the data is stored, and knowledge of which application program was used to create and maintain the information.

In some specific cases, one application program can read and interpret the computer files created by another application program. For example, Microsoft Word can read the files created by WordPerfect (although not always with the exact same results as WordPerfect).

The vendor of a given application program often takes the position that the file format used by the program is proprietary (or least does not publish the information). This creates a situation where the only way that a file in a particular format can be accessed and processed is by obtaining a copy of the specific software used to create it. This becomes costly and time consuming — because of the actual cost of the software (some specialized document programs less widely used than those from Microsoft can cost around \$1,000, with specialized computer-aided design software costing two or three times more than that) and the time required to switch between applications when reviewing the evidence.

The problem is further compounded because different versions of the same application software may process slightly (or substantially) different file formats. This then demands that the same specific version of the application software be used to process the file.

A further problem occurs with such files as spreadsheets and databases (the latter being discussed more fully later in this document). Spreadsheets have a schizoid existence: they contain both the results of calculations, and, "behind the screens" the formulae that make those calculations. Spreadsheets also have user-defined format insofar as the columns and rows can contain any particular data that a user wishes to enter — and each field or value of a formula

can be encoded in a way most suitable for a user's purpose. There is no such thing as a "standard" format spreadsheet, nor can there ever be.

The Need For Common File Formats

Adobe Acrobat Portable Document Files

The problem of proprietary file formats needing proprietary software to read them spurred companies such as Adobe Systems to create what they called "Portable Document Files," ("PDF") using a program called Adobe Acrobat.

While PDF files need to be read and printed using Adobe Acrobat, Adobe distributes the Adobe Acrobat reader/printer software at no cost. One must only pay to license a copy of the Adobe Acrobat PDF *creation* software.

Over the past few years more and more organizations have realized that PDF files represent a common denominator in file formats. Once a PDF file has been created it can be read and printed on any computer on which the free Acrobat Reader software has been installed and, perhaps more to the point for commerce, when viewed and printed the document will always look the same — thus bypassing the other bane of the computing world where a document created using WordPerfect on an Apple Macintosh did not have the same fonts or layout when it was printed using Microsoft Word on a PC.

There really are two different variants of PDF files: one are those files that are created by "printing" the original document to the virtual printer created by the Adobe Acrobat software (the application program "thinks" that it is printing to a real printer, but it is an illusion created by the Adobe Acrobat software). This kind of document can, provided the correct options are selected at creation time, contain a document index and can be searched either when using the Adobe Acrobat Reader or by an associated program, Adobe Catalog, that can search groups of PDF files.

The second type of PDF file is a "PDF image" file and is usually created using a document scanner (such as the Hewlett Packard Digital Sender). These PDF files have very different traits — they are merely a scanned image of the document and do not therefore have any means for being searched. There is no text embedded within the document — just images of text.

TIFF Files

Tagged Image File Format ("TIFF", sometimes "TIF") files are another common denominator file format that is gaining in popularity, in part because this is the format used by FAX machines and in part, because Microsoft Windows (in all its flavors) contains software that allows these files to be opened and printed. In functional terms, TIFF files are most closely related to PDF image files insofar as they do not contain any searchable text, but are just images of text.

Discovery Issues

The use of common denominator file formats such as PDF and TIFF, while appearing to solve the problem of proprietary file formats and software, raises several important discovery issues:

- a) The costs of converting the original evidence can be significant.
- b) The act of converting the original evidence alters and/or obliterates potentially relevant data in the form of file names, the hierarchical structure of the original evidence and the dates and times associated with the original files. This conversion will also redact the documents in undesirable ways (such as losing the formulae associated with a spreadsheet).
- c) If PDF image files and TIFF files are created, then it will no longer be possible to search through the textual material embedded in the original files using computerized search techniques. This may significantly hamper the analysis of the data.
- d) Converting the original evidence to PDF or TIFF makes it more difficult to relate the converted file to associated data such as e-mail attachments and headers, document properties, and operating system information such as the date the original file was created or accessed.

Databases

The term "database" is an ambiguous term that has been used to cover everything from simple text files, where each text line contains a separate "record" of information, to giant data structures such as those used by credit card companies and banks to track customer contact information, spending history, and transaction records. From the point of view of discovery, the

definition does not matter as much as the problems raised for the producing and the receiving party.

What raises databases as an issue for the Law is that more and more litigants are keeping more and more data in the form of databases. Dealing with databases and discovery is a non-trivial problem because (in common with much of computing) all is not as simple as it would seem.

The Anatomy Of Databases

Databases have a very simple, perhaps deceptively simple, anatomy. Attorneys who understand this anatomy will be able to address discovery-related issues with far more facility than those who do not. We have seen counsel for large American companies involved in multi-district litigation, who felt that it was appropriate to produce printed-on-paper copies of database records (selected by them) rather than provide the underlying database information. Such a production is about as rational as having Domino's Pizza deliver color photographs of pizza rather than the real thing. It is the production of redacted, reformatted, and spoliated information in the wrong format for any useful analysis.

Fields

Individual data elements in a database are stored in "fields." For example, a customer name might consist of three fields: a first name, middle initial, and a last name. A purchase date might be a single field, consisting (if relevant to the processing) of three other fields: the month, the day, and the year.

Records

Data elements associated with a particular customer, transaction, or event are grouped together in records (the word "record" being used pretty much in its pre-computer, paper system sense). An individual record (describing a vehicle owner who is filing a complaint, say) might be:

customer name, customer id. number, address, telephone number⁸

Tables, Columns, And Rows

Conceptually, the easiest way of thinking about data in databases is to visualize it as tables, with data fields arranged in columns and rows. Each horizontal row is an individual record, and each column contains the same data field for each respective row. Continuing with the example of customer information for those customers of a car company that have filed complaints, the database table that holds information describing customers, called CustomerInfo, might appear as:

| CustomerName | CustomerId | CustomerAddress | CustomerPhone |
|------------------|------------|--|---------------|
| Alice Dogsbody | 11521 | 115, The Peebles, Scappoose, OR | 2061113232 |
| Fluffy Serpentes | 15390110 | Apt. 12, Lolita Gardens, Mississauga, Ont. | 4162015481 |
| * | 0 | | |

Record: 1 of 2

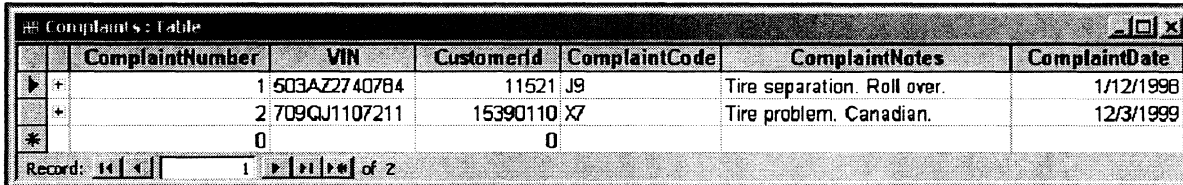
Each row represents a different customer. Each column (as the column headings suggest) represents a specific data value for that entity.

Of particular note is that the CustomerId is apparently an arbitrary number assigned (one presumes) by the car manufacturer (or the dealer) to whom the complaint was reported. There is no specific link to any complaint or complaints (it being entirely feasible that a single customer could have lodged one or more complaints).

What is not apparent is how this table could be searched? Would the CustomerName field or the CustomerId field be considered the “key” value? For proper searching, the “primary key” field (as it is known) must be unique for all of the rows in a table, and therefore the CustomerName could not be used as it would potentially be ambiguous. Therefore, one could predict that the CustomerId is likely to be the primary key (but, absent any information that explicitly states this, this is conjecture).

⁸ This is hypothetical data. A real customer record would probably contain far more information and far more detail.

In this hypothetical example (of customers complaining to a car company), there would need to be other tables that record the specific complaints, and details of the vehicles. Here, for example, is a hypothetical table for complaints:



| ComplaintNumber | VIN | CustomerId | ComplaintCode | ComplaintNotes | ComplaintDate |
|-----------------|--------------|------------|---------------|-----------------------------|---------------|
| 1 | 503AZ2740784 | 11521 | J9 | Tire separation. Roll over. | 1/12/1998 |
| 2 | 709QJ1107211 | 15390110 | X7 | Tire problem. Canadian. | 12/3/1999 |

This table reveals a sneak preview of the challenges that lie ahead in that, even with this ultra-simple hypothetical, one must start *inferring* information about the contents of the tables in order to be able to turn the *data* in the tables into useful *information*. Specifically, one must infer:

- a) The only link between a complaint record and a customer record is the CustomerId code. In technical terms, the CustomerId is acting both as a Primary Key for the CustomerInfo table, and also as a "Foreign Key" in the CustomerInfo table for each entry in the Complaints table (in that it occurs in the CustomerInfo table and is used to access data in the Complaints table). However the CustomerId cannot be the Primary Key for the Complaints table as one customer may have filed more than one Complaint and database rules demand that the Primary Key be unique within the table.
- b) The ComplaintCode is encoded in some arbitrary way that is opaque. Without the specific semantics for this ComplaintCode field, one could never determine what the meaning was. What is a J9 complaint? Could it mean that the incident about which the customer complained involved a fatality?
- c) In the ComplaintNotes, which appears to be a free form text field, there is no guarantee that a tire might not be a tyre (if any of the dealers were in the U.K.).
- d) The ComplaintDate format has not been identified, so 1/12/1998 could be either January 12th, or December 1st.

The final table for the hypothetical is the VehicleInfo table:

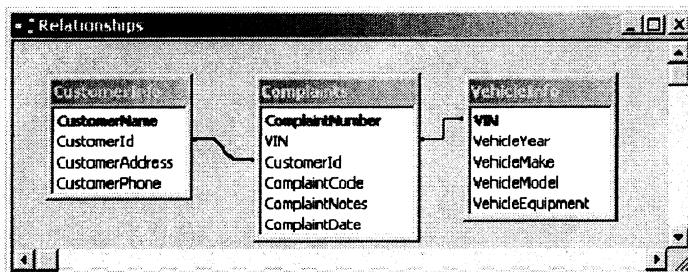
| VIN | VehicleYear | VehicleMake | VehicleModel | VehicleEquipment |
|--------------|-------------|-------------|--------------|-------------------|
| 503AZ2740784 | 1996 | Ford | Explorer | ATX tires |
| 709QJ1107211 | 1998 | Ford | Expedition | Bridgestone tires |

We can reasonably infer that the VIN (Vehicle Identification Number) is unique, and that this will be used as the Primary Key. All other fields appear to be self-evident (which is unusual and unrealistic were this to be a real-world database).

Relationships

What is less than obvious is that these hypothetical tables have relationships between them. A customer may have more than one vehicle. A customer may have filed more than one complaint about each vehicle. A vehicle might have more than one owner, each of whom might have filed more than one complaint.

These relationships, none of which are explicitly stated in the tables, can be represented diagrammatically – but even then, they are not all immediately obvious:



Views

The hypothetical thus far has focused on the possible *physical* organization of the data in the database. Life is rarely kind enough to allow us to use the data only in the way it has been stored. Often we need to get a different view of the data in order to make better sense of it. For example, we might wish to view this hypothetical data in a way that would show either (a) which customers have which vehicle models, or (b) which vehicles have which complaints against them.

An example report for Customers and Vehicles is shown below:

CustomersWithModels

Which Customers Have Which Vehicle Models

| Customer Name | CustomerId | Customer Address | Phone | Year |
|----------------|---------------|---------------------------------|-------------------|------|
| Alice Dagsbody | 11521 | 115, The Peebles, Scappoose, OR | 2061113232 | 1996 |
| Vehicle Make | Vehicle Model | VIN | Vehicle Equipment | |
| Ford | Explorer | 503AZ2740784 | ATX tires | |

| Customer Name | CustomerId | Customer Address | Phone | Year |
|------------------|---------------|--|-------------------|------|
| Fluffy Serpentes | 15390110 | Apt. 12, Lolita Gardens, Mississauga, Ont. | 4162015481 | 1998 |
| Vehicle Make | Vehicle Model | VIN | Vehicle Equipment | |
| Ford | Expedition | 709QJ1107211 | Bridgestone tires | |

Page: 1

And here is the report showing which vehicles have which complaints:

Complaints

Which Vehicles Have Which Complaints

| VIN | Code | Date | CustomerId | Complaint # | Notes |
|--------------|------|-----------|------------|-------------|-----------------------------|
| 503AZ2740784 | J9 | 1/12/1998 | 11521 | 1 | Tire separation. Roll over. |
| 709QJ1107211 | X7 | 12/3/1999 | 15390110 | 2 | Tire problem. Canadian. |

Page: 1

The most salient aspect about Database Views is that the views that are available depend entirely on the availability of the underlying data – if portions of the database have been omitted from production, then certain views of the data will either be impossible, or costly and time-consuming to produce.

Turning Databases Into Useful Information

Databases are merely organized versions of individual data fields. As a result, they too are subject to the same traits as the simple data values discussed earlier in this paper: unless you have knowledge of the encoding, format, syntax, and semantics you will not be able to transform the *data* that you received from the opposing party into the useful *information* that you requested and need to build your case. For databases, unlike individual data fields, you also need to know the relationships that exist between the various tables. While some of this

information could be inferred, in a medium to large corporation there can be hundreds or thousands of database tables, and making those inferences by inspecting the data can be burdensome in the extreme.

Discovery

Evidence Preservation

The main focus of this paper is discovery, but if evidence is not preserved it cannot be produced. In the authors' experience, aggressive early preservation should be discussed, and if need be, ruled on, very early in the litigation. This is especially true because computer-based evidence can easily be destroyed by improper handling, hardware or software failures, virus activity, or even normal use of the computer system.

Many computers use automated housekeeping tasks, often invisible to the casual user, which can result in the wholesale destruction of relevant evidence. Preservation discussions or orders should explicitly identify whether routine automated tasks such as tape recycling, deletion of unused files, and purges of e-mail older than thirty days should be allowed to continue. To avoid allegations of spoliation, producing parties should communicate preservation requirements to their computer system administrators and ask for their help to identify all manual or automated processes that might result in data destruction.

Orders to preserve or copy the contents of hard disks should explicitly state whether or not deleted files and file fragments are to be copied. If a "mirror image" (an exact copy of the entire contents of a hard disk, including deleted files and file fragments) is desired, special software must be used to prepare the disk copy. The routine backups that most individuals and companies use for their computers do *not* normally accomplish such preservation.

To avoid any possible confusion, the court order should use the term "a mirror image backup, including active files, deleted files, and file fragments" if this is the intended preservation requirement. On more than one occasion the authors have observed lengthy arguments about whether an order "to preserve the entire contents of the hard disk" included preservation of deleted files.

In litigation involving large businesses, care should also be given to identifying proper handling for computers used by departing contractors or employees, as these computers are

often “recycled” and assigned to a new user. The “recycling” process generally includes removing all old files and re-installing fresh copies of the computer’s software. Left in place, these processes typically result in the destruction of all files left behind by the previous user.

If databases are to be produced, care should be taken to preserve a record of the database structure and relationships, along with the information required to decode data stored as encoded numeric codes or abbreviations. Preserving this information along with the data itself is important because the database structure, relationships, and encoding information may all be changed in the normal course of business and may be difficult (or impossible) to recreate at some future point in time.

The Challenge Of Discovery

Business records, correspondence, e-mail, databases, spreadsheets, presentations, documents, electronic calendars, contact lists, digital images, photographs, recordings, and faxes all originate on computers. Only a small fraction of this information is ever printed, mandating the need for production of computer-based evidence.

Not only is data encoded, but it is also formatted according to rules used by the specific computer hardware and software that created the data. Different kinds of documents, databases, pictures, and recordings each have their own format. This means you cannot use just any program to read a file – it has to be a program that recognizes the file’s specific data format and encoding, and is capable of turning the raw data back into useful information. In order to effect this transformation the program often requires additional supporting information

What Do You Ask For?

When discovering electronic evidence, you must therefore ask for both the electronic data itself and also *for sufficient information about the data you receive to allow you to use it.*

It is important to determine what kind of software and hardware was used to create and maintain the data received or produced. Three important questions are: “What type of computer was the data created and maintained on?”, “What operating system was the computer using?”, and “What specific programs and settings were used to create or copy the data?”.

You may need this information early in the discovery process, even before any electronic information is produced. For example, consider the case where both parties agree to limit production of e-mail and documents to files that contain specific keywords. It is possible for the producing party to use computer programs to search for documents containing the keywords, but the programs used for the search must be able to read the file format for each type of file to be searched. Failure to choose an appropriate search program will yield unreliable results.

Even after the initial three questions are answered, additional information will be required to extract information from the data in databases, spreadsheets, computer generated reports, and certain other computer files. Such files all contain data with user-defined syntax and formatting – the nature of the data, number of fields, and arrangement of the data was initially defined by the data's user.

For business records and databases it is also common for information to be represented using abbreviations or codes composed of alphabetic or numeric characters. For example, numeric codes might be assigned to represent a specific customer number, product number, medical procedure, or type of consumer complaint. In order to locate relevant evidence you must know the *semantics* of what specific codes mean, which data files are used to record the information you seek, and how the data is arranged.

If discovery involves databases, computer generated files, or computer reports, your discovery request should seek information about the *format, syntax, semantics, organization, and schema* of any data you receive.

Computer-based evidence can often be context-sensitive – that is, its relevance to the case may change depending upon where it was found and when it was created, accessed or last modified, and by whom. All of these are traits that may be found in meta-evidence (which is discussed in the following section on meta-data). Electronic discovery often involves data from more than one source. The production may involve multiple individuals, files, computers, backup copies, or business entities. In such cases it is important to make sure that the *provenance and business context* is preserved for any electronic evidence produced. At minimum, this information should contain the facility, business unit, computer, user, and relevant date information.

The Discovery Of Meta-Data

Meta-data is a term used to include a hierarchy of information that is automatically generated and recorded during the course of a computer's normal use. Most meta-data is invisible to the casual user.

At the lowest level of abstraction, file specific meta-data is recorded automatically by the computer when a file is created or used. At this level, the meta-data is specific to a single data file, document, or e-mail. Meta-data may include information such as the file's author, when it was created, when it was changed, and when it was used. E-mail meta-data includes information about where the e-mail originated, how it was routed during delivery, whether it was ever opened, what (if any) files were attached, and who else may have received a copy.

Other types of meta-data provide information about the configuration or use of entire computer systems or networks. This information includes records of system activity such as sign-on logs that identify when and who was using a computer, backup logs that identify what backups may exist, when they were created, and what each backup might contain. Other forms of system meta-data include records of whether the computer was attached to a network, what files a computer hard disk contains, and event logs that show network traffic, file transfers, faxes sent, or system configuration changes.

Many forms of meta-data are fragile, and can be easily destroyed by improper handling. Meta-data is valuable for both analysis and authentication and therefore its preservation must be explicitly requested.

Careful consideration should be given to which forms of meta-data should be produced during the discovery of electronic evidence. Because courts vary their interpretation (and understanding) of meta-data you may find it necessary to explain the need for e-mail specific, file specific, and system specific meta-data separately. It is important to note that steps must be taken to preserve meta-data as early as possible, since acts such as restarting the computer or opening files for inspection result in the destruction of certain types of meta-data.

Rule 26(b)1 of F.R.C.P. states:

COMPUTER-BASED EVIDENCE : CUTTING THE COST OF DISCOVERY

Andy Johnson-Laird and Barbara A. Frederiksen

For good cause, the court may order discovery of any matter relevant to the subject matter involved in the action. Relevant information need not be admissible at the trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence.

Of particular note is the fact that the court will admit discovery of information "reasonably calculated to lead to the discovery of admissible evidence." This is perhaps the closest that the F.R.C.P. comes to describing the very nature of the system level meta-data, which may not be direct evidence, but almost inevitably *leads* to direct evidence.

We Requested Information, The Other Party Produced Data!

Once discovery commences, expect the technology to present you a new set of challenges. You know what you asked for, but what did you get? With paper-based productions, you can simply look in the box and review its contents. With computer-based productions all you can tell by looking in the box is whether you got square things or round things – even if the media is labeled there is no way you can read the contents of the media without resorting to a computer, and no way to even tell if it is readable until you try.

Even attempting to read the media may be a challenge. Hardware and data formats will present a series of barriers, nested like Russian dolls, between the evidence and understanding. Once one has determined what hardware and software was used to produce a tape or disk one will need to use a compatible hardware and software configuration to read the media, which, in the case of a computer backup tape, will probably be thousands of discrete files. To determine what each file contains one must now open and inspect each file, again using a program that is compatible with the format imposed by the software that created the file. If the file is a spreadsheet, database, table, or chart, one must then decipher what the rows and columns mean, what context they are specific to, and what encoded data values and abbreviations represent, before the data becomes information.

It is not uncommon during this phase to discover that one must ask for production of additional evidence, documentation, or meta-data in order to determine what exactly one has received.

Inventory Issues

One of the problems that emerge immediately as you attempt to inventory electronic evidence is the not-so-simple matter of tracking electronic documents. With paper documents it

is common for each page to be individually Bates stamped. Each physical item you can hold in your hand bears a separate Bates number. In contrast to this, a single disk may contain tens of thousands of documents, each with multiple pages. All of this material is likely to share a single Bates number and without modifying the evidence, there is no way to electronically affix a Bates stamp to individual files.

Unlike paper documents, which are often filed (and occasionally produced) in an orderly fashion, there is often little or no organization to the contents of a computer disk. A single disk or tape may contain documents created and maintained by many different individuals, with responsive and irrelevant information intermixed, and no apparent order with respect to chronology, context, or subject.

To complicate matters further, there is no requirement that files on a disk or tape have unique names -- many different files on a disk may all have the same name⁹, even if they have different contents. File names are independent from content -- there may be many different files, each with a unique name but identical contents.

Several techniques exist to help manage tracking for electronic documents and files. One of the simplest is to create a directory containing a list of the contents for each individual piece of computer media. The listing should show each file name, along with the full path of sub-directories needed to access it. Since file names are unique within a directory, this listing can then be imported into a simple spreadsheet or database to allow tracking of individual files.

Programs such as MD5SUM10 can be used to generate message digest "signatures" based on the contents of electronic files. These signatures can be used like fingerprints to help identify files that contain identical information, as well as to identify instances where files with the same name have different contents. By making these signatures a part of your tracking

⁹ The computer requires only that files with the same name not be present in the same sub-directory. It is common to see many files on a hard disk with the same name. In some cases the contents of the files is also the same (they are all copies of the same original). In other cases even though the files have the same name, their contents (and context) may differ.

¹⁰ MD5SUM.exe is a program that uses a one-way mathematical hash function to generate a single string of digits (called a message digest) that can be used to aid in file identification and authentication. A copy of this program is available free on the Internet. See the following specific site reference:

http://www.openoffice.org/dev_docs/using_md5sums.html (Visited June 1, 2002).

document you can use them to identify duplicate documents during review and also to identify multiple revisions of the same document. As an added benefit, these same signatures can also be used to identify any tampering. If even a single character in a file is changed the electronic signature will also change.

Search and concordance software can be used to help identify documents relating to specific subjects. Once identified, subject keywords can also be added to the tracking spreadsheet.

Ancient (And Modern) Geek Archeology

Another problem you may encounter during discovery or inventory is that of unknown or unreadable media or file types. In cases involving electronic evidence that is more than a couple of years old, you may have difficulty finding either hardware or software that can read your files. In the case of databases and computer files with proprietary file formats you will also need information about the specific file's organization, contents, and data relationships. In the authors' experience it is a sad truth that such documentation seldom lives as long as the data itself.

Assuming that the producing party still possesses the requisite technology and documentation, the discovery process should include negotiations for access to the appropriate hardware and software. If neither party possesses the required technology, some media types may need to be sent to third party conversion companies. Be warned that you may encounter unexpected problems with the conversion process, so scheduling should be generous enough to allow for some delays.

At the opposite end of the hardware life cycle is media that represents state-of-the-art technologies. Drives capable of reading such media may be back ordered or difficult to find. Emerging technologies may be plagued with unstable software or subtle (and not-so-subtle) incompatibilities between releases of hardware or software. If the case involves multinational entities, be prepared for the possibility that some devices may be unavailable or inoperable in your home country.

Printed Evidence Is Often The Most Maximally Inconvenient Form

Once you begin your inventory, you will discover another characteristic of computer based evidence – its volume. A 110 gigabyte hard disk you can hold in the palm of your hand may contain documents that when printed yield a stack of paper several miles high (36.7 million pages). A single CD-ROM can yield a stack of paper 66 feet high.

From time to time the authors have been asked to print and produce the contents of an entire hard disk, but we recommend this approach be avoided. Aside from the obvious danger of avalanche, printing redacts the meta-data from electronic evidence, and renders impossible most forms of computer-aided analysis.

Unless special steps are taken to preserve it, most meta-data is lost when a document is printed. This includes document properties such as author, creation date, revision date, revision history, date of last accessed, and location on the hard disk where the document was found. When printing spreadsheets (and many databases) the choice must be made to print either a cell's value or the numeric formulae used to derive it – either way something valuable is lost.

The printed version of electronic evidence cannot be searched electronically. It cannot be used to derive earlier revisions, or readily sorted into chronological sequence. Automated techniques cannot be used to compare the contents of multiple printed documents, or to identify printed duplicates.

Production Completeness, Quality, And Scope

As discovery progresses, expect to identify issues relating to the scope and completeness of production. In the early phases of discovery it is common to uncover new databases, applications, computers and even facilities that must be added to the scope of the production effort. At the outset the parties will probably not know how many computers must be searched or what backups may exist.

If the discovery involves corporate computers you are likely to discover that there is no central person or department knowledgeable about *all* of the computer systems that exist. In the business world it is quite common for computers to be administered according to the type of operating system they run rather than the business purpose they serve. Mainframe computers,

servers, and desktop computers will normally be backed up separately, and the resultant backups managed by separate groups, following separate policies.

A further distinction exists between the *system level* backups (typically made by system administrators who are responsible for recovery from catastrophic failures) and *application level* backups (typically made by programmers working for or with the specific business unit who owns the business application). If database systems are involved there is often a separate set of backups performed by the database administrators.

In large scale litigation, testimony of 30(b) 6 witnesses can be extremely helpful in identifying information relating to the scope of production. Key areas of inquiry include corporate electronic document retention policies, *system level backup processes* and retention, *application level backup processes* and retention, number and topology of networked computers, operating systems used, database architectures and applications, and what techniques were used to locate and preserve data relating to the litigation.

Another valuable source of information relating to both scope and completeness of production is system level meta-data. System level meta-data such as control files and logs can be used to help identify which computers run which software, which computers, programs, and users have access to which hard disks or databases, where e-mail is stored, and what backup tapes or disk files exist. File specific meta-data can be used to limit the scope of production to only those files from a specific period of interest or (in some cases) user.

As discovery proceeds it is also important to evaluate the quality of the electronic evidence. Any oral testimony about what computers, backups, or databases exist should be compared to the actual production. If samples of reports have been produced on paper it is important to compare them to their electronic counterparts, to make sure all related data files have actually been produced, and that the files contain all of the relevant information elements needed to compose the corresponding report.

Media should be checked to determine if it can be read, and if the data it contains is consistent with any description provided for the media's contents. Despite careful handling some media may be mislabeled or damaged during shipping, requiring replacement copies or supplemental information to remedy the production.

If multiple computer files exist for the same domain of data they can often be used to cross check each other, allowing one to identify missing records, missing date ranges, or records that appear to have missing elements.

Computer files should also be checked to ensure that the data they contain is consistent with their file specific meta-data. An examination of file modification and creation dates can help determine if the data has been tampered with or contaminated during production. When using meta-data to evaluate the quality of production, it is important to first evaluate the quality of the meta-data itself. Care should be taken to ensure that the system dates and times, which are based on the computer's internal clock are accurate, and that the meta-data itself has not been damaged or altered.

Beyond Bates - Identification, Validation, And Authentication

During discovery it is important to obtain the information that will help you identify and authenticate any electronic evidence you rely on in the courtroom. Since electronic files are not individually Bates numbered special care must be taken to record where and how they were located. Sufficient chain of custody information should be preserved to document who has handled or copied computer media and what has been done to it. Information required to validate origin, establish authorship, and authenticate contents must be preserved if available.

In the authors' experience it is valuable to both parties to identify and follow a protocol for the production of computer-based evidence. Such a protocol specifies the logistic details of production, identifies mutually acceptable media formats, media labeling, Bates numbering, and specifies the records that will be created to track origin or custody of the evidence.

Records that permit identification of the producing agent and business unit responsible for production should accompany electronic media. Information should include the name of the entity producing the information along with country, city, site, and department sufficient to uniquely identify the producing agent.

These records should also identify the specific computer system from which the backup was produced or information copied. If known, the records should also preserve the identity of the specific computer system upon which the information was originally created along with the name of the individual who created or maintained the data.

For copies of hard disks, tapes, or CD-ROMs, records should be maintained and produced along with each piece of media to document how, when, and by whom the copy was prepared.

For individual computer files, records should be maintained to document both the file's origin and how it was copied. In the case of databases or other files which are not produced in the same format as they are stored, the record should identify the original format (e.g. "Oracle database") and the format used for the production ("Oracle database unload" or "tab delimited text file"). Any process used to redact or reformat the data should also be identified.

For e-mail, it is important to preserve the origin of the e-mail (producing party, computer, e-mail id, and mailbox or folder). The original e-mail headers and routing information must be produced along with the body of the e-mail and identification of all attachments. The e-mail header and routing information is important because it offers valuable information that can aid in determining the true origin and authenticity of the e-mail.

Bates Number Files At Your Peril

Occasionally, parties will insist upon imposing the paper document paradigm on the computer-based evidence and will want to Bates number each document by prefixing or suffixing a Bates number on a file name. The presumed thinking being that it will make it easier to identify a particular document unambiguously.

Unfortunately, this is a false economy, because changing the name of the file has the effect of a controlled spoliation of the evidence.

For example, imagine a file called "Business Plan.doc". There are essentially two choices for associating a Bates number with this name: prefixing it, or suffixing it, thus giving rise to either "JLI004721-Business Plan.doc" or "Business Plan.doc-JLI004721".

Both strategies create problems. Prefixing the name with a Bates number means that directory listings with file names cannot (without significant machinations) be used to identify documents that are *likely* to be different versions of the same document – the Bates number serves to make the file names sort differently. Suffixing the name with the Bates number completely bamboozles Microsoft Window's ability to open the document with the appropriate software – a feature that uses the characters after the last period in the name to associate the file

with appropriate application software. Double-clicking on a file named "Business Plan.doc-JLI004721" produces the equivalent of a computational "huh?"

The far less invasive method is, as suggested in this paper, identify the *media* produced, and then rely on the normal naming of computers, directories and subdirectories and files that serve to uniquely identify files as normal (outside the context of litigation). For example, if a magnetic tape is identified as JLI000109 and it is a backup of a computer called **fire**, then within the file system on **fire**, each file is uniquely identified by its directory "path" and file name. For example: "d:/My Documents/Business Plans/Business Plan.doc".

A complete listing of all media, showing all directories and files can then be created and Bates numbers can be assigned to each line item in that – or you can accept that a reference such as "JLI000109 fire d:/My Documents/Business Plans/Business Plan.doc" is unique and therefore serves the identical purpose that a Bates number would do. Indeed, it can be argued that it is far more efficient than a Bates number because it directly identifies what the material is likely to be, as well as the provenance of that material.

Production Pitfalls

The Trouble With TIFFs

As a general rule, computer-based evidence is most useful when produced in the form in which it is created and maintained on the computer. However, we have seen an increasing trend (especially in large scale litigation) where counsel stipulate that all documents be produced in an altered, but mutually-acceptable form, such as Adobe Acrobat Portable Document Format (PDF) or as a Tagged Image File Format file (TIFF).

Production in a form other than the original is not without risk. Inevitably there will be some sacrifice in both the quality of the data and the ability to process it either using the original software used to create and manage it, or the ability to deploy forensic tools to perform computer-based analysis for litigation.

That said, forms such as PDF may offer some convenience by virtue of the ease with which they can be viewed without the need for special software. If special care is taken early enough in the negotiations between the parties, then much of the meta-evidence can be preserved. The challenge is to preserve it so that it can be used as though it was still associated

with the original document before conversion to, say, PDF. For example, if the dates/times when documents were created, modified or last accessed are properly preserved, and they are linked to the associated PDF, then one can sort the PDF files in chronological order just as one could do with the original documents.

Conversion of documents to scanned images carries a further downside — as a scanned document, one cannot perform any textual searches. With appropriate homage to Rene Magritte¹¹, the document is no longer a document, but is an image of a document. This also applies to PDFs, which have the further confusing characteristic that they can either contain just a scanned image (which cannot be searched), or a scanned image with appropriate textual content for searching, indexing etc. (albeit only with Adobe software).

This means that the available options for searching and indexing depend entirely on the process used to convert a document into a PDF or TIFF form. This conversion must be negotiated *before* thousands of documents are converted as the process is irreversible if one creates files that are purely scanned images.

Database Production Issues

A *database* is a specialized type of computer file in which the organization of the data is optimized to support flexible reporting and data retrieval. In discovery, databases require additional intellectual life-support and special handling to render the information they contain useable.

A formal definition of the data in a database and the relationships that exist between various data elements is called a *schema*.

These data relationships allow for very flexible data retrieval and reporting, using different logical *views* of the data. A logical view determines which data elements, from which table(s) will be processed. Logical views can be used to produce extracts of the data for use by programs, or to produce printed reports that serve some particular business need.

¹¹ Who painted an image of a tobacco pipe with the caption (albeit in French) "This is not a pipe." The point being that it is an *image* of a pipe, not the pipe itself. As such it has very different characteristics than those of a real pipe.

Data is retrieved from databases using *queries* that are written in a specialized language such as Structured Query Language (SQL). Queries may include data from several different tables, or even several different databases into a single logical view. Queries may also exclude specific data elements, records (rows), or tables from a logical view.

Logical views reveal only specific portions of the data in the database, arranged in a specific order. Looking at the contents of a database through a particular view is like looking into a room through a keyhole in a door. Unless the actual queries used to extract data from a database are known, one cannot know what data has been included (or excluded) from the results.

There are many different database management systems (DBMS) such as Oracle, DB2, Informix, IMS, SAS, and Microsoft Access. Each of these has potentially different implications with respect to discovery.

From the purely technical standpoint, the least burdensome and most cost effective form in which to produce or *receive* a database, is the so called "unload" created by the actual database software used to create and maintain the database. To be useful, though, the "unload" must be accompanied with sufficient format, syntax, semantics, and schema information to permit rebuilding the database. This approach normally only works if the data is to be reloaded by the same software used to create the unload (and it may prove expensive in time and cost to obtain the software or configure the environment).

An alternative approach is to get the entirety of the database in some "neutral" format not tied to a specific database program. With this format the data can readily be reloaded using any DBMS for analysis, presuming that appropriate format, syntax, semantic, and schema information are also available.

In addition to format, syntax, semantics, provenance, and context, electronic discovery requests for databases should also ask for the information required to restore the database and understand its relationships. The data itself must be accompanied by appropriate information about the underlying DBMS, the exact unload or extract process, the selection criteria and view imposed on data extracts, an explanation of any redaction process, and sufficient information about the schema or data relationships to allow the database to be rebuilt for analysis.

Computer Programs

Computer programs can exist in two forms – as human readable *source code* (the form used by a programmer to create and maintain the program) and machine readable *object code*. Source code is used to understand what a program does and how it operates. Object code is needed to actually run the program.

If discovery is to include computer programs, the discovery language must be explicit as to which of these forms are to be produced¹² and what accompanying documentation is required.

E-mail or E-mangle?

In discovery, e-mail may require special handling. If individual e-mails are to be produced the parties should agree in advance about what formats should be used, and how header information, meta-data, and attachments are to be handled.

As a general rule, e-mail is most useful when produced in the form which it is created and maintained on the computer. The authors have noted a growing trend where counsel stipulates that all e-mail will be produced as TIFF or PDF images. Special care must be taken to ensure that the resultant production is still electronically searchable and that the textual body of each e-mail can still be linked to its associated headers, meta-data, and attachments. Without these links the receiving party will be unable to authenticate the origin of the e-mail, open associated attachments, identify other recipients, or readily sort the e-mails into chronological sequence.

The Damned

Modern computer-based evidence adds new meaning to the phrase “damned if you do, damned if you don’t.”

¹² For more information about source code and object code see Andy Johnson-Laird’s article, “Discovery in Computer Software Patent Litigation,” 1998 Fed. Cts. L. Rev. at <http://www.fclr.org/1998fedctslrev1.htm>

So Much Evidence, So Little Time

The over-arching challenge with computer-based evidence, as has been described above, is the sheer massive volume of it. It is not unusual in large cases to have to deal with 450 *gigabytes* of evidence.

Such volumes, unthinkable just a few years ago, are becoming routine. This mass of evidence creates major problems for the producing party who has to actually manage its production, the receiving party, who has to find a place to put it, and for both parties with the courts, who are still generally marching to the drummer of document production on paper.

A prudent approach may be to stipulate to a document production schedule that takes into account the volume of evidence to be produced rather than permit a court-imposed (and thereby inappropriately short) amount of time.

This is not a new problem. The volume of computer-based evidence in productions has been growing exponentially – all that has happened in the last few years is that we are now on the steep part of the exponential growth curve, but the courts (and many attorneys) have not yet fully grasped just how technologically serious this problem is.

Saving The Best Until Last

Murphy's Law For Forensics clearly states: "For any given case, you will find the best evidence last." It will be, more likely than not, the *last* magnetic tape, or the *last* hard disk, or the *last* set of computer files, that contain the heart of the case. Or so it seems.

However, the Court and opposing counsel are not likely to be sympathetic to this – because it has the *appearance* of deliberately trying to sneak relevant evidence in at the last minute.

The fundamental problem is that, with a vast amount of evidence, you cannot find everything all at once even with dozens of supercomputers searching and sifting the evidence. Forensic analysis of evidence is not a drunkard's walk through that evidence, nor is it a massive combine harvester consuming entire bodies of evidence at a single pass. The analysis must be systematic and follow rational threads of research and chains of inference.

It is a no-win situation. If one finds the evidence consistent with Murphy's Law, then you will be damned for finding it "late" – and, of course, if you do not find it all, you will implicitly be damned for one's inadequacy.

The fallacy in the notion of being "late" is caused by the notion that we know how long it should take to analyze a terabyte of evidence. Not only do we not know, but we cannot know – because the answer depends upon what is contained therein and what one finds first.

Shot In The Foot By Your Own Smoking Gun

For the producing party the challenge of marshalling and inspecting the evidence prior to production is a significant one. It does not serve a client's interest well to merely hand over gigabytes of information if, hidden in the mass of data, are privileged documents.

Assuming that there are indeed smoking gun documents in the production, it is prudent in the extreme to at least know that they are there before producing them to opposing counsel. But to do this may demand a small army of paralegals reviewing documents, uncompressing compressed files (and the compressed files that may be contained therein), searching documents for key words and phrases before documents are produced.

Again, this is a no-win situation. One is damned if one takes too "long" to produce or analyze the evidence, or damned if you meet the artificially set deadline and overlook the smoking gun document.

De-duping Or Duping?

De-duplicating (that is the removal of duplicate documents) demands that considerable care be taken to document which documents are thereby removed.

De-duplication can distort the truths that the evidence contains unless a complete, detailed log file is kept of all files removed from a production.

Indeed, as a general rule, it would be better for a producing party *not* to perform the de-duplication. While the absence of de-duplication by the producing party increases the burden for the receiving party (by increasing the overall volume of evidence), it gives the receiving party far better opportunities to determine the factual truths contained in the evidence, rather than have to analyze an evidentiary jig-saw puzzle with unknown pattern and missing pieces.

Conclusion

Electronic evidence poses its own special set of challenges for the discovery process. Without the intellectual life-support of information about data's format, syntax, semantics, organization, schema, and context it is extremely difficult to transform computer data into useable information. This information should be requested as part of the normal discovery process.

Attorneys who understand the pros and cons of the production and analysis of computer-based evidence can better manage (and potentially reduce) the costs of the litigation and better inform the courts of the realities of scheduling.

In the authors' experience it is advantageous if the parties can agree in advance to a protocol for the production of electronic evidence. Many of the pitfalls and problems of electronic discovery can be avoided by careful planning and record keeping. If the parties can agree on how media should be labeled and tracked problems due to defective media or accidental omissions can be quickly identified and remedied.

The time and cost of the production of computer-based evidence can be managed rationally but to do so requires some technical knowledge of the pitfalls.

*** END ***

Appendix A : Sample Production Protocol And Discovery Language

DEFINITION

1. "DOCUMENT" has the broadest meaning accorded to that term by Rule 34 of the Federal Rules of Civil Procedure and Rule 26 of the Federal Rules of Evidence, and includes, but is not limited to, any kind of written or graphic material, however produced or reproduced, of any kind or description, whether sent or received or neither, including originals, copies, drafts and both sides thereof, and including, but not limited to: papers, writings, objects, letters, bills, memoranda, electronic mail, notes, notations, work papers, reports, books, book accounts, photographs, tangible things, correspondence, reports and recordings of telephone conversations, telephone logs, statements, summaries, opinions, agreements, ledgers, journals, records of accounts, checks, summary of accounts, spreadsheets, databases, receipts, balance sheets, income statements, confirmation slips, questionnaires, desk calendars, appointment books, diaries, graphs, test results, charts, data files, log files of computer access and activity, and all of the records kept by electronic, photographic or mechanical means and things similar to any of the foregoing, including computer media, regardless of their author.

PRODUCTION PROTOCOL

2. Each individual piece of computer media produced must be clearly labeled with a unique media control or Bates number which is indelibly written on, or affixed to, both the media itself and any enclosure or case produced with the media. This label or marking will be affixed in a place and manner which does not obliterate any labeling on the original media, and which does not interfere with the ability to examine or use the media.

3. Electronic records and computerized information must be produced with sufficient information to permit identification of the producing agent and business unit responsible for the production. This information shall include, but not be limited to:

- a) The name of the corporation or other entity that is producing the information, along with information such as country, city, site, and department sufficient to uniquely identify the producing agent.

- b) The name or identity of the specific server or computer system from which the backup was produced or information copied.
- c) The name or identity of the specific server or computer system upon which the information was originally created, and the name of the individual who created and/or maintained the information.
- d) The name or identity of the specific server or computer system upon which the information was maintained during the course of normal business, if different from the system where it was created.

4. Electronic records and computerized information must be produced in an intelligible format or together with a technical description of the system from which they were derived sufficient to permit rendering the records and information intelligible. This description shall include, but not be limited to:

- a) The manufacturer's name and model number for electronic hardware used to create and maintain the electronic records.
- b) The name and version of the operating system used on the computer where the electronic records were created and maintained.
- c) The manufacturer's name, product ID, and version number for any software used to create and maintain the electronic records, along with any proprietary software, written documentation, special parameters, and instructions sufficient to permit those records to be read from the media produced.
- d) The date, if known, when the information was first created, along with the date of its most recent modification.
- e) All decryption or access passwords necessary to unlock any computerized information produced, including without limitation, electronic mail passwords and file decryption passwords.

5. Except where redaction is required by law or privilege, any record, document, or data item which was created on a computer or computer system must be produced on computer media in the original unredacted form in which it was created and/or maintained. For all such media produced, external labels on the media shall contain a unique tracking

number which can be used to associate the media with appropriate identification for the computer(s) from which the copies of computer files were made, and the full names of the individuals or business units who used the computer so identified. A record shall also be maintained and produced which shows how the information on the media was copied, and whether or not it is a complete and forensically accurate copy of the original.

6. For any electronic records, documents or data items produced, the producing party shall verify that it has modified its document retention policies in a manner that will ensure retention of the original records, documents and data items. These document retention policies shall include, without limitation, policies which automatically delete electronic mail or remove unused files, policies which permit overwriting of computer media for system backup functions, and similar policies.

7. Should the producing party seek to withhold any document based on some limitation of discovery (including but not limited to a claim of privilege), the producing party shall supply a list of the documents for which such limitation of discovery is claimed, indicating:

- a) The identity of each document's author, writer, sender.
- b) The identity of each document's recipient, addressee, or person for whom it was intended.
- c) The date of creation or transmittal indicated on each document, or an estimate of that date, indicated as such, if no date appears on the document.
- d) The general subject matter as described on each document, or, if no such description appears, then some other description sufficient to identify the document.
- e) The claimed grounds for the limitation of discovery (e.g., "attorney-client privilege").

8. Should the producing party seek to redact any document based on some limitation of discovery (including but not limited to a claim of privilege), the producing party shall supply a list of the documents for which such limitation of discovery is claimed, indicating:

- a) The claimed grounds for the redaction.
- b) The nature of the redacted material (e.g., "patient name", "trade secret", etc.).
- c) A description of the exact process used for redaction.

9. All computer media must be properly packaged to ensure safe shipping and handling. If any piece of media produced is known to have any physical defect, electronic defect, damaged data, or is infected with any virus or other harmful software of any kind, it should be clearly labeled so that appropriate care can be taken during its examination.

10. All computer media, which can be write protected should be write protected before production.

11. All copies of computer files for production will be created in such a way as to preserve the original directory structure and any information about the files that is created and maintained by the operating system and the software used to create and maintain the information. This will include, but is not limited to, dates, times, authorship, and transmittal information.

ELECTRONIC DOCUMENTS REQUEST

12. We request that you produce the following materials in your possession, custody or control:

REQUEST NO. 1: (E-mail relevant to this litigation)

13. All electronic mail, electronic correspondence, or electronic peer-to-peer messages ("e-mail") shall be produced in electronic form, in an accessible standard format, and on industry-standard computer media along with all files included as attachments to such e-mail. Back-up and archival copies of e-mail and e-mail attachments shall be restored as necessary to create a comprehensive collection of e-mail. No modifications, alterations, or additions to e-mails (or to the meta-data and attachments associated with such e-mails) from their original state shall be performed.

REQUEST NO. 2: (Data existing in electronic form)

14. All data relating to <<the matter in dispute>> that exists or is stored in electronic form including but not limited to: computerized applications used to collect, process, store, display, or report on relevant data, computer presentations (e.g. PowerPoint slides), Internet web pages, marketing information, prescription information, sales information, databases, detail or product education, sales call information, spreadsheets, statistical analysis, computer generated graphs and charts, graphics, animations, videotapes, slides, photographic images, audio tapes, voice annotation, and backup tapes or similar media relating to any of the foregoing) shall be produced in electronic form, in a mutually acceptable format on mutually acceptable computer media. Databases (and the software and manuals associated with such databases) shall be produced as used and maintained in the normal ordinary course of business (including any forms and variations thereof) and shall include without limitation the computer readable code associated with any reports, file formats, forms, queries, or structure for any databases. If proprietary software is necessary to access and view the data, a reasonable number of copies of the proprietary software and operating manuals shall be made available for use by the parties receiving the discovery during the pendency of the litigation. Where specialized syntax and/or semantics are present and encoded in the information contained in any database or file, then appropriate computer files and documentation sufficient to permit the processing and understanding of the information shall be provided.

REQUEST NO. 3: (Proprietary software used to perform redaction)

15. For any redaction software or custom application software relating to any of the DOCUMENTS, the producing party will provide a copy of the software, a description of how the software functions and how it was used, the entire source code for the software, along with any existing documentation and the exact control parameters used to control the redaction function, including but not limited to all source files, control files, library files, header files, project and make files, and source files for the routines that are called out in the header files, and which are sufficient to allow the compilation of a functioning copy of each version of each redaction product used. Where any such source code or any other computer files are maintained under a document control or revision control system, including but not limited to the Source Code Control System (SCCS), Revision Control System (RCS), Microsoft SourceSafe, or Polytron Version Control System (PVCS), then the entire source code or other computer files

are to be produced in the form managed by the document or revision control system, rather than specific versions of the files, along with DOCUMENTS sufficient to identify the individuals' initials appearing in the revision control system's historical records. Any third party source code libraries or header files are to be identified by name, purpose, vendor and version number, as is the manufacturer and version number of any and all compilers and assemblers used to translate the source code into object code.

REQUEST NO. 4: (Commercial software used to perform redaction)

16. For any commercially available redaction software relating to any of the DOCUMENTS, the producing party shall provide a description of the program and its use, which includes at least the program name, version number, vendor, and the exact parameters or settings used to control the redaction process.

REQUEST NO. 5: (Meta-data used to describe backup and archival media)

17. Computer system logs and control files used to manage and record the existence of backup and archival copies of computer files relevant to this litigation. This information may include, but is not limited to: logs and control files relating to backup software, tape management systems, vault inventories, backup policies, logs and control files relating to data archival systems, control files or policies relating to off-site storage control, system catalogs containing entries for backup files, policies and procedures relating to disaster recovery, job run schedules, operator run books, standard operating procedures (SOP) manuals, and any other records relating to data backup, restore, archival, or storage which are maintained by computer operations, data base administration, or specific business application groups.

REQUEST NO. 6: (Meta-data used to identify computer systems relevant to this litigation)

18. Files containing information about computer systems and the applications that run on them, including but not limited to files that are used to document network topology, files that identify the association of applications or database to servers or computer systems,

operator run books, SOP manuals, and guidelines to users that describe data file management policies.

REQUEST NO. 7: (Meta-data used to identify computer access relevant to this litigation)

19. Files containing information about which business groups or individuals were able to access or modify information relating to << the matter in dispute>> . This information includes but is not limited to files and documentation used to control or describe access to applications or files that contain information relating to << the matter in dispute>>, files used to control or describe access to specific computer systems, and files used to control or describe access and administration rights for data bases, computer files, and backup media.

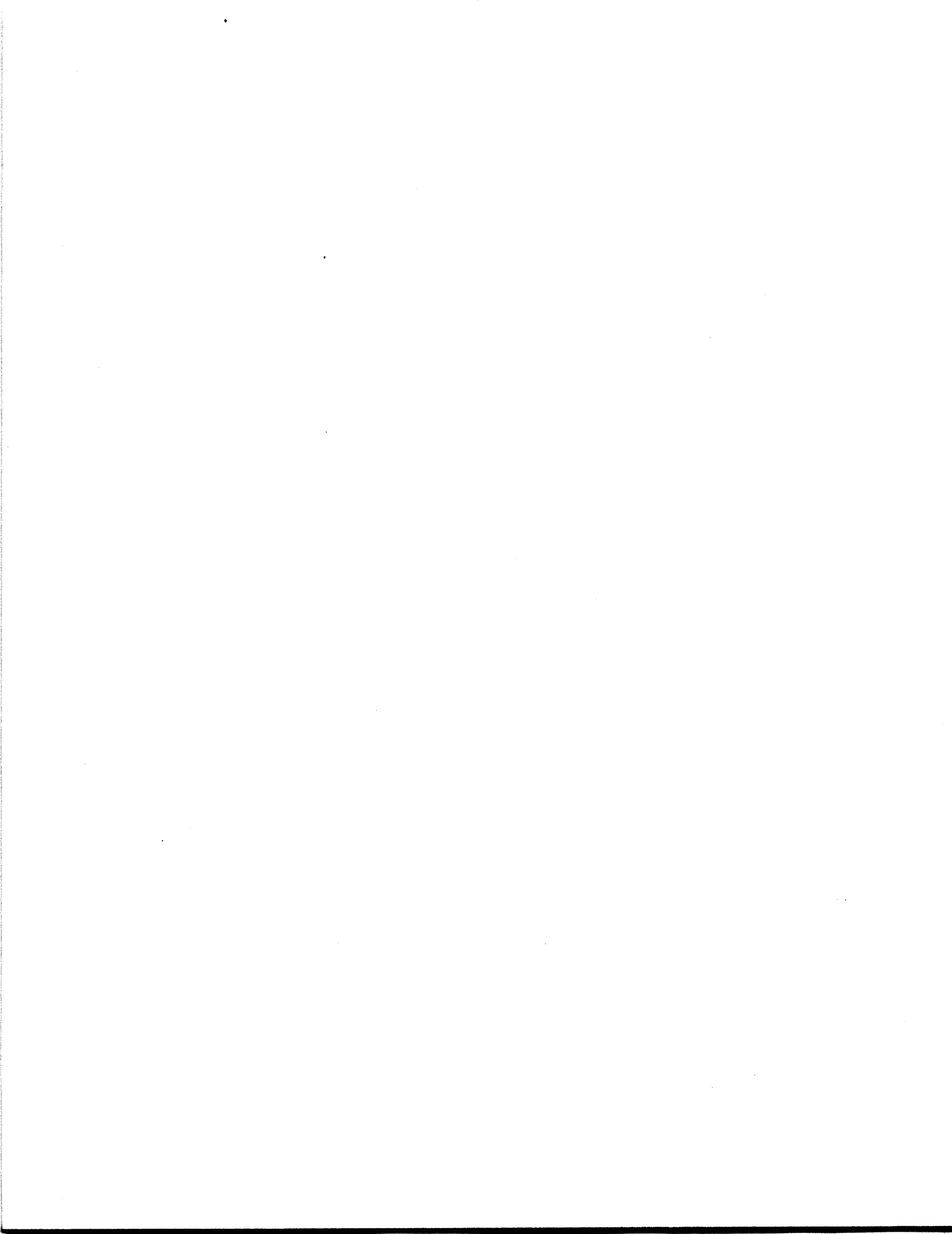
*** END ***



SOFTWARE LICENSES:

From Mass Market End User License Agreements to Mission Critical Development and Installation Agreements

*William L. Montague, Jr.
Stoll, Keenon & Park, LLP
Lexington, Kentucky*



SOFTWARE LICENSES:

From Mass Market End User License Agreements to Mission Critical Development and Installation Agreements

*William L. Montague, Jr.
Stoll, Keenon & Park, LLP
Lexington, Kentucky*

Table of Contents

| | | |
|-------------|--|------------|
| I. | Introduction..... | B-1 |
| II. | Copyright Law | B-1 |
| A. | Subject Matter of Copyright | B-2 |
| B. | Authorship and Ownership | B-3 |
| 1. | Joint Ownership | B-3 |
| 2. | Work for Hire Doctrine..... | B-3 |
| 3. | Transfer of Rights in Copyright..... | B-3 |
| C. | Notice and Registration of Copyright | B-3 |
| D. | Rights Afforded by Copyright Law | B-4 |
| 1. | Section 107: Fair Use..... | B-4 |
| 2. | Section 109: Transfers of a Particular Copy of Phonorecord | B-5 |
| 3. | Section 117: Computer Programs | B-5 |
| E. | Copyright Infringement Actions | B-5 |
| F. | Remedies for Copyright Infringement..... | B-7 |
| III. | Current Approaches to Licensing... .. | B-7 |
| A. | End User License Agreements..... | B-7 |
| 1. | Manifesting Assent | B-8 |
| 2. | Description of License | B-8 |
| 3. | Liability Limitations | B-10 |
| B. | Negotiated License Agreements | B-11 |
| 1. | Warranty Protection..... | B-12 |
| 2. | Pre-implementation Testing and Change Orders..... | B-13 |
| 3. | Confidential Information | B-14 |
| 4. | Software Maintenance, Training and Support | B-14 |

| | | |
|------------|---|-------------|
| IV. | The Effect of UCITA on Licensing..... | B-16 |
| A. | UCITA's Scope of Coverage..... | B-17 |
| B. | UCITA's Structure..... | B-19 |
| C. | Important Sections/Hot Topics | B-21 |
| 1. | Mass Market Licenses and Consumer Protection..... | B-21 |
| 2. | Electronic Self-Help..... | B-24 |
| 3. | Choice of Law | B-25 |
| 4. | Additional Resources Concerning UCITA | B-27 |
| a. | Websites | B-27 |
| b. | Articles..... | B-27 |

**SOFTWARE LICENSES: FROM MASS MARKET END USER LICENSE AGREEMENTS
TO MISSION CRITICAL DEVELOPMENT AND INSTALLATION AGREEMENTS**

By Will Montague and Richard Warne
Intellectual Property & Technology Department
STOLL, KEENON & PARK, LLP

I. INTRODUCTION.

In the current economic climate, there has been some question about whether computer information technologies will continue to play the same prominent role in business economic development as they have in the past. While capital expenditures in computer hardware and software have slowed in recent quarters, there seems to be little question in the business community as to the value that such technologies can bring to an enterprise in terms of enhanced productivity and efficiency. Of course, the cost to acquire such enabling technology remains high for many business ventures, and thus the need remains for contractual arrangements that carefully and completely implement the business goals of the software developer and purchaser alike.

The goal of these materials is to assist the legal practitioner in meeting that need by helping to identify the key issues in such agreements in a variety of contexts, and to provide some insight into different ways to approach those issues. The materials are divided into three parts: an explanation of background principles of copyright law and their effect on software licensing; a discussion of current approaches to licensing, from a simple end-user license agreement to a complex development and implementation agreement; and an analysis of UCITA and its effect on software licensing.

II. COPYRIGHT LAW.

Much of modern day transactions in information takes place in the form of copyright licenses. In the now seemingly ubiquitous software license, state law governs the license transaction from a contractual standpoint, but federal copyright law generally governs the bulk of the rights actually being licensed. A cursory understanding of copyright law therefore should be helpful in understanding software licensing.

U.S. copyright law is founded on Article I, § 8, clause 8 of the U.S. Constitution, which grants Congress the power “[t]o promote the progress of science and useful arts, by securing for limited times to authors and inventors the exclusive right to their respective writings and discoveries.” Title 17, sections 101 through 1332 of the United States Code, now controls federal copyright law.

Prior to passage of the Copyright Act of 1976, state common law of copyright protected unpublished works of authorship, while federal law protected published works. After January 1, 1978, the effective date of the Copyright Act of 1976, federal copyright law has preempted any state common law copyright protection, and established a uniform federal system for the protection of works of authorship fixated in a tangible form. Protection now

exists from the moment an original work on authorship is fixed in a tangible medium of expression (such as paper, digital media, phonorecords, *etc.*) and exists for the duration of the author's life plus a term of 70 years. *See* 17 U.S.C. §§ 102(a), 302(a).¹ Significantly, use of copyright notice (such as the copyright symbol ©) is no longer required for copyright protection, although it does afford certain advantages to the copyright holder.

A. Subject Matter of Copyrights.

Section 102 of the Copyright Act sets forth the general subject matter of copyrights:

a) Copyright protection subsists, in accordance with this title, in original works of authorship fixed in any tangible medium of expression, now known or later developed, from which they can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device. Works of authorship include the following categories:

- (1) literary works;
- (2) musical works, including any accompanying words;
- (3) dramatic works, including any accompanying music;
- (4) pantomimes and choreographic works;
- (5) pictorial, graphic, and sculptural works;
- (6) motion pictures and other audiovisual works;
- (7) sound recordings; and
- (8) architectural works.

(b) In no case does copyright protection for an original work of authorship extend to any idea, procedure, process, system, method of operation, concept, principle, or discovery, regardless of the form in which it is described, explained, illustrated, or embodied in such work.

As section 102 suggests, to be protected by copyright law, a work must be the product of some original thought process by the author and cannot be a mere copy of a preexisting work. Furthermore, it must be fixed in a manner that is sufficiently permanent. Even if an original work is fixed and falls clearly within one of the above categories, it may not be copyrightable if it is an idea, procedure, system, process, or other similar work that constitutes the only conceivable method of using or expressing an idea. Similarly, mere collections of factual information are not protected by copyright absent some element of originality in the selection, arrangement, or coordination of the facts. *See, e.g., Feist Publications v. Rural Tel. Serv. Co.*, 499 U.S. 340 (1991).

Section 103 of the Copyright Act provides protection for compilations (collections of preexisting works or uncopyrightable data) and derivative works (works derived from preexisting works) but extends that protection only to the new contributions of the author, such as the selection, coordination, and arrangement of materials in compilations.

¹ Copyright for works made for hire and anonymous or pseudonymous works endure for 95 years from publication or 120 years from creation, whichever expires first. 17 U.S.C. § 302(c).

B. Authorship and Ownership.

Although the Copyright Act grants rights to the author of a work, it is common for multiple authors to collaborate on a project. Issues can also arise when a creative work is done at the request of a third party or when the owner of a copyright transfers some or all of his rights to a third party.

1. Joint authorship. Joint authorship exists if each author intended to contribute a copyrightable expression to the unitary whole that comprises the copyrightable subject matter. *See* 17 U.S.C. §101 (defining “joint work”).

2. Work for hire doctrine. 17 U.S.C. § 201(b) of the Copyright Act provides that the employer or person for whom a work is created is considered the author of a work made for hire. To constitute a work for hire, however, the work must either be prepared by an employee within the scope of employment or fall within one of the enumerated work for hire categories and be the subject of a work for hire agreement signed by both parties. *See* 17 U.S.C. § 101 (defining “work made for hire”). The Supreme Court has held that the determination of whether the author is an “employee” for purposes of the work for hire doctrine is determined by traditional principles of agency law. *See Community for Creative Non-Violence v. Reid*, 490 U.S. 730, 742-43 (1989).

3. Transfer of rights in copyright. 17 U.S.C. § 201(d) of the Copyright Act provides that the owner of a copyright may transfer any and all rights associated with the copyright. Other than transfers by operation of law, however, any transfer of ownership of a copyright must be in a writing signed by the owner. 17 U.S.C. § 204(a).

C. Notice and Registration of Copyright

Chapter 4 of the Copyright Act governs copyright notice and registration. Under current copyright law, neither notice of copyright nor registration of the copyright with the United States Copyright Office is required for protection.² However, both confer certain advantages to the copyright holder, especially in litigation.

Copyright notice typically contains either the word “Copyright,” the abbreviation “Copr.,” or the copyright symbol ©, followed by the year of first publication and the name of the author. (Example: © 2002 John Smith.) The advantages of providing copyright notice on works are that notice informs the public that the work is protected by copyright, identifies the author

² For works published prior to March 1, 1989, copyright notice is required and is governed by the complex interplay of the Copyright Act of 1909 and the Copyright Act of 1976. Works published prior to January 1, 1978, entered the public domain if no notice was attached, and works published between January 1, 1978, and March 1, 1989, were subject to a notice requirement that could be cured if initially omitted. For any work published prior to March 1, 1989, therefore, a strong understanding of the copyright law in effect at the time of publication is necessary to determine both the existence and continuing duration of any copyright protection.

and year of first publication, and weakens the ability of a defendant in an infringement action to interpose an innocent infringer defense.

Registration is accomplished by submission of the proper form and filing fee, along with a deposit of the copyrighted work, to the Copyright Office. More detailed information is available from the Copyright Office's website, <http://lcweb.loc.gov/copyright/>. There are several advantages to registering a copyright. First, registration prior to or within five years of first publication constitutes *prima facie* evidence of the validity of a copyright. Furthermore, registration is required in order to bring suit for infringement in federal court (which has exclusive jurisdiction over copyright cases), and a copyright plaintiff may recover statutory damages and attorney fees only if registration is accomplished within three months of first publication or prior to the defendant's first act of infringement. 17 U.S.C. § 412.

Finally, it should be noted that regardless of registration, copyright owners are required to deposit copies of their work upon publication pursuant to 17 U.S.C. § 407.

D. Rights Afforded by Copyright Law.

The scope of rights granted to a copyright holder is substantial. Subject to certain enumerated limitations, a copyright holder has exclusive rights to reproduce, distribute, perform, and display the protected work. 17 U.S.C. § 106. Additionally, copyright holders have exclusive rights to prepare and distribute derivative works based upon the copyrighted material. *Id.*

Included among the statutory limitations on the copyright holder's exclusive rights are the following important sections:

§ 107 – Fair Use. Section 107 provides that the "fair use" of a copyrighted work for purposes such as criticism, comment, news reporting, teaching, and research is not an infringing act. However, the statute does not explicitly define fair use, leaving the issue to the courts to decide on a case-by-case basis. The statute states that the factors in determining fair use include:

- (1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;
- (2) the nature of the copyrighted work;
- (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
- (4) the effect of the use upon the potential market for or value of the copyrighted work.

In *Harper & Row Publishers, Inc. v. Nation Enterprises*, 471 U.S. 539, 566 (1985), the Supreme Court stated that the fourth enumerated factor, the effect of the defendant's use of the infringing work on the potential market for the copyrighted work, is the most important factor. However, the four factors are, by the plain wording of the statute, non-exclusive, and

the Court has also said that none of the factors should be viewed in isolation. *See Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 578 (1994).

Parodies of serious works of art, music, and literature often fall within the fair use exception as a useful form of social commentary. A parody will not usually be considered infringing when the effect is clearly recognized as a commentary and not a substitute for an original. *See, e.g., Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569 (1994).

Another significant form of fair use is the reverse engineering of computer software. The influential Ninth Circuit Court of Appeals, as well as other courts that have followed in its path, has held that reverse engineering (or “decompiling”) software from an executable program to human-readable source code, in which a copy of the software program is necessarily made, is permitted as fair use so long as decompilation is the only means of gaining access to the uncopyrightable aspects of the program, and the defendant has a legitimate interest in gaining access to those aspects. *Sony Computer Entertainment, Inc. v. Connectix Corp.*, 203 F.3d 596, 602 (9th Cir. 2000); *Sega Enterprises v. Accolade, Inc.*, 977 F.2d 1510, 1527-28 (9th Cir. 1992).

§ 109 – Transfers of a Particular Copy or Phonorecord. Better known as the “first sale doctrine,” this particular limitation allows the owner of a particular copy of a copyrighted work to sell or otherwise dispose of that particular copy. The copyright owner has the right to control the *initial* sale of the copy, but after that sale is completed, its present owner may transfer the copy. Notably, however, subsection (b) of 109 provides an exception for the rental of computer programs and phonorecords, which is not permissible absent the copyright owner’s authorization. Note also that the first sale doctrine does not affect the underlying copyright, which is always retained by the copyright owner. The doctrine only applies to individual copies and phonorecords embodying the copyright.

§ 117 – Computer Programs. Subject to certain conditions, section 117 allows the owner of a particular copy of a computer program to reproduce it for the following limited purposes: 1) for utilization of the program as it was intended; 2) for archival purposes; and 3) for maintenance purposes. Because the loading of a computer program into the computer’s RAM (random access memory) constitutes reproduction of the copyrighted program, *see MAI Sys. Corp. v. Peak Computer*, 991 F.2d 511, 518-19 (9th Cir. 1993), the owner or licensee’s rights to utilize a computer program are severely limited and generally determined by the license agreement under which the program was obtained.

E. Copyright Infringement Actions.

As noted above, federal courts have exclusive jurisdiction over copyright infringement suits, and a prerequisite to filing suit in federal court for infringement is that the allegedly infringed work must be registered. 17 U.S.C. § 411(a). The work need not be registered at the time of infringement, however, meaning that a potential plaintiff may seek expedited registration by the Copyright Office and then file suit.

Once jurisdiction is established, the plaintiff must prove infringement. The Sixth Circuit recently described in an unpublished opinion the burden a copyright plaintiff bears in this circuit:

To establish a claim for copyright infringement, a plaintiff must prove two elements: “(1) ownership of a valid copyright, and (2) copying of constituent elements of the work that are original.” *Feist Publ’ns., Inc. v. Rural Tel. Servs., Inc.*, 499 U.S. 340, 361, 111 S. Ct. 1282, 113 L. Ed. 2d 358 (1991). In the absence of direct evidence of duplication, “the copyright holder frequently proves copying by showing that the defendant or the person who composed the defendant’s work had access to the copyrighted material and that the defendant’s work is *substantially similar* to the protected work.” *Robert R. Jones Assocs. v. Nino Homes*, 858 F.2d 274, 276-77 (6th Cir. 1988) (emphasis added). The test for substantial similarity is sometimes called the “ordinary observer test.” See *Ellis v. Diffie*, 177 F.3d 503, 506 n.2 (6th Cir. 1999). A plaintiff bears the burden of proving the substantial similarity between protected material and the allegedly infringing work. See *Mihalek Corp v. Michigan*, 814 F.2d 290, 294 (6th Cir. 1987).

Waite v. Patch Prods., 2001 U.S. App. LEXIS 13379 (6th Cir. 2001).

In addition to direct infringement, the plaintiff may assert contributory or vicarious infringement. Those forms of infringement were recently at issue before the Ninth Circuit in *A&M Records v. Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001). There the court described contributory infringement in the following manner:

Traditionally, “one who, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another, may be held liable as a ‘contributory’ infringer.” *Gershwin Publ’g Corp. v. Columbia Artists Mgmt., Inc.*, 443 F.2d 1159, 1162 (2d Cir. 1971); see also *Fonovisa, Inc. v. Cherry Auction, Inc.*, 76 F.3d 259, 264 (9th Cir. 1996). Put differently, liability exists if the defendant engages in “personal conduct that encourages or assists the infringement.” *Matthew Bender & Co. v. West Publ’g Co.*, 158 F.3d 693, 706 (2d Cir. 1998).

Id. at 1019. The court described vicarious liability as:

an “outgrowth” of respondeat superior. In the context of copyright law, vicarious liability extends beyond an employer/employee relationship to cases in which a defendant has the right and ability to supervise the infringing activity and also has a direct financial interest in such activities.

Id. at 1022. In either case, however, “[s]econdary liability for copyright infringement does not exist in the absence of direct infringement by a third party. It follows that [a defendant] does not facilitate infringement of the copyright laws in the absence of direct infringement by [another].” *Id.* at 1013, n. 2.

F. Remedies for Copyright Infringement.

As with most intellectual property infringement actions, an injunction to halt future infringing uses is a common remedy upon a successful showing of infringement. *See* 17 U.S.C. § 502. In addition, a copyright owner may recover actual damages and any additional profits made by the infringer. 17 U.S.C. § 504. As with trademark infringement, a successful copyright plaintiff need only show the defendant's gross revenue resulting from the infringement, leaving it to the defendant to prove appropriate deductions attributable to expenses or profit that resulted from something other than the infringement. 17 U.S.C. § 504(b).

Because actual damages in copyright cases frequently prove difficult to show, and the defendant's profits are often minimal, plaintiffs commonly elect to recover statutory damages and attorney fees instead. As noted above, the infringed work must have been registered prior to the infringement for these recoveries to be available. If that is the case, however, the amounts can be substantial. For each infringed work, the plaintiff may recover up to \$35,000.00 for non-willful infringement, and up to \$150,000.00 per infringed work in the case of willful infringement. 17 U.S.C. § 504(c). Those potential recoveries, coupled with the threat of attorney fees, often prove much more successful in bringing the defendant to the bargaining table prior to trial.

Finally, a successful plaintiff may obtain destruction or other appropriate disposition of the infringing materials, as well as items by means of which additional infringing copies can be made. 17 U.S.C. § 503.

III. Current Approaches to Licensing.

In drafting the license agreement, the legal practitioner's greatest challenge is to ensure that the license meets the business needs of both the licensor and the licensee in light of the nature and context of the transaction. This requires an analysis of many factors, such as how the software is delivered to the buyer, what tasks the software performs, whether the software will be the same for all buyers or customized to meet the purchaser's needs, whether proprietary or confidential information of the buyer is needed to develop the software or will be used in its operation, whether the software will be exported out of the country, etc. Thus, a license that makes sense between a software developer selling small application software over the internet to numerous anonymous buyers will likely be wholly inappropriate for a programmer working part-time to develop software for a single company to be used in-house to manipulate confidential data or dangerous equipment. As shown below, there is a certain amount of overlap between both types of licenses.

A. End User License Agreements

Despite a software license's dependence on all of these potentially different factors, many types of provisions are found in almost all software licenses. This is because such provisions address realities intrinsic in the nature of the way such software is licensed. One of the

simplest forms of software licensing is the “End User License Agreement” (or “EULA”) typically used in commercially available software for home use. A review of these types of licenses demonstrates that they include most or all of the same kinds of provisions. This similarity is dictated by the fact that the developer is developing the software for home use or for use at a place of business, with little or no interaction with the ultimate purchaser, no customization of the software to see if the software will meet the purchaser’s particular needs, and no direct knowledge of the ways different purchasers will attempt to use the software. Given such circumstances, it is understandable that the software developer will narrowly circumscribe the rights granted to the software purchaser, and broadly limit its liability for consequences arising out of unforeseen uses of its software. The following types of provisions are found in almost all EULAs.

1. Manifesting Assent

Because in the context of commercial software most EULAs are not agreements signed by either of the parties, the first and most critical provision is to establish that the EULA is binding upon the parties. In the case of most “boxed” software purchased off the shelf, this is accomplished with a “shrink-wrap” provision, which provides that the buyer’s opening of the package will bind her to the terms of the EULA unless she returns the software within a short period unused. An example:

BY OPENING THE PACKAGE CONTAINING THE PROGRAM, YOU ARE ACCEPTING AND AGREEING TO THE TERMS OF THIS LICENSE AGREEMENT. IF YOU ARE NOT WILLING TO BE BOUND BY THE TERMS OF THIS LICENSE AGREEMENT, YOU SHOULD PROMPTLY RETURN THE PACKAGE IN UNOPENED FORM, AND YOU WILL RECEIVE A REFUND OF YOUR MONEY.

However, a number of recent court decisions have refused to hold all or certain provisions of agreements enforceable where the provision at issue is not prominently displayed to the purchaser before acceptance of the EULA is required. This is of greater concern in the context of “browse-wrap” licenses (where assent is to be inferred by an internet user’s ability to view web pages containing terms and conditions) and “shrink-wrap” licenses. In both of these instances, the buyer’s assent to the contract terms is inferred by their *opportunity* to review the terms of the contract. This is less of a concern in the context of “click-wrap” licenses, where the terms of the license are directly presented to the buyer and she is required to click a button to affirmatively manifest assent. The careful practitioner should therefore instruct the developer of this risk, and suggest that some form of affirmative assent be built into the process of installing and running the software, such as through the presentation of a dialogue box to the user during the initial installation of the software.

2. Description of License

The next type of provision found in a EULA is the “licensed not sold” provision, which states directly “The Software is licensed, not sold, to Licensee pursuant to the terms and

conditions of this Agreement.” This is designed to inform the buyer that her purchase of the software product only grants her a limited right to use the product, not to treat it as her own.

Any EULA, as with any kind of software license, will necessarily include a provision defining the scope of the license, stating that “the Seller grants you a personal non-exclusive right and license to use and execute the Program in object code form.” The provision will go on to explain that this right includes the rights to copy the Program from the media (such as a CD-ROM disc) to the computer (usually the hard drive), on a single computer (as opposed to a file server). Additionally, the provision may permit the buyer to make a backup copy of the Program: “You may make a single copy of the Software for backup and archival purposes only.” The EULA may prohibit the user from decompiling or reverse engineering the software (“User may not translate, reverse engineer, or de-compile the Software Products.”).

Finally, EULAs generally provide only “restricted rights” to government purchasers under federal guidelines. An example:

U.S. Government Restricted Rights. The Software and related documentation are provided with RESTRICTED RIGHTS. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs (c)(1) and (2) of the Commercial Computer Software - Restricted Rights at 48 C.F.R. 52.227-19, as applicable. Manufacturer for such purpose is Lighthouse Software, 555 12th Street, Lexington, Kentucky 40507.

In addition to defining what the purchaser may do with the software, a EULA may identify specific things that the purchaser may not do with the software. One such common exclusion is to prohibit the software’s use in “high risk” activities:

The Software is not fault-tolerant and is not designed, manufactured or intended for use or resale as online equipment control equipment in hazardous environments requiring fail-safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life support machines, or weapons systems, in which the failure of the Software could lead directly to death, personal injury, or severe physical or environmental damage. Developer does not authorize You to use the Software in applications where the Software’s failure to perform can reasonably be expected to result in a significant physical injury, or in loss of life. Any such use by You is entirely at Your own risk, and You agree to hold Developer harmless from any claims or losses relating to such unauthorized use.

Further, in order to comply with export restrictions promulgated by the Commerce Department, the Treasury Department, and other federal agencies, the license may provide as follows:

The Software is developed by Developer in its offices within the United States and is designed for use within the United States. Developer makes no

representation that the Software is appropriate for use in other locations, and use of the Software from territories where its contents are illegal is prohibited. Those who choose to use the Software from other locations do so on their own volition and are responsible for compliance with applicable local laws. You may not export or re-export the Software except in full compliance with all United States laws and regulations. In particular, none of the Software or underlying information or technology may be exported or re-exported into (or to a national or resident of) any country to which the U.S. embargoes goods, or to anyone on the U.S. Treasury Department's list of Specially Designated Nationals or the U.S. Commerce Department's Table of Denial Orders. In addition, You are responsible for complying with any local laws in Your jurisdiction that may impact Your right to import, export or use the Software.

3. Liability Limitations

Having informed the Buyer what she may do with the software, the EULA will go on to state, in very broad terms, that the software is provided "as is" and that the developer is not responsible for any consequences that flow from the buyer's use of the software. This is usually accomplished through three separate, but related, types of provisions. The first is a broad disclaimer of any kind of warranty, other than perhaps a warranty that the physical media on which the software is delivered is not defective. An example:

DEVELOPER PROVIDES THE SOFTWARE TO YOU "AS IS", AND DOES NOT REPRESENT THAT THE PERFORMANCE OR OPERATION OF THE SOFTWARE WILL MEET YOUR NEEDS OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, DEVELOPER DISCLAIMS ANY AND ALL WARRANTIES, DUTIES AND CONDITIONS, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTIES OR CONDITIONS OF OR RELATED TO TITLE, NON-INFRINGEMENT, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, LACK OF VIRUSES, ACCURACY OR COMPLETENESS OF RESPONSES, RESULTS, LACK OF NEGLIGENCE, AND CORRESPONDENCE TO DESCRIPTION. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE SOFTWARE AND DOCUMENTATION IS WITH YOU.

Having disclaimed almost any kind of conceivable warranty, most EULAs go on to include a provision designed to exclude any liability for most types of damage:

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL DEVELOPER BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT, PUNITIVE, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR: LOSS OF PROFITS, LOSS OF CONFIDENTIAL OR OTHER INFORMATION, BUSINESS INTERRUPTION, PERSONAL

INJURY, LOSS OF PRIVACY, FAILURE TO MEET ANY DUTY (INCLUDING OF GOOD FAITH OR OF REASONABLE CARE), NEGLIGENCE, AND ANY OTHER PECUNIARY OR OTHER LOSS WHATSOEVER) ARISING OUT OF OR IN ANY WAY RELATED TO THE USE OF OR INABILITY TO USE THE PROGRAM, OR OTHERWISE UNDER OR IN CONNECTION WITH ANY PROVISION OF THIS EULA, EVEN IF DEVELOPER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER ARISING IN CONTRACT, TORT (INCLUDING NEGLIGENCE), OR OTHERWISE.

Having provided for the exclusion of almost all types of claims and nearly all types of damages, the EULA will generally provide that any remaining types of damages are specifically limited in amount to the purchase price of the software:

NOTWITHSTANDING ANY DAMAGES THAT YOU MIGHT INCUR FOR ANY REASON WHATSOEVER (INCLUDING, WITHOUT LIMITATION, ALL DAMAGES REFERENCED ABOVE AND ALL DIRECT OR GENERAL DAMAGES), THE ENTIRE LIABILITY OF DEVELOPER AND YOUR EXCLUSIVE REMEDY FOR ALL OF THE FOREGOING UNDER ANY PROVISION OF THIS EULA SHALL BE LIMITED TO THE AMOUNT ACTUALLY PAID BY YOU FOR THE PROGRAM. THE FOREGOING LIMITATIONS, EXCLUSIONS AND DISCLAIMERS SHALL APPLY TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, EVEN IF ANY REMEDY FAILS ITS ESSENTIAL PURPOSE.

As noted above, each of these provisions is generally found in one form or another in all EULAs where the transaction is an "open market" transaction involving little or no contact between the buyer and seller and no customization by the software developer to the user's specific needs. Because such software is offered in a "one size fits all" manner at a comparatively low price to the purchaser, such license agreements appropriately impose significant limits on both the user's rights in the software and on liability for use of the software in a context unknown to the developer.

B. Negotiated License Agreements

In stark contrast to the foregoing scenario, in more complex software development and licensing transactions there is significantly more interaction between the developer and the purchaser. In such transactions, the purchaser takes a much more significant role in defining his business needs for the software so that the developer may customize the software to address specific issues and requirements of the purchaser's business. Because much greater care and responsibility is undertaken by both parties in the development process, the license agreement must accurately and fairly reflect the different role of each party. For instance, the developer can reasonably be expected to undertake greater responsibility for the proper functioning of the software upon delivery, particularly in terms of the representations and warranties undertaken in the contract. However, for its part the purchaser must also undertake some responsibility for providing accurate information to the developer. In

comparison to the “mass market” transaction described above, the developer commands a far greater price for the customized software in exchange for much greater involvement in the planning stage of the development process and greater accountability for the software’s suitability and performance. In addition, the buyer may obtain a license that is greater in scope and may offer more rights in the final work product. As before, the software license must reflect these different conditions.

Unlike a “mass market” license, where the terms of the software license are offered solely on a “take it or leave it” basis, in a more complex development transaction the terms described below are subject to prior negotiation between the parties. Accordingly, the appropriateness of each of these provisions depends entirely on the circumstances and business needs of each of the parties.

1. Warranty Protection

In the case of highly customized software, the software designer has typically worked hand-in-hand with the user of the software to develop it to the purchaser’s specifications. Thus, the purchaser has a reasonable expectation that the software will function as promised so long as it is used in accordance with the instructions:

Developer warrants that, for a period of one (1) year after installation of the Software, the Software will operate in substantial conformity to the system specifications when used in accordance with the operational parameters described in the Documentation. Developer, at its own expense, will make all adjustments and modifications necessary to cause the Software to so operate upon receipt of written notice from Purchaser within such period that the Software has failed to so operate.

In addition, the software designer may warrant that it holds proper title to the software and that its use will not violate the rights of third parties:

Developer warrants that it has the right and authority to grant Purchaser the right and license in the Software granted herein, and that Purchaser’s use of the Software in accordance with this Agreement shall not infringe the rights of any third parties under any patent, copyright, trademark, trade secret or unfair competition law in the United States.

Of course, as a matter of due diligence the purchaser of a complex and expensive software system may wish to require the software developer to provide further assurances. This might take the form of a representation in the agreement that all of the developer’s employees and subcontractors have signed appropriate assignments or work-made-for-hire agreements. The purchaser may take the further step of having the software designer provide copies of all such agreements.

2. Pre-implementation Testing and Change Orders

In some instances, a business may rely on one or more software programs to assist them on a daily basis to perform their core functions. In such instances, it is simply unacceptable for such programs to be rendered inoperable for any extended period. For example, an architectural design firm may incur unacceptable losses if its work force is idled because its design software will not function. To avoid such potential disasters, the license agreement should provide for full testing of the newly designed software before the old system is entirely supplanted:

Following installation of the Software at the Purchaser's premises, Developer shall conduct an installation test in order to confirm that the Software conforms to the Software Specifications in all material respects. Developer shall give Purchaser notice of the installation test at least seven (7) days before it is scheduled to commence, and Purchaser may permit any Purchaser personnel to observe the installation test and verify the results. Developer shall correct any defects in the Software revealed by the installation test and thereafter confirm in writing to Purchaser that such defects have been corrected. Upon satisfactory completion of the installation test, Developer shall send Purchaser a certificate indicating proper installation.

Once the software programs have been installed and appear to work properly, the purchaser will have the opportunity to see how well the software works under actual operating conditions. The purchaser may determine that one or more aspects of the functioning of the software should be modified in order to improve its function. The license agreement should anticipate this need and establish a process to facilitate such changes:

After Developer issues a certificate of proper installation, Purchaser may test the Software as installed for conformity to the Software Specifications under actual operating conditions during the ensuing thirty (30) calendar days. During this period, Purchaser may review and request in writing from Developer revisions to the Software. Upon receipt of that request, Developer shall use commercially reasonable efforts to implement those revision requests that are within the scope of, and consistent with, the Software Specifications.

If Purchaser wishes to implement any revisions to the Software that deviate in any material respect from the Software Specifications, Purchaser shall submit to Developer a written change order containing (i) the revisions in detail and (ii) a request for a price quotation for each change (collectively, the "Change Order"). Developer shall promptly evaluate the Change Order and submit to Purchaser for its written acceptance a proposal for undertaking the applicable tasks and a price quote reflecting all fees associated with Purchaser's Change Order. Purchaser shall have five (5) business days from receipt of that proposal to accept or reject Developer's proposal in writing. If Purchaser accepts Developer's proposal to undertake the work necessitated by the

Change Order, then the Change Order, as supplemented and/or modified by Developer's proposal, shall amend the Software Specifications. Developer shall proceed to implement such revisions in accordance with the Software Specifications as so modified.

3. Confidential Information

In order for the software designer to customize the software to meet the purchaser's needs, the purchaser may need to provide detailed business, financial, or customer information to the software designer. Such information is often gathered by the purchaser over time and at substantial expense. Accordingly, the purchaser may wish to keep this information secret from other businesses to keep its competitive advantage. Likewise, the software designer may need to reveal certain aspects of the software's functioning to the purchaser in order to assist in a meaningful exchange of information in the process of designing the software. The software designer may wish to protect this information as well.

To facilitate the open exchange of needed information under these circumstances, the license should provide that neither party is to disclose such information to any outside party, and may only use such information in order to fulfill their obligations under the license agreement:

Purchaser and Developer each acknowledge that Purchaser's Business Data and Developer's Software may embody proprietary trade secrets of substantial value. Purchaser and Developer shall treat all Trade Secrets identified in Exhibit E as proprietary and confidential, and neither use, copy, or disclose, nor permit any of their respective Personnel to use, copy, or disclose such Trade Secrets, except as necessary to fulfill their obligations under this Agreement.

Developer further acknowledges that any and all personal, business, financial or other data contained in customer files delivered to Developer by Purchaser to assist in the development and implementation of the Software are the exclusive property of Purchaser and shall constitute part of Purchaser's Business Data. Developer shall make no unauthorized use of such customer data owned by Purchaser. Developer shall hold in confidence all information relating to the business or affairs of Purchaser that is received by Developer in rendering services under this Agreement, except where it is authorized by Purchaser or compelled by governmental regulation or legal process. If necessary, Developer shall provide back-up records and media reasonably necessary to reconstruct current records of Purchaser.

4. Software Maintenance, Training, and Support

Many software designers develop and market software designed to assist businesses in a certain specialized field of business, such as medical billing and payment systems or flight control software for small regional airports. Such designers often develop an initial

“template” software package that they then customize to meet the needs of a particular customer. In such instances the software may be updated with some frequency, with the updates offered to purchasers through a software maintenance provision

Developer will periodically issue Maintenance Releases, containing incremental enhancements and modifications to the Software, to the Purchaser if it is current in its Maintenance Fees. Maintenance Releases may include new features other than major revisions, which are to be provided as described in paragraph 3. There will be a media and documentation fee of \$50 per release. The maintenance fee and support begin upon installation of the Software on Purchaser’s hardware system(s).

The advantage of this type of system is that it ensures the most recent version of the software to the purchaser while providing the developer with a reliable income stream and a pre-established market for updates.

Particularly where the newly designed software represents a significant departure from the purchaser’s old practices or software, one of the purchaser’s greatest costs is generally the cost to train employees to use and fully implement the new software. The experienced practitioner will bring this need to the purchaser’s attention and incorporate needed provisions into the agreement:

Once Purchaser has selected personnel who are qualified to operate the Software, Developer shall provide Purchaser’s personnel with training in the operation of the Software. Such training shall take place at the dates, times, and locations set forth in Exhibit D. Travel expenses related to the conversion, or training, shall be reimbursed by Purchaser at cost. Developer shall provide further training on mutually acceptable terms at Developer’s customary rates then in effect.

Finally, even the best training is unlikely to adequately simulate the demands and stresses placed upon the software and employees alike under real-world conditions. Accordingly, the agreement may wish to provide for additional remote support through the use of a customer support line maintained by the software designer:

Developer will provide operational assistance for Purchaser’s employees using the Software via its toll-free Support Line between 8:00 am and 6:00 p.m., Central Time, Monday through Friday, excluding scheduled holidays (New Year’s Day, Memorial Day, 4th of July, Labor Day, Thanksgiving Day, the day after Thanksgiving, Christmas Eve and Christmas Day). Support Line Services include Developer’s “Application Support Line” (assistance in proper use of the Software) at no charge. Purchaser may access Developer’s “Technical Support Line” (assistance addressing hardware or technical problems related to use of the Software) at a rate of \$2.00 per minute. Developer shall determine whether each call is technical in nature and charge Purchaser accordingly; employees of Purchaser are encouraged to inquire at

the outset of the call whether the support requested is chargeable. The Application Support Line may not be used to receive training on the use of the Software over the telephone. Separate fees apply to such training whether received during the initial implementation process or post-implementation.

The foregoing provisions are by no means exhaustive of the kinds of provisions that may be needed to adequately document the needs of the parties to such a complex transaction. For example, the parties may wish to negotiate in advance the costs for the customer to purchase significant software upgrades, provide that the purchaser is entitled to "most-favored customer status" for new software products or modules, carefully delineate the circumstances under which one or either party may terminate the development agreement and the consequences of such termination at each step of the development process, or provide the customer with rights to assistance from the developer in the event of termination before full implementation of the software or thereafter.

Not even the most well thought out license and development agreement can hope to address every possible situation that may arise between the parties. When a situation does arise that is not addressed by the agreement, the parties may be left with little more than general statements of intention in the opening habendum clauses of the contract, or worse, conflicting recollections of conversations held early in the development stage. Of course, in commercial law the Uniform Commercial Code has long provided "gap-filling" sections to address "holes" in the contract. As described below, the Uniform Computer Information Transactions Act (if it applies) can act to fill those holes, as well as perhaps provide answers to previously troubling questions in the context of software licensing, such as issues of contract formation.

IV. THE EFFECT OF UCITA ON LICENSING

UCITA is an acronym for the Uniform Computer Information Transactions Act. As the name indicates, UCITA is a uniform statutory scheme designed to govern transactions in computer information – e.g., software licenses, database licenses, and other legal components of the information age. In the absence of legislation specifically encompassing such transactions, courts historically have tended to find contracts such as software licenses to be governed by Article 2 of the Uniform Commercial Code. *See, e.g., Advent Sys. v. Unisys Corp.*, 925 F.2d 670, 675-76 (3rd Cir. 1991); *Dahlmann v. Sulcus Hospitality Techs. Inc.*, 63 F.Supp.2d 772, 775 (E.D. Mich. 1999). A central premise of UCITA is that current law, and particularly UCC Article 2, is ill suited to govern modern transactions involving computer information and that a uniform statutory scheme specifically focused on such transactions is necessary.

The current version of UCITA, which can be accessed along with the official commentary over the Internet at <http://www.law.upenn.edu/bll/ulc/ulc.htm#ucita>, is the result of over a decade of efforts by various groups to craft a set of uniform laws to govern information transactions. Originally proposed as Article 2B of the UCC, the Act took on its current name when the views of the National Conference of Commissioners on Uniform Laws (NCCUSL) and the American Law Institute (ALI) diverged. When ALI withdrew its support for the Act in the Spring of 1999 because it favored making certain changes to Article 2 of the UCC to

accommodate information transactions, NCCUSL renamed the Act to reflect its independent status from the UCC.

On July 29, 1999, NCCUSL officially adopted UCITA. Two states – Virginia and Maryland – have since passed the Act, *see* Va. Code Ann. § 59.1-501.1, *et. seq.*; Md. COMMERCIAL LAW Code Ann. § 22-101, *et. seq.*, and it is currently under consideration in other states as well (though not yet in Kentucky). Because the Act is controversial, however, its future is less than certain. Various interest groups, as well as Attorneys General from thirty-two states, have voiced objection to the Act, and at least one state (Iowa) has adopted “anti-UCITA” legislation – *i.e.* legislation that allows a contracting party to void a previously agreed upon choice of law provision that selects UCITA or a substantially similar law. *See* Iowa Code § 554D.104(4) (2002).

A. UCITA’S SCOPE OF COVERAGE

One of the most important aspects of any law – something that corporate counsel and general practitioners should know even if they know nothing else about a law – is the law’s scope of coverage. Knowing when a particular law is potentially applicable gives a lawyer the ability to spot issues and consult the specific provisions of the potentially applicable law.

UCITA’s scope of coverage is set forth in Section 103, which provides as its baseline that UCITA “applies to computer information transactions.” “Computer information transactions” is defined in Section 102 (the definitions section) as “an agreement or the performance of it to create, modify, transfer, or license computer information or informational rights in computer information The term does not include a transaction merely because the parties’ agreement provides that their communications about the transaction will be in the form of computer information.” UCITA § 102(11). The term “computer information” is, in turn, defined as “information in electronic form which is obtained from or through the use of a computer or which is in a form capable of being processed by a computer. The term includes a copy of the information and any documentation or packaging associated with the copy.” UCITA § 102(10). Thus, the initial scope of UCITA would appear to include a wide assortment of transactions involving digital information, such as software licenses, software and internet development agreements, database licenses, software assignments, digital videos and audio recordings, *etc.* *See* UCITA § 103, Official Comment 2(a) – (e). Importantly, however, UCITA section 105 specifically acknowledges the preemptive effect of federal law. For example, as noted above, section 204(a) of the Copyright Act imposes certain requirements on transfers of exclusive copyright interests, which requirements preempt any contrary provisions in UCITA. *See* 17 U.S.C. § 204(a).

Operating from the section 103(a) baseline, the remainder of section 103 provides certain specific exceptions and sets forth rules governing transactions of a mixed nature such as a sale of goods containing embedded software (an increasingly common occurrence these days):

(b) Except for subject matter excluded in subsection (d) and as otherwise provided in Section 104, if a computer information transaction includes subject matter other than computer information or subject matter excluded under subsection (d), the following rules apply:

(1) If a transaction includes computer information and goods, this [Act] applies to the part of the transaction involving computer information, informational rights in it, and creation or modification of it. However, if a copy of a computer program is contained in and sold or leased as part of goods, this [Act] applies to the copy and the computer program only if:

(A) the goods are a computer or computer peripheral; or

(B) giving the buyer or lessee of the goods access to or use of the program is ordinarily a material purpose of transactions in goods of the type sold or leased.

(2) Subject to subsection (d)(3)(A), if a transaction includes an agreement for creating, or for obtaining rights to create, computer information and a motion picture, this [Act] does not apply to the agreement if the dominant character of the agreement is to create or obtain rights to create a motion picture. In all other such agreements, this [Act] does not apply to the part of the agreement that involves a motion picture excluded under subsection (d)(3), but does apply to the computer information.

(3) In all other cases, this [Act] applies to the entire transaction if the computer information and informational rights, or access to them, is the primary subject matter, but otherwise applies only to the part of the transaction involving computer information, informational rights in it, and creation or modification of it.

(c) To the extent of a conflict between this [Act] and [Article 9 of the Uniform Commercial Code], [Article 9] governs.

(d) This [Act] does not apply to:

(1) a financial services transaction;

(2) an insurance services transaction;

(3) an agreement to create, perform or perform in, include information in, acquire, use, distribute, modify, reproduce, have access to, adapt, make available, transmit, license, or display:

(A) a motion picture or audio or visual programming, other than in (i) a mass-market transaction or (ii) a submission of an idea or information or release of

informational rights that may result in making a motion picture or similar information product; or

(B) a sound recording, musical work, or phonorecord as defined or used in Title 17 of the United States Code as of July 1, 1999, or an enhanced sound recording, other than in the submission of an idea or information or release of informational rights that may result in the creation of such material or a similar information product.

(4) a compulsory license;

(5) a contract of employment of an individual, other than an individual hired as an independent contractor to create or modify computer information, unless the independent contractor is a freelancer in the news reporting industry as that term is commonly understood in that industry;

(6) a contract that does not require that information be furnished as computer information or a contract in which, under the agreement, the form of the information as computer information is otherwise insignificant with respect to the primary subject matter of the part of the transaction pertaining to the information;

(7) unless otherwise agreed between the parties in a record:

(A) telecommunications products or services provided pursuant to federal or state tariffs; or

(B) telecommunications products or services provided pursuant to agreements required or permitted to be filed by the service provider with a federal or state authority regulating those services or under pricing subject to approval by a federal or state regulatory authority; or

(8) subject matter within the scope of [Article 3, 4, 4A, 5, [6,] 7, or 8 of the Uniform Commercial Code].

....

UCITA § 103(b) – (d).

B. UCITA'S STRUCTURE

Probably the second most important aspect of UCITA for a general practitioner to know is the overall structure of the Act. If one knows the general scope and structure of a particular set of law, he or she is in a very good position not only to spot potential issues but also to quickly find the answers to those issues. Because UCITA began its drafting life as a proposed Article 2B of the Uniform Commercial Code, the structure of the Act is quite similar to that

of UCC Article 2, something that should provide a level of comfort to those otherwise unfamiliar with the Act.

Part 1 of UCITA sets forth the Act's General Provisions, including a lengthy set of defined terms (section 102), provisions regarding the Act's scope and applicability (sections 103 through 105), provisions regarding contract construction, enforceability, and authenticity (sections 106 – 108, 111, 113, 114), and provisions regarding choice of law and choice of forum (sections 109 and 110).

Part 2 addresses the formation and terms of a contract, including traditional contract issues such as the formal requirements of a contract (section 201), offer and acceptance (section 203), acceptance with varying terms (section 204), conditional offer and acceptance (section 205), and the impact of things like trade usage and course of dealing (section 210). In addition, however, Part 2 sets forth specific provisions governing circumstances that have arisen only recently with the growing prominence of information technology, such as offer and acceptance by electronic agents or "bots" (section 106), mass market licenses (section 209), and the effect of electronic error in an automated transaction (section 214).

Part 3 contains specific provisions governing contract construction and interpretation issues, such as parol and extrinsic evidence (section 301) and modification and rescission (section 303).

Part 4 addresses warranties. The kinds of warranties include traditional ones well known to most lawyers, such as express warranties (section 402), implied warranties of merchantability (section 403), and disclaimed warranties (section 406). In addition, however, the Act also addresses other, more modern forms of warranties such as warranties of noninfringement (section 401), warranties regarding informational content (section 404), and warranties concerning system integration (section 405).

Part 5 deals with the transfer of interests and rights in computer information. Subpart A addresses transfers of ownership, such as ownership of informational rights such as copyright interests (section 501) and ownership of particular copies (section 502). It also addresses transfer of contractual interests and, particularly, sublicensing (sections 503 through 506). Subpart B of Part 5 deals with various transfers as part of financing arrangements, including those where the financier does and does not become a licensee of the computer information being transferred (sections 507 and 508).

Part 6 concerns the performance of contracts and other transactions involving computer information. There are several sections that address general aspects of performance (sections 601 through 605) and several that address performance by the delivery of particular copies of computer information (sections 606 through 610). In addition, Part 6 deals with certain specific types of contracts such as access contracts (section 611), software support and maintenance contracts (section 612), and contracts concerning the distribution of computer information (mainly software) from publishers through dealers to the ultimate end-users (section 613). Finally, Part 6 deals with traditional performance issues such as risk of loss (section 614), impossibility (section 615), and termination (sections 616 through 618).

Part 7 deals with situations involving breach of contract. These include traditional issues such as material breach (section 701), waiver (section 702), the right to cure (section 703), the providing of assurances of performance (section 708), and repudiation of performance (sections 709 and 710). In addition, Part 7 addresses breach by the providing of defective copies of the computer information – e.g. software with significant “bugs” or other errors in it (sections 704 through 707).

Part 8 addresses remedies. Again, the Act addresses both traditional remedy issues such as the right to cancel (section 802), liquidation of damages (section 804), the limitations period for bringing suit (section 805), measure of damages (sections 807 through 809), recoupment (810), and specific performance (section 811), as well as issues more attuned to modern computer information transactions.

Part 9 is the final part of the Act, and, as with UCC Article 2 and others, provides an assortment “miscellaneous provisions” concerning matters such as severability of the Act’s various provisions (section 901) and the Act’s effective date and its effect on transactions occurring prior to the effective date (sections 902 and 904).

C. IMPORTANT SECTIONS / HOT TOPICS

Even the most superficial survey of all the provisions of UCITA would be a lengthy undertaking well beyond the scope of these materials. This section will therefore focus on several of the more significant or controversial aspects of the Act. Those wishing to access more in-depth treatment of the various sections of UCITA may consult the sources mentioned at the end of these materials, all of which provide excellent and detailed discussions of various issues.

1. Mass Market Licenses and Consumer Protection

One of the most difficult issues dividing the proponents and opponents of UCITA is the question of how to treat consumers, especially in light of the ubiquitous nature of mass market software licenses in today’s world. UCITA’s current version expressly provides that the various consumer protection laws already in existence control to the extent of any conflict with UCITA. *See* UCITA § 105(c). The Act also provides different rules applicable to “mass-market licenses” and “mass-market transactions.” *See, e.g.*, UCITA §§ 105(44) – (45),

209, 304(b)(2), 503(4). “Mass-market licenses” and “mass-market transactions” are defined in section 102 in the following manner:

(44) “Mass-market license” means a standard form used in a mass-market transaction.

(45) “Mass-market transaction” means a transaction that is:

(A) a consumer contract; or

(B) any other transaction with an end-user licensee if:

(i) the transaction is for information or informational rights directed to the general public as a whole, including consumers, under substantially the same terms for the same information;

(ii) the licensee acquires the information or informational rights in a retail transaction under terms and in a quantity consistent with an ordinary transaction in a retail market; and

(iii) the transaction is not:

(I) a contract for redistribution or for public performance or public display of a copyrighted work;

(II) a transaction in which the information is customized or otherwise specially prepared by the licensor for the licensee, other than minor customization using a capability of the information intended for that purpose;

(III) a site license; or

(IV) an access contract.

UCITA § 102 (44) – (45). If an agreement constitutes a mass-market license, for instance, there are special rules regarding the enforceability of terms and the opportunity for review and assent that are designed to protect consumers. UCITA § 209. Similarly, provisions in mass-market licenses that prohibit the transfer of contractual interests must be conspicuous, a provision again designed to protect the consumer. UCITA § 503(4).

Notwithstanding these special rules, opponents of UCITA believe that the Act does not go nearly far enough to protect consumers and instead places consumers at the mercy of software vendors in many respects. UCITA opponent Cem Kaner’s recent comments reflect that sentiment:

UCITA defines the typical consumer software transaction as an intangible license, the purchase of a right to use the software, rather than the sale of a copy of the software. So, when you buy a copy of Microsoft Word and a book on how to use Microsoft Word at your local computer store, you buy two things that contain copyrighted intellectual property. The sale of the book is a sale of goods under UCITA but under UCITA, the sale of the software is not. If you download that same book from Barnes & Noble, instead of buying the paper copy at Barnes & Noble, the book is treated like software under UCITA.

By defining consumer purchases of software as licenses, rather than sales, UCITA pulls consumer software out of the scope of all of the consumer protection statutes that protect buyers of "consumer goods." All of the consumer warranty laws, for example, are "consumer goods" laws.

Comments of Cem Kaner in Educational CyberPlayground, dated December 21, 2001, (viewed April 4, 2002, at <http://www.edu-cyberpg.com/Technology/securityUCITA.html>).

Similarly, the Attorneys General of thirty-two states recently opined in a letter to NCCUSL:

Since UCITA would identify the transactions it covers as "licenses" of "information" rather than "sales of goods," it would remove a vast range of transactions from laws that specifically apply to the sale of goods. In addition to the UCC, UCITA could effect an end-run around such federal statutes as the Robinson-Patman Act (prohibiting price discrimination), which arguably does not apply to mere "licensing agreements," and the Magnuson-Moss Act (setting standards for consumer warranties), which applies to any "buyer ... of any consumer product."

Likewise, arguments are sure to be made that state consumer protection laws do not extend to "licenses" of "information." Thus, by designating a wide range of consumer transactions as the licensing of "information," rather than the purchase of "goods," UCITA could provide the basis for sellers to argue that state consumer protection laws are inapplicable in the first instance. While we believe any such argument should ultimately fail, it will still generate litigation, create uncertainty and increase the likelihood that consumers will not receive all the protections of existing consumer law in transactions that are subject to UCITA.

Letter from Attorneys General to Carlyle C. Ring, dated Nov. 13, 2001 (viewed April 4, 2002, at [http://www.4cite.org/pdf/Nov132001 Letter from AGs to Carlyle Ring.pdf](http://www.4cite.org/pdf/Nov132001%20Letter%20from%20AGs%20to%20Carlyle%20Ring.pdf)).

NCCUSL has responded to criticisms such as these by noting that, to the extent state consumer protection laws apply only to consumer *goods*, those laws should be updated in any event to reflect the modern-day prevalence of computer software licensing:

What is dealt with here is the relationship between UCITA and prior consumer protection law in a state. *Subsequent* consumer protection laws will, of course, contain their own scope and preemptive terms.

....

The legislative note in UCITA alerts legislatures of the need to examine state consumer protection statutes applicable to goods to determine whether they ought to be amended to apply to computer information. Both Virginia and Maryland engaged in close analysis of their own consumer protection rules, amending those laws to cover information transactions when appropriate. This type of examination is needed for appropriate results since some consumer law requirements would make no sense if applied to information transactions (e.g., a consumer statute requiring a label to appear on outside packaging for goods cannot automatically be applied to downloaded software or to the right to access a database; there is no “outside” in either case).

Agenda of UCITA Standby Committee for Nov. 16-18, 2001, meeting at p. 21 (viewed on April 4, 2002, at http://www.nccusl.org/nccusl/meetings/UCITA_Materials/Agenda-nov-01.pdf).

2. Electronic Self-Help

Another highly contentious issue, albeit one that may be largely resolved now, has been the availability under UCITA for parties under certain circumstances to agree to allow a software provider to exercise “electronic self-help” in the event of a dispute. “Electronic self-help occurs when licensed software contains a mechanism that allows the provider to remotely disable or “shut down” the software. Many opponents of UCITA have raised the specter of software vendors disabling mission-critical software whenever disputes arose with the software user. For example, the AFFECT coalition’s website has stated:

UCITA would allow software to be disabled without notification.

- UCITA allows software publishers to shut down mission critical software *remotely* without court approval and without incurring liability for the foreseeable harm caused.
- UCITA allows software publishers to modify the terms of contracts after the sale simply by sending an e-mail -- regardless of whether the consumer receives the notification or not.
- UCITA allows software publishers to remove their product, simply because usage fees arrive late.
- UCITA puts consumers at the mercy of software publishers to “blackmail” users for more fees by their unhindered ability to disable or remove their product for unspecified “license violations.”

Why We Oppose UCITA (viewed on April 4, 2002, at <http://www.4cite.org/why.html>).

The issue may be largely resolved now, however, because Section 816, which permitted electronic self-help in limited circumstances, was recently amended along with all other references to electronic self-help in the Act to provide that electronic self-help is banned. Nevertheless, initial reactions from UCITA's opponents to the proposed amendment were luke-warm, suggesting that software vendors will find alternative means of accomplishing the same ends. AFFECT's website stated:

At first glance, the recommended amendments to electronic self-help also appear to provide some degree of relief. "Electronic self-help" in UCITA means the remote disabling of a licensee's use of software or computer information. Controversy about this issue has persistently plagued UCITA. Although the proposed amendment is an improvement over existing language, the complexity of the model statute makes it uncertain that the equivalent of electronic self-help would not be permitted through other sections of the law. Further, the proposed amendment does not prohibit a licensor from relying on a contractual exclusion or limitation of damages to limit its liability for an improper exercise of electronic self-help. As a result, a licensor could ignore UCITA's prohibition of electronic self-help with little fear of the consequences.

AFFECT Statement on Proposed New Amendments to UCITA (viewed on April 4, 2002, at <http://www.4cite.org/why.html>). Similarly, Cem Kaner opined:

Electronic self-help is banned, but a vendor retains extensive power to protect its rights under UCITA. For example, the software can come with a built-in automatic termination, stopping performance after a specified number of days or uses. In the event of a dispute, the vendor can simply refuse to renew the license. The vendor can also get an injunction.

Comments of Cem Kaner in Educational CyberPlayground, dated December 21, 2001, (viewed April 4, 2002, at <http://www.edu-cyberpg.com/Technology/securityUCITA.html>).

3. Choice of Law

A final issue that has provoked opposition to UCITA, and that is important to attorneys practicing in states that have not yet adopted UCITA, is that of choice of law. Section 109 of the Act provides:

(a) The parties in their agreement may choose the applicable law. However, the choice is not enforceable in a consumer contract to the extent it would vary a rule that may not be varied by agreement under the law of the jurisdiction whose law would apply under subsections (b) and (c) in the absence of the agreement.

(b) In the absence of an enforceable agreement on choice of law, the following rules determine which jurisdiction's law governs in all respects for purposes of contract law:

(1) An access contract or a contract providing for electronic delivery of a copy is governed by the law of the jurisdiction in which the licensor was located when the agreement was entered into.

(2) A consumer contract that requires delivery of a copy on a tangible medium is governed by the law of the jurisdiction in which the copy is or should have been delivered to the consumer.

(3) In all other cases, the contract is governed by the law of the jurisdiction having the most significant relationship to the transaction.

(c) In cases governed by subsection (b), if the jurisdiction whose law governs is outside the United States, the law of that jurisdiction governs only if it provides substantially similar protections and rights to a party not located in that jurisdiction as are provided under this [Act]. Otherwise, the law of the State that has the most significant relationship to the transaction governs.

(d) For purposes of this section, a party is located at its place of business if it has one place of business, at its chief executive office if it has more than one place of business, or at its place of incorporation or primary registration if it does not have a physical place of business. Otherwise, a party is located at its primary residence.

UCITA § 109. Critics of UCITA complain that this provision gives software vendors the ability to thrust unfavorable laws on their licensees in non-negotiable mass-market agreements. However, as NCCUSL's Standby Committee noted prior to its November meeting, existing law generally supports choice of law provisions in contracts:

Common law generally enforces contractual choices of law unless they are unconscionable or violate fundamental public policy of a state. *See Medtronic Inc. v. Janss*, 729 F.2d 1395 (11th Cir. 1984); *Northeast Data Sys., Inc. v. McDonnell Douglas Computer Sys. Co.*, 986 F.2d 607 (1st Cir. 1993). *Compare Application Group, Inc. v. Hunter Group, Inc.*, 61 Cal. App.4th 881, 72 Cal. Rptr.2d 73 (Cal. App. 1998) (California fundamental policy invalidates choice of law that would be enforceable under Maryland law, where the contract was made). The *Restatement (Second) of Conflicts of Law* 188 provides:

(1) The law of the state chosen by the parties to govern their contractual rights and duties will be applied if the particular issue is one which the parties could have resolved by an explicit provision in their agreement directed to that issue.

(2) The law of the state chosen by the parties ... will be applied, even if the particular issue is one which the parties could not have resolved by an explicit provision in their agreement directed to that issue, unless either

(a) the chosen state has no substantial relationship to the parties or the transaction and there is no other reasonable basis for the parties' choice, or

(b) application of the law of the chosen state would be contrary to a fundamental policy of a state which has a materially greater interest than the chosen state in the determination of the particular issue and which, under the rule of § 188, would be the state of the applicable law in the absence of an effective choice of law by the parties.

Agenda of UCITA Standby Committee for Nov. 16-18, 2001, meeting at p. 32 (viewed on April 4, 2002, at http://www.nccusl.org/nccusl/meetings/UCITA_Materials/Agenda-nov-01.pdf).

The current state of the law is significant for two reasons. First, UCITA's critics are focusing on an aspect of UCITA that makes no change to existing law and instead is patterned after the rule set forth in the Restatement (Second) of Conflicts of Laws. Second, and more importantly for attorneys drafting licenses outside jurisdictions that have adopted UCITA, non-UCITA law would appear to enforce contractual provisions that choose either (1) the law of a state that has adopted UCITA if a reasonable basis can be shown for choosing that state's law or (2) UCITA itself. Since it may be difficult to show a reasonable basis for the choice of Maryland or Virginia law in many licensing situations, it may be more feasible at this point for the parties to choose to apply UCITA to their transaction to the extent of UCITA's scope of coverage and to apply the law of a particular state (regardless of whether that state has adopted UCITA) to any issues outside the scope of UCITA. Given the ill-suited nature of UCC Article 2 and common law to software licenses and other computer information transactions, it would seem quite reasonable for the parties to such a transaction to choose UCITA. Under existing law, therefore, that choice is likely to be enforced.

4. ADDITIONAL RESOURCES CONCERNING UCITA

Websites:

UCITA Online - <http://www.ucitaonline.com>

AFFECT Coalition website - <http://affect.ucita.com/>

Cem Kaner's website - <http://www.badsoftware.com/uccindex.htm>

Articles:

Cem Kaner, *Software Engineering and UCITA*, 18 J. MARSHALL J. COMPUTER & INFO. L. 435 (1999).

Cem Kaner, *Why You Should Oppose UCITA*, 17 COMPUTER LAWYER No. 5, 20 (May 2000) (available at <http://www.badsoftware.com/claw2000.htm>).

Carlyle C. Ring, Jr., *Uniform Rules for Internet Information Transactions: An Overview of Proposed UCITA*, 38 DUQUESNE L. REV. 319 (2000).


Holly K. Towle, *Mass Market Transactions in the Uniform Computer Information Transactions Act*, 38 DUQUESNE L. REV. 371 (2000).

Brian D. McDonald, *The Uniform Computer Information Transactions Act*, 16 BERKELEY TECH. L.J. 461 (2001).

Matthew J. Smith, *An Overview of the Uniform Computer Information Transactions Act: Warranties, Self-Help, and Contract Formation Why UCITA Should Be Renamed "The Licensors' Protection Act,"* 25 S. ILL. U. L. J. 389 (2001).

Software Licenses

Will Montague
 Chair, Intellectual Property &
 Technology Department
Stoll, Keenon & Park, LLP
 300 West Vine Street, Suite 2100
 Lexington KY 40507
 859.231.3946
wlm2@skp.com



www.skp.com


1

Legal Protection for Software

Primary sources of protection:

- > Copyright Law
- > Trade Secret Law
- > Contract Law

- > Patent Law (not discussed)
- > Trademark Law (not discussed)




www.skp.com

2

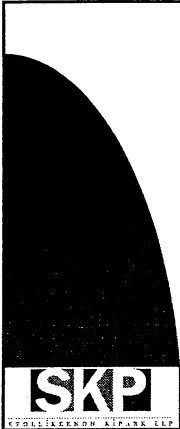
Copyright: What's Protected?

- > Governed exclusively by federal law.
- > Copyright exists "in original works of authorship fixed in a tangible medium of expression, now known or later developed, from which they can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device."
- > Copyright comes into being as soon as a work is fixed in a tangible medium (e.g. paper, digital medium, photograph).
- > Use of a copyright notice (©) is **not** required for works first published after March 1, 1989.



www.skp.com

3



Copyright: Examples

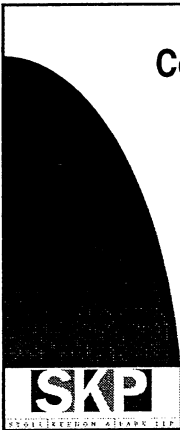
Protected:

- ✓ Writings
- ✓ Photographs
- ✓ Musical works
- ✓ Software
- ✓ Selection and Arrangement in Databases

Not Protected:

- ✓ Ideas or Concepts
- ✓ Raw Facts or Data
- ✓ Methods of Operation

www.skp.com 4



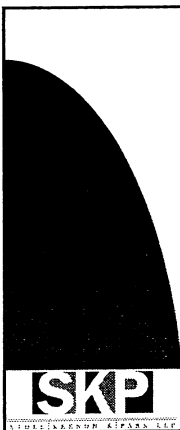
Copyright: Who Owns It?

Fundamental principle:
The author of a “work” owns the copyright but can assign the right or license it to others.

“Work for Hire” exceptions:

- 1) Employer owns copyright to work created by employee (employee status determined by traditional agency principles).
- 2) Hiring party owns copyright to a work created by an independent contractor **if** both parties have signed a work for hire agreement **and** the work fits into one of nine statutorily defined categories of works.
 - Some software may fit in “collective work” or “compilation” categories

www.skp.com 5




Copyright: What rights?

Copyright owner has the exclusive right to:

- Reproduce the work
- Prepare derivative works
- Distribute copies of the work
- Publically perform or display the work


www.skp.com 6



Copyright Infringement: What Not To Do

- > Anyone who does something without permission (*i.e.* a license) that the copyright owner has the exclusive right to do is potentially liable for infringement.
- > Sections 107 through 122 provide certain specific limitations to a copyright holder's exclusive rights.
 - > Most are very specific results of particular interest groups' lobbying efforts


www.skp.com 7



Limitations on Exclusive Rights: Fair Use

- > Fair Use is a defense to infringement but is **very** case-specific and is one of the most misunderstood areas of copyright law.
- > Fair Use factors (17 U.S.C. § 107):
 - (1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;
 - (2) the nature of the copyrighted work;
 - (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
 - (4) the effect of the use upon the potential market for or value of the copyrighted work.

www.skp.com 8



Limitations on Exclusive Rights: Computer Programs

- > Copy of program created in computer's RAM is copy for purposes of Copyright Act
- > Limitations:
 - > 17 U.S.C. §117
 - > Not an infringement for "owner" of copy of software to make a copy if copy is:
 - an essential step in utilization of software;
 - for archival purposes only (*i.e.* a back-up copy); or
 - made solely by virtue of activating the computer in order to provide maintain or repair the computer
 - > Fair Use
 - > Reverse engineering to ascertain noncopyrightable aspects of program

www.skp.com 9

Copyright: Remedies

Important Note: Federal Courts have exclusive jurisdiction over copyright disputes, and the plaintiff must have a registered copyright before he or she may sue.

The owner of an infringed copyright potentially can recover:

- > **Injunctive relief** and seizure/forfeiture of infringing materials
- > **Money damages** – either actual damages or statutory damages (up to \$150,000 per infringed work)
- > **Attorney's Fees** – recovery of the copyright owner's attorney's fees and costs in bringing suit

BUT, statutory damages and attorney's fees are recoverable only if the infringed work was registered with the United States Copyright Office before the infringement began.



www.skp.com

10

Copyright: Criminal and Corporate Liability

The Copyright Act also imposes criminal liability for infringement, and may impose corporate liability by employees:

- > Criminal liability can be imposed, even if the user does not make money from the infringement, with a fine of up to \$250,000, a jail term of up to five years, or both.
- > Vicarious liability can be imposed on a corporation, even absent any knowledge of copyright infringement, if corporation has the right and ability to supervise the conduct of the infringing employee and has a direct financial interest in the infringing activity.



www.skp.com

11

Copyright: Software (and the Internet)

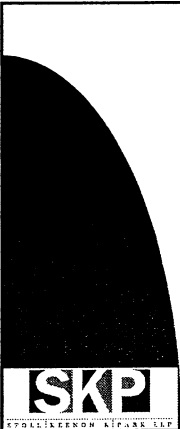
Computer software has pushed copyright law to the edge repeatedly over the last several decades.

The functional nature of software makes it quite different from many other forms of copyrighted works.



www.skp.com

12



Copyright: Software (and the Internet)

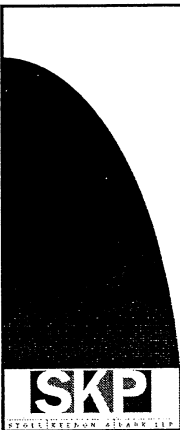
What aspects of software are potentially protected by copyright?

- > Object code
- > Source code
- > Structure and organization of the program (i.e. "non-literal aspects" of the program)

What aspects are not protected?

- > Purpose and idea of program
- > Methods of operation

www.skp.com 13

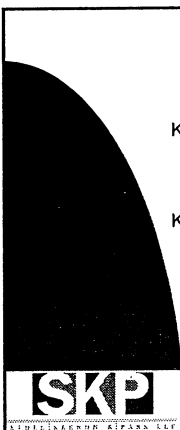


Trade Secrets: What Are They?

In very general terms, a trade secret is any information that has value by virtue of being secret.

However, trade secrets are governed by state law, and the precise definition of a trade secret can vary from state to state. What constitutes a trade secret in one state may not necessarily be one in another state.

www.skp.com 14



Trade Secrets: What Are They?

Kentucky and most other states have adopted the Uniform Trade Secrets Act. (KRS 365.800 - .900)

KRS 365.880(4) defines a trade secret as:
information, including a formula, pattern, compilation, program, data, device, method, technique, or process, that:

- (a) Derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and
- (b) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

www.skp.com 15

Trade Secrets: Examples

The following are all examples of potential trade secrets if maintained in secrecy:

- > source code and object code
- > database information
- > customer lists
- > research & development results
- > techniques and methods of doing things
- > production processes
- > product design tolerances and specifications
- > know-how (and negative know-how)
- > fried chicken recipes

SKP
www.skp.com

What is a "license" (compared to other agreements)?


- > Simple definition -- permission to do something for which licensee otherwise could be sued.
 - > Usually accompanied by numerous other agreements in form of "license agreement" (e.g. compensation, warranties, dispute resolution, etc.)
- > "Assignment" is transfer of ownership.
 - > Exclusive license may be tantamount to assignment.
- > "Covenant-not-to-sue" is personal agreement by rights holder not to sue.
 - > Does not run with right.

SKP
www.skp.com

License Grant

- > Licensed rights?
 - > intellectual property rights licensed
 - > program(s) licensed
 - > documentation
 - > rights to source code?
- > Licensee?
 - > single person
 - > limited "seats"
 - > company-wide
 - > subsidiaries, related companies, etc.
- > Exclusive or non-exclusive?
- > Geographic scope?
- > Limited field of use?
- > Term of license? Renewal terms?

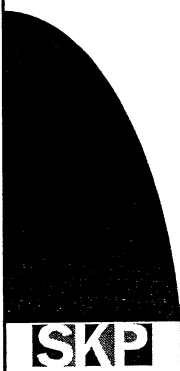
SKP
www.skp.com



Compensation

- Up-front, lump sum payment
- Continuing royalties
 - basis for calculation?
 - royalty rate?
 - minimum royalty?
- Mixture of up-front and continuing
- Revenue recognition issues
- Most-favored licensee

www.skp.com 19

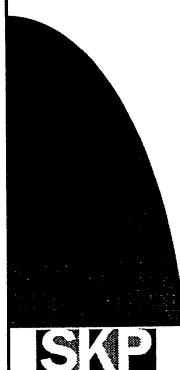


Mass Market Licenses

Typical provisions in End User License Agreements (EULA):

- Software is “licensed” not “sold”
- Nonexclusive right to use 1 copy of program on 1 computer (not on network)
- May make 1 copy for backup purposes

www.skp.com 20




Mass Market Licenses

Typical EULA provisions (cont'd)

- All warranties typically disclaimed, including merchantability and fitness for a particular purpose
- Licensor's liability limited to cost of license; no liability for consequential damages (lost profits, business interruption), punitive damages, etc
- No reverse-engineering
- Dispute resolution procedures, governing law, and forum selection
- Export restrictions due to federal law

www.skp.com 21




Customized software - IP Warranties

Licensor warrants title to program and associated intellectual property rights

- > Licensor has right to grant license
- > Software will not infringe any third party intellectual property (sometimes with "best of knowledge" qualification)
- > Indemnification for intellectual property infringement claims by third parties
- > Rights (through sublicense or otherwise) to third party content

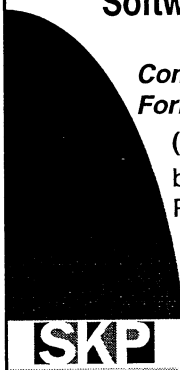
www.skp.com 22



Customized software - other provisions

- > Confidentiality of licensee's trade secrets and business information
- > Pre-implementation testing of mission-critical software; error-correction schedule
- > Source code escrow and disaster recovery
- > Licensee's right to major software updates
- > Software maintenance, phone support, employee training
- > Conditions for termination, transition assistance


www.skp.com 23



Software Licensing Resource

Computer Software Agreements: Forms and Commentary
(West Group, 3rd ed. 2002)
by Peter Quittmeyer, Clarence Ridley, John Matuszeski


www.skp.com 24



Antitrust / Unfair Competition Laws

- > *****DOESN'T JUST APPLY TO MONOPOLIES*****
- > **Complex interplay between intellectual property and antitrust laws**
- > **Antitrust Guidelines for the Licensing of Intellectual Property**
 - > Issued by Department of Justice and Federal Trade Commission in 1995
 - > available at:
<http://www.usdoj.gov/atr/public/guidelines/fgguide.htm>
- > **Pendulum is swinging back to more careful scrutiny of intellectual property deals for anti-competitive effects**


www.skp.com 25



UCITA

- > Uniform Computer Information Transactions Act
 - > uniform state law
 - > would cover software licenses and other computer information transactions
 - > formerly UCC Article 2-B
- > Withdrawn by the American Law Institute (ALI) in Spring 1999
- > Adopted by the National Conference of Commissioners on Uniform Laws (NCCUSL) in July 1999
- > Passed in Virginia and Maryland ("UCITA Lite")
- > "Bomb shelter" legislation in Iowa


www.skp.com 26



UCITA's Scope

- > applies to "computer information transactions" (Section 103)
- > "computer information transaction" = "an agreement ...to create, modify, transfer, or license computer information or informational rights in compute information" (Section 102)
- > "computer information" = "information in electronic form which is obtained from or through the use of a computer or which is in a form capable of being processed by a computer[,] ... include[ing] a copy of the information and any documentation or packaging associated with the copy." (Section 102)


www.skp.com 27



UCITA's Scope - Examples

- > Software licenses and assignments
- > Software development agreements
- > Database licenses or access agreements
- > Website development agreements
- > Agreements concerning digital video and audio recordings
- > **BUT**, requirements of federal copyright law may preempt!

www.skp.com 28




UCITA's Scope - Exclusions

Examples:

- > Mixed transactions of goods and computer information (e.g. microwave with embedded software)
- > Subject matter governed by UCC
- > Financial and insurance services transactions
 - due to regulatory control
- > Certain motion picture or audio/video programming transactions
- > Compulsory licenses under the Copyright Act (music)
- > Employment contracts
- > Transactions in which information is furnished in computer form but does not have to be

www.skp.com 29




UCITA's Structure

Very similar to UCC Articles

- > Part 1 – General Provisions
- > Part 2 – Formation & Terms of Contract
- > Part 3 – Contract Construction
- > Part 4 – Warranties
- > Part 5 – Transfer of Interests and Rights
- > Part 6 – Performance of Contract
- > Part 7 – Breach of Contract
- > Part 8 – Remedies
- > Part 9 – Miscellaneous Provisions


www.skp.com 30



Unenforceable terms

- > Sections 105(b) and 111 permit a court to refuse to enforce a contract or specific terms within a contract that either:
 - (a) violate "fundamental public policy" (§105(b); or
 - (b) were "unconscionable" at the time the contract was made (§ 111).
- > Sections will be most applicable to mass market, non-negotiated contracts.
- > Section 105(b) has been characterized as a "heightened unconscionability standard."
- > public policies likely to be those relating to innovation, competition, and fair comment
www.skp.com


31



Electronic Signatures and Manifestation of Assent

- > Section 108 gives legal effect to electronic signatures
 - > Electronic signatures already recognized now by UETA and E-Sign legislation
- > Also binds party to assent made by electronic agents ("bots")
- > Other sections guarantee that assent is valid only if done intentionally and with at least an opportunity to review terms.
www.skp.com


32



Choice of Law and Forum Selection Clauses

- > Section 109 validates parties' choice of law provisions and provides rules where no choice of law is made:
 - > Law of state where information provider is located if information provided electronically.
 - > Law of state where information recipient is located if recipient is consumer and information to be provided on tangible medium.
 - > All other contracts governed by "most significant relationship test."
- > Section 110 validates parties' choice of exclusive forum so long as choice is not "unreasonable or unjust" (to be changed to unreasonable or unjust)
www.skp.com

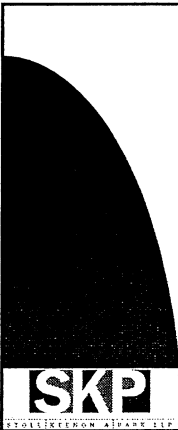
33



Warranties

- > Implied warranty of noninfringement (§ 401(a))
 - > Only given by merchants that regularly deal in information of the kind (e.g. software vendors)
 - > Obligation may be reversed if licensee provided specs and method to create information (e.g. custom-designed software)
- > Implied warranty of quiet enjoyment (§ 401(b))
 - > Given by all licensors
 - > Limited to claims by third parties that arose from act or omission of licensor
 - > Includes warranty that patent and other IP rights of licensor are valid and exclusive


www.skp.com 34



Implied Warranty of Merchantability of Computer Program - § 403

- > Merchant with respect to computer programs (e.g. software vendor) warrants to end user that program is fit for the ordinary purposes for which such programs are used
- > Norm in software industry is that software vendors rarely provide such a warranty

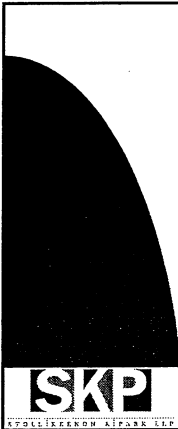
www.skp.com 35



Informational Content Warranty - § 404

- > New form of warranty
- > Implied warranty that there is no inaccuracy in the informational content caused by provider's lack of reasonable care
- > Applies only to a "merchant that, in a special relationship of reliance with a licensee, collects, compiles, processes, provides, or transmits informational content"

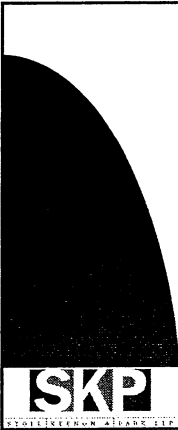
www.skp.com 36



Warranty of Fitness for a Particular Purpose - § 405

- > Implied warranty that information is fit for a particular purpose if licensor has reason to know of purpose and that licensee is relying on licensor
- > System integration is warranted if licensor is required to provide or select a system of hardware and software and knows that the licensee is relying on the licensor's judgment or skill

www.skp.com 37



Disclaimer or Modification of Warranties - § 406

- > All implied warranties except § 401 noninfringement and quiet enjoyment warranties can be disclaimed by “as is” or “with all faults” language.
- > § 401 warranties can only be disclaimed by specific language or circumstances (§ 401(d))

www.skp.com 38



Software Licenses

Will Montague
Stoll, Keenon & Park, LLP
Chair, Intellectual Property & Technology Department
300 West Vine Street, Suite 2100
Lexington, KY 40507
859.231.3946
wlm2@skp.com

www.skp.com 39

PATENT UPDATE:

**The Patentability of a Business Method,
the Survival and Future of Internet Patents and
Other Important Patent Topics**

*Andrew D. Dorisio
and
Michael S. Hargis
King & Schickli, PLLC
Lexington, Kentucky*

Copyright 2002, Andrew D. Dorisio and Michael S. Hargis

SECTION C



PATENT UPDATE:

The Patentability of a Business Method, the Survival and Future of Internet Patents and Other Important Patent Topics

Michael S. Hargis
And
Andrew D. Dorisio
King & Schickli, PLLC
Lexington, Kentucky

Table of Contents

| | | |
|-------------|---|------------|
| I. | What is a Patent? | C-2 |
| | A. Utility, Design & Plant | C-2 |
| | B. Statutes..... | C-2 |
| II. | Patentable Subject Matter | C-3 |
| III. | Utility Patent “Parts” | C-6 |
| IV. | Claims | C-7 |
| | A. Basic Types..... | C-7 |
| | 1. Product Claims..... | C-7 |
| | 2. Method Claims..... | C-7 |
| | B. New Types to Cover Developing Technologies | C-7 |
| V. | Patentability of Inventions | C-8 |
| | A. Must Meet Requirements of Patent Act..... | C-8 |
| VI. | Patent “Life” | C-9 |
| | A. Prepare and File Application | C-9 |
| | B. Prosecution..... | C-9 |
| | C. Allowance | C-9 |
| | D. Enforcement..... | C-9 |

| | | |
|--------------|---|-------------|
| VII. | Claims - Infringement..... | C-10 |
| A. | Direct Infringement..... | C-10 |
| B. | Indirect Infringement | C-11 |
| 1. | Contributory Infringement | C-11 |
| 2. | Inducement of Infringement | C-11 |
| 3. | Important Considerations..... | C-11 |
| VIII. | Business Methods - History..... | C-12 |
| A. | Not New | C-12 |
| B. | Originated in Dicta From Two Cases | C-13 |
| C. | PTO Originally Followed Exception | C-14 |
| D. | <i>Ex Parte Murray</i> | C-15 |
| E. | 1996 Edition of MPEP | C-16 |
| F. | PTO White Paper (2001) | C-17 |
| G. | <i>State Street Bank & Trust Co. v. Signature Financial Group</i> | C-18 |
| IX. | Business Methods - Generally..... | C-19 |
| A. | Rule..... | C-19 |
| B. | <i>State Street Bank & Trust Co. v. Signature Financial Group</i> | C-20 |
| C. | Pre- <i>State Street</i> Examples..... | C-21 |
| 1. | <i>Arrhythmia Tech. Inc. v. Corazonix Corp.</i> | C-21 |
| 2. | <i>In re Abele</i> | C-22 |
| X. | Business Method - Definition.... | C-23 |
| A. | No Clear Definition..... | C-23 |
| B. | Why Does it Matter? | C-24 |
| C. | Examples of Business Methods | C-25 |
| D. | Other Ways to Cover | C-28 |
| E. | Statutory First Inventor Defense..... | C-30 |
| XI. | First Inventor Defense | C-31 |
| A. | Apparatus/Product Claims | C-31 |
| B. | “Prior art”..... | C-31 |
| C. | Advice to Patent Applicant/Patent Drafter | C-34 |
| D. | Examples..... | C-35 |
| XII. | Problems/Considerations.... | C-40 |
| A. | Identifying Business Methods..... | C-40 |
| B. | Examination – Quality Issues | C-41 |
| C. | Examination – Other Issues | C-42 |
| D. | Enforceability of Business Method Patents | C-45 |
| E. | Treated Differently in Different Countries | C-47 |
| XIII. | Benefits/Advantages..... | C-48 |
| A. | Uncertainty Provides Patentee with Large Advantage in Litigation | C-48 |

| | |
|--|-------------|
| XIV. Method Patents – Special Case..... | C-49 |
| XV. Internet/Software Patents | C-52 |
| A. The (Recent) Past..... | C-52 |
| B. Past and Recent Enforceability..... | C-53 |
| C. The Present..... | C-57 |
| D. The Future..... | C-58 |
| XVI. Fixing the “Problems”..... | C-59 |



Patent Update: The Patentability of a Business Method, the Survival and Future of Internet Patents and Other Important Patent Topics

Michael S. Hargis

Andrew D. Dorisio



KING & SCHICKLI, PLLC

Patent, Trademark, Copyright & Unfair Competition Law

What is a Patent?

- A grant by the Federal Government to an inventor of the right to exclude others from making, using, selling, offering to sell, or importing an invention in the United States
- Three types - Utility, Design, and Plant
- Statutes – Title 35, United States Code



KING & SCHICKLI, PLLC

Patent, Trademark, Copyright & Unfair Competition Law

Patentable Subject Matter

- 35 U.S.C. 101 –

“Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.”



KING & SCHICKLI, PLLC

Patent, Trademark, Copyright & Unfair Competition Law

Patentable Subject Matter

- Congress intended statutory subject matter to “include anything under the sun that is made by man.” *Diamond v. Chakrabarty*, 447 U.S. 303
- Three categories of unpatentable subject matter – “laws of nature, natural phenomena, and abstract ideas.” *Diamond v. Diehr*, 450 U.S. 175



Patentable Subject Matter

- Einstein could not patent $E = mc^2$; nor could Newton patent the law of gravity
- Mathematical algorithms are not patentable subject matter "to the extent that they are merely abstract ideas." *Diehr, 450 U.S. 175*



Utility Patent “Parts”

- Background of the Invention
- Summary of the Invention
- Brief Description of the Drawings
- Detailed Description
- Drawings
- Claims – “Metes and Bounds” of Invention



Claims

- Basic Types –
 - Product claim – covers an apparatus, composition, machine, or structure
 - Method claim – covers a method or process by defining a series of steps to be followed in forming a process
- New Types Defined to Cover Developing Technologies



KING & SCHICKLI, PLLC

Patent, Trademark, Copyright & Unfair Competition Law

Patentability of Inventions

- Must meet requirements of Patent Act
 - Invention must be “statutory subject matter” and useful
 - Invention must be properly described
 - Novel – not found in the prior art in identical form
 - Non-obvious – not “obvious” in view of the prior art



Patent "Life"

- Prepare and file patent application
- "Prosecution" – consideration by Examiner at PTO; rejections, appeals, etc.
- Allowance
- Issuance
- Enforcement



KING & SCHICKLI, PLLC

Patent, Trademark, Copyright & Unfair Competition Law

Claims – Infringement

- Direct Infringement – Two types
 - Literal Infringement – each and every element of the claim must be found in the accused product or process
 - Doctrine of Equivalents – element performs substantially the same function in substantially the same way to achieve substantially the same result; “insubstantially different”



Claims – Infringement

- Indirect Infringement – Two Types
 - Contributory Infringement
 - Inducement of Infringement
- Important Considerations for Indirect Infringement
 - Both require knowledge or intent
 - Must have direct infringer in U.S.



Business Methods – History

- Business Method Patents are not new
 - Example
 - U.S. Patent No. 63,889 (issued April 10, 1867), entitled “Hotel Register” arguably describes method of advertising in hotel register
- However, business “methods” originally not considered patentable – non-statutory “business method” exception



Business Methods – History

- Originated from dicta in two cases
 - *Hotel Security Checking Co. v. Lorraine Co.*, 160 F. 467 (2d Cir. 1908):

“A system of transacting business disconnected from the means for carrying out the system is not, within the most liberal interpretation of the term, an art.”
 - *Loew’s Drive-In Theaters, Inc. v. Park-In Theaters, Inc.*, 174 F.2d 547 (1st Cir. 1949):

“[A] system for the transaction of business, . . . However novel, useful, or commercially successful is not patentable apart from the means for making the system practically useful, or carrying it out.”



Business Methods – History

- PTO originally purported to follow exception – 1994 Edition of Manual of Patent Ex. Proc. (MPEP):
“Though seemingly within the category of process or method, a method of doing business can be rejected as not being within the statutory classes.”
MPEP § 706.03(a) (1994).

C-14



KING & SCHICKLI, PLLC

Patent, Trademark, Copyright & Unfair Competition Law

Business Methods - History

- *Ex Parte Murray, 9 USPQ2d 1819 (PTO Bd. Pat. App. & Int. 1988):*

“While it may in some situations be problematic to ascertain what falls within the penumbra of the judicially prescribed ‘method of doing business,’ we find no such difficulty in the present case. We are convinced that the claimed accounting method, requiring no more than the entering, sorting, debiting and totaling of expenditures as necessary preliminary steps to issuing an expense analysis statement, is, on its very face, a vivid example of the type of ‘method of doing business’ contemplated by our review court as outside the protection of the patent statutes.”



Business Methods - History

- Next (1996) edition of MPEP provided “[o]ffice personnel have had difficulty in properly treating claims directed to methods of doing business. Claims should not be categorized as methods of doing business. Instead such claims should be treated like any other process claims.”



Business Methods - History

- PTO White Paper (2001) –
“Business data processing has followed an unbroken evolutionary path from mechanical technology up to today’s software controlled microprocessors. . . . The business method claim format has been used in various forms throughout that period.”



KING & SCHICKLI, PLLC

Patent, Trademark, Copyright & Unfair Competition Law

Business Methods - History

- *State Street Bank & Trust Co. v. Signature Financial Group*, 149 F.3d 1368, 47 USPQ2d (BNA) 1596 (Fed. Cir. 1998).
- Considered “landmark” decision - analyzed past decisions, brought problems to light, and cleared up PTO misconceptions, but really only recognized and adopted standards from past cases.



KING & SCHICKLI, PLLC

Patent, Trademark, Copyright & Unfair Competition Law

Business Methods

- Rule – business methods and mathematical algorithms are patentable provided they produce some “useful, concrete, and tangible result.”
- Taken from *In re Alappat*, 33 F.3d 1526 (Fed. Cir. 1994), where a mathematical algorithm produced “useful, concrete and tangible result” - a smooth waveform.



Business Methods

- In *State Street*, the claim was directed to a data processing system for use with mutual funds
- The court held that “the transformation of data, representing discrete dollar amounts . . . into a final share price, constitutes a practical application of a mathematical algorithm, formula, or calculation, because it produces “a useful, concrete and tangible result”--a final share price . . . ,” just like the smooth waveform in *Alappat*.



Business Methods

- Pre-*State Street* examples
 - *Arrhythmia Tech. Inc. v. Corazonix Corp.*, 958 F.2d 1053 (Fed. Cir. 1992)
 - Claim 1 – “A method of analyzing electrocardiograph signals, comprising the steps of . . . determining an arithmetic value” of an amplitude
 - Holding – the number obtained is not a mathematical abstraction, but rather a measure in microvolts of a specified heart activity



Business Methods

- *Pre-State Street* examples
 - *In re Abele*, 684 F.2d 902 (Fed. Cir. 1992)
 - Claim 5 – “A method of displaying data in a field comprising the steps of calculating the difference between the local value of the data . . . and the average value of the data . . . and displaying the difference.”
 - Holding – claim directed solely to the mathematical portion of the invention and, hence, not statutory subject matter



Business Method – Definition

- What is a “business method”?
 - No clear PTO, legislative, or judicial definition yet
 - Legislation proposed to provide definition – e.g., “Business Method Patent Improvement Act of 2000” defined “business method” as:
 - (1) a method of (A) administering, managing, or otherwise operating an enterprise or organization, including a technique used in doing or conducting business; or (B) processing financial data; (2) **any technique used in athletics, instruction, or personal skills**; and (3) any computer-assisted implementation of a method described in paragraph (1) or a technique described in paragraph (2).



Business Method- Definition

- Why does it matter?
 - For purposes of Section 101, it does not.
 - Recognized in *State Street*. Claim 1 in the patent at issue was directed to a machine. The court stated:

“for the purposes of a § 101 analysis, it is of little relevance whether claim 1 is directed to a ‘machine’ or a ‘process,’ as long as it falls within at least one of the four enumerated categories of patentable subject matter, ‘machine’ and ‘process’ being such categories.”



KING & SCHICKLI, PLLC

Patent, Trademark, Copyright & Unfair Competition Law

Business Method – Definition

C-25

US006269347B1

(12) **United States Patent**
Berger

(10) Patent No.: **US 6,269,347 B1**
(45) Date of Patent: ***Jul. 31, 2001**

(54) **METHOD FOR CALCULATION OF A REDUCED INTEREST MORTGAGE PAYMENT PLAN** 5,878,404 * 3/1999 Stout, Jr. et al. 705/38

(76) Inventor: **Jay M. Berger, 7 Bala Ave., Suite 202, Bala Cynwyd, PA (US) 19004**

(*) Notice: This patent issued on a continued prosecution application filed under 37 CFR 1.53(d), and is subject to the twenty year patent term provisions of 35 U.S.C. 154(a)(2).
Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/192,852**

(22) Filed: **Nov. 17, 1998**

(51) Int. Cl.⁷ **G06F 17/60**

(52) U.S. Cl. **705/38**

(58) Field of Search **705/38, 36**

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,739,478 * 4/1988 Roberts et al. 705/38
5,058,009 * 10/1991 Yoshino et al. 705/38
5,673,402 * 9/1997 Ryan et al. 705/38
5,689,649 * 11/1997 Altman et al. 705/36

FOREIGN PATENT DOCUMENTS

WO 00/67169 * 7/1997 (WO) G06F/17/60
WO97/27549 * 11/2000 (WO) G06F/17/00

OTHER PUBLICATIONS

"Sanwa Ball Offers Loan Patent Refunds"—2/98/ Business Editors pp 19–21.*
"Accounting For Impaired Loans"—Ward Dan—National Public Accountant V4n4 pp19–21.*
* cited by examiner

Primary Examiner—V. Millin
Assistant Examiner—Geoffrey Akers
(74) **Attorney, Agent, or Firm**—Robert B. Famiglio, Famiglio & Associates

(57) **ABSTRACT**

A method for calculating a mortgage which provides application of mortgage payments to principle first and then interest in the amortization schedule of repayment of a conventional loan is disclosed. The disclosure provides a method for calculating mortgage payments on a conventional mortgage loan by applying such payments first to reduction of principle while accumulating accrued interest. Payments are applied towards accrued interest after the principle amount of the loan is reduced.

4 Claims, 1 Drawing Sheet

| | Table 1 | Table 2 | Table 3 | Table 4 |
|--------------------------------|--------------|--------------|--------------|--------------|
| Amount | \$100,000.00 | \$100,000.00 | \$100,000.00 | \$100,000.00 |
| Interest Rate (in percentages) | 7% | 7% | 7% | 7% |
| Monthly Payment | \$665.30 | \$665.30 | \$456.19 | \$583.33 |
| Term of Loan | 360 mo. | 216 mo. | 360 mo. | 257 mo. |
| Total Interest | \$139,508.00 | \$43,704.00 | \$64,228.00 | \$49,915.00 |

- Example of true "business method" or process
- U.S. Patent No. 6,269,347, "Method for Calculation of a Reduced Interest Mortgage Payment Plan."
- www.uspto.gov



KING & SCHICKLI, PLLC
Patent, Trademark, Copyright & Unfair Competition Law

Business Method - Definition



US005960411A

United States Patent [19] [11] **Patent Number:** 5,960,411
Hartman et al. [45] **Date of Patent:** Sep. 28, 1999

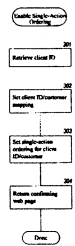
[54] **METHOD AND SYSTEM FOR PLACING A PURCHASE ORDER VIA A COMMUNICATIONS NETWORK**
 [75] Inventors: **Perl Hartman, Jeffrey P. Bezos, Shel Kaphan, Joel Spiegel**, all of Seattle, Wash.
 [73] Assignee: **Amazon.com, Inc.**, Seattle, Wash.
 [21] Appl. No.: **08/928,951**
 [22] Filed: **Sep. 12, 1997**
 [51] Int. Cl.⁶ **G06F 17/60**
 [52] U.S. Cl. **705/26, 705/27, 345/962**
 [58] **Field of Search** **705/26, 27, 380/24, 380/25, 235/2, 375, 378, 381, 395/188.01, 345/962**

[56] **References Cited**
U.S. PATENT DOCUMENTS
 4,937,863 6/1990 Robert et al. 380/4
 5,204,897 4/1993 Wyman 380/4
 5,260,999 11/1993 Wyman 384/4
 5,627,940 5/1997 Rohra et al. 395/12
 5,640,501 6/1997 Turpin 395/768
 5,640,577 6/1997 Scharmer 395/768
 5,654,111 9/1997 Nahan et al. 705/27
 5,715,314 2/1998 Payne et al. 380/24
 5,715,399 2/1998 Bezos 705/27
 5,727,163 3/1998 Bezos 705/27
 5,745,681 4/1998 Levine et al. 395/200.3
 5,758,126 5/1998 Daniels et al. 395/500

FOREIGN PATENT DOCUMENTS
 0855659 A1 1/1998 European Pat. Off. G06F 17/30
 0855687 A2 1/1998 European Pat. Off. G07F 19/00
 0845747A2 6/1998 European Pat. Off. G06F 17/60
 0883076A2 12/1998 European Pat. Off. G06F 17/60
 WO 95/30961 11/1995 WIPO G06F 17/60
 WO 96/38799 12/1996 WIPO G06F 17/60
 WO 98/21679 5/1998 WIPO G06F 17/60

OTHER PUBLICATIONS
 Jones, Chris. "Java Shopping Cart and Java Wallet; Oracles plans to join e-commerce initiative." Mar. 31, 1997, Info-World Media Group.
 "Pacific Coast Software Software creates virtual shopping cart." Sep. 6, 1996, M2 Communications Ltd 1996.
 "Software Creates Virtual Shopping Cart." Sep. 5, 1996, Business Wire, Inc.
 Terdoslavich, William. "Java Electronic Commerce Framework." Computer Reseller News, Sep. 23, 1996, CMP Media, Inc., 1996, pp. 126, http://www.elibrary.com/id/101/101/getdoc...rydocid=902269@library_d&dtype=0-0&dist=0. [Accessed Nov. 19, 1998].
 "Internet Access: Disc Distributing Announces Interactive World Wide." Cambridge Work-Group Computing Report, Cambridge Publishing, Inc., 1995, http://www.elibrary.com/id/101/101/getdoc...docid=1007497@library_a&dtype=0-0&dist=0. [Accessed Nov. 19, 1998].

26 Claims, 11 Drawing Sheets



- Another Example of claim to business "method"
- U.S. Patent No. 5,960,411, Amazon's "one-click" patent



KING & SCHICKLI, PLLC
 Patent, Trademark, Copyright & Unfair Competition Law

Business Method - Definition



US005794207A

United States Patent [19] **Patent Number:** 5,794,207
Walker et al. [45] **Date of Patent:** Aug. 11, 1998

[54] **METHOD AND APPARATUS FOR A CRYPTOGRAPHICALLY ASSISTED COMMERCIAL NETWORK SYSTEM DESIGNED TO FACILITATE BUYER-DRIVEN CONDITIONAL PURCHASE OFFERS**

[75] **Inventors:** Jay S. Walker, Ridgefield, Conn.; Bruce Schneier, Oak Park, Ill.; James A. Jorasch, Stamford, Conn.

[73] **Assignee:** Walker Asset Management Limited Partnership, Stamford, Conn.

[21] **Appl. No.:** 797,660

[22] **Filed:** Sep. 4, 1996

[51] **Int. Cl.⁶** G06F 15/20

[52] **U.S. Cl.** 785/23; 705/26; 380/49; 380/23; 380/25

[58] **Field of Search** 395/226, 227; 395/237, 238, 239, 244; 380/23, 24, 25, 49; 705/26, 27, 37, 38, 39, 44, 1, 5, 6

[56] **References Cited**

U.S. PATENT DOCUMENTS

| | | | |
|-----------|---------|-----------------|---------|
| 4,247,759 | 1/1981 | Yaris et al. | 235/381 |
| 4,449,186 | 5/1984 | Kelly et al. | 395/205 |
| 4,553,222 | 11/1985 | Kadmad et al. | 395/215 |
| 4,789,928 | 12/1988 | Fujisaki | 364/401 |
| 4,799,156 | 1/1989 | Sawvit et al. | 395/226 |
| 4,933,201 | 2/1990 | Wagner | 364/408 |
| 5,021,953 | 6/1991 | Webber et al. | 364/407 |
| 5,168,446 | 12/1992 | Wiseman | 395/237 |
| 5,191,613 | 3/1993 | Graziano et al. | 380/25 |
| 5,557,518 | 9/1996 | Rosen | 364/408 |

OTHER PUBLICATIONS

Richard E. Speidel & Lee A. Schott, "Impact of Electronic Contracting on Contract Formation Under Revised UCC Article 2, Sales," C878 *ALI-ABA* 335, Dec. 9, 1993.

Jeffrey B. Ritter, "Scope of the Uniform Commercial Code: Computer Contracting Cases and Electronic Commercial Practices," 45 *Bus. Law* 2533 (Aug. 1990).

Laura Del Rosso, "Market Says it Plans to Launch Air Fare 'Auction' in June," *Travel Weekly*, Apr. 29, 1991.

Jeff Peltine, "Travelers Bidding on Airline Tickets; SF Firm Offers Chance for Cut-rate Fares," *San Francisco Chronicle*, Section A4, Aug. 19, 1991.

Michael Schrage, "An Experiment in Economic Theory: Labs Testing Real Markets," *The Record* Section B1, Nov. 26, 1989.

Laura Del Rosso, "Ticket-Bidding Firm Closes its Doors," *Travel Weekly*, Mar. 12, 1992.

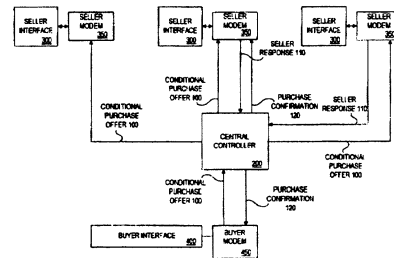
(List continued on next page.)

Primary Examiner—Thomas H. Turcza
Assistant Examiner—Pinchus M. Laufer
Attorney, Agent, or Firm—Morgan & Finnegan LLP; Jeffrey L. Brandt

ABSTRACT

The present invention is a method and apparatus for effectuating bilateral buyer-driven commerce. The present invention allows prospective buyers of goods and services to communicate a binding purchase offer globally to potential sellers, for sellers conveniently to search for relevant buyer purchase offers, and for sellers potentially to bind a buyer to a contract based on the buyer's purchase offer. In a preferred embodiment, the apparatus of the present invention includes a controller which receives bidding purchase offers from prospective buyers. The controller makes purchase offers available globally to potential sellers. Potential sellers then have the option to accept a purchase offer and thus bind the corresponding buyer to a contract. The method and apparatus of the present invention have applications on the Internet as well as conventional communications systems such as voice telephony.

44 Claims, 20 Drawing Sheets



- Apparatus claims covering business "method"
- U.S. Patent No. 5,794,207, Priceline.com's Reverse Auction Patent



KING & SCHICKLI, PLLC
 Patent, Trademark, Copyright & Unfair Competition Law

Business Method – Definition

- Other ways to cover:
 - Computer-readable medium claims (apparatus, computer program product, “Beauregard” claims”)
 - “A computer-readable medium containing instructions for . . . by a method comprising”
 - *In re Beauregard*, 53 F.3d 1583 (Fed. Cir. 1995)



KING & SCHICKLI, PLLC

Patent, Trademark, Copyright & Unfair Competition Law

Business Method – Definition

- Data Structure claims
- “A computer-readable medium containing a data structure for use in allocating memory, the data structure containing”
- *In re Lowry*, 32 F.3d 1579 (Fed. Cir. 1994)



Business Method - Definitions

- Why does it matter what type?
- American Inventors Protection Act of 1999 – “First Inventor Defense”
- 35 USC Section 273:

“It shall be a defense to an action for infringement . . .with respect to any subject matter that would otherwise infringe one or more claims for a **method** in the patent being asserted against a person, if such person had, acting in good faith, actually reduced the subject matter to practice at least 1 year before the effective filing date of such patent, and commercially used the subject matter before the effective filing date of such patent” (emphasis added).



First Inventor Defense

- Apparatus/Product Claims – Invalidity is a Defense to Infringement – claimed invention is anticipated by or obvious in view of the prior art
- “Prior art” comprises, *inter alia*, prior use of an apparatus, product, etc., but there can be no abandonment, suppression, or concealment of the invention



First Inventor Defense

- Here, defense provided against “method” in the patent based on “commercial” use
- “Commercial Use” defined in statute – does not require public knowledge or accessibility
- Defense is personal to alleged infringer; commercial use may not invalidate patent
- “Use” cannot be abandoned
- If successful, can only expand use on site, not to other sites
- “Exhaustion” principle – does not extend to product produced by patented method



First Inventor Defense

- Makes it less risky to maintain trade secret protection, BUT:
 - Only extends to method claims in patents, not apparatus/product claims
 - Defense must be proven by “clear and convincing evidence”
 - If an unreasonable assertion of the defense is made, the judge can declare the case exceptional and award attorneys fees



First Inventor Defense

- Advice to patent applicant's/patent drafters – whenever possible, present different types of claims (apparatus, computer-readable medium, data structure) to avoid wholesale unenforceability against alleged infringer



First Inventor Defense



US006457317B1

(12) **United States Patent**
O'Donnell

(10) Patent No.: **US 6,457,317 B1**
(45) Date of Patent: **Oct. 1, 2002**

(54) **METHOD OF SELLING MERCHANDISE ON A GOLF COURSE**

(76) Inventor: **Michael O'Donnell, 43510 Bannockbaun, Canton, MI (US) 48187**

(* Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/766,804**

(22) Filed: **Jan. 22, 2001**

(51) Int. Cl.⁷ **B65B 63/08; F25D 3/08; G06F 17/60; G06G 1/14**

(52) U.S. Cl. **62/60; 62/371; 705/22**

(58) Field of Search **62/371; 156/270; 206/139; 224/274; 235/462.43; 705/22**

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,429,290 A • 3/1995 Greene, Jr. 224/274
5,535,883 A • 7/1996 Henderson 206/139

5,878,401 A • 3/1999 Joseph 705/22
5,930,770 A • 7/1999 Edgar 235/462.43
5,975,390 A • 11/1999 Saroli 224/274
6,067,813 A • 5/2000 Smith 62/371
6,129,796 A • 10/2000 Steinberg et al. 156/270

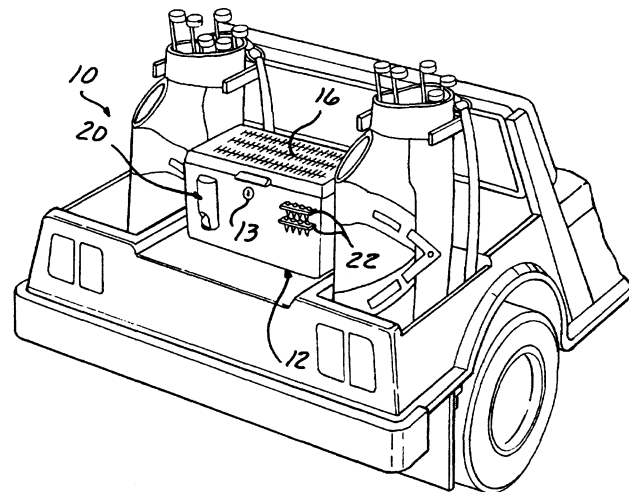
* cited by examiner

Primary Examiner—William C. Doerrier
Assistant Examiner—Filip Zec
(74) *Attorney, Agent, or Firm*—John R. Benefiel

(57) **ABSTRACT**

A method selling merchandise to golf course patrons, in which a storage unit is stocked with an exactly inventory of merchandise and is loaded onto a rental golf cart at the beginning of each rental period and made accessible to the rental patron as desired, the inventory retailed at the end of each rental period and the patron debited for the merchandise computed to have been removed from inventory. Cooled beverages can be dispensed from a storage unit which is cooled, as by the use of solar power, during the rental period.

5 Claims, 2 Drawing Sheets



- But, sometimes, presenting claims besides those directed to the method may not be possible
- Example – U.S. Patent No. 6,457,317, "Method of Selling Merchandise on a Golf Course"



KING & SCHICKLI, PLLC

Patent, Trademark, Copyright & Unfair Competition Law

First Inventor Defense



US005616089A

United States Patent [19]
Miller

[11] Patent Number: 5,616,089
[45] Date of Patent: Apr. 1, 1997

[54] METHOD OF PUTTING

[76] Inventor: Dale D. Miller, 4801 Indigo Dr., Wausau, Wis. 54401

[21] Appl. No.: 624,264

[22] Filed: Mar. 29, 1996

[51] Int. Cl.⁶ A63B 53/00

[52] U.S. Cl. 473/409; 473/131; 473/300

[58] Field of Search 473/131, 409, 473/207, 212, 213, 214, 226, 251, 266, 293, 300, 294, 252

[56] References Cited

U.S. PATENT DOCUMENTS

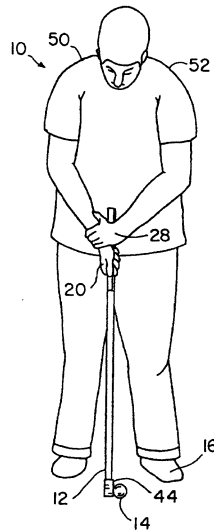
| | | | |
|-----------|---------|----------------|---------|
| 3,263,998 | 8/1966 | Fanning | 473/409 |
| 3,486,755 | 12/1969 | Hodge | 473/293 |
| 4,067,573 | 1/1978 | Key, Jr. | 473/300 |
| 4,272,077 | 6/1981 | Spivey | 473/300 |
| 4,605,228 | 8/1986 | Gwendling, Jr. | 473/293 |

Primary Examiner—Steven B. Wong
Attorney, Agent, or Firm—Andrus, Scales, Starke & Sawall

[57] ABSTRACT

A method of putting features the golfer's dominant hand so that the golfer can improve control over putting speed and direction. The golfer's non-dominant hand stabilizes the dominant hand and the orientation of the putter blade, but does not otherwise substantially interfere with the putting stroke. In particular, a right-handed golfer grips the putter grip with their right hand in a conventional manner so that the thumb on the right hand is placed straight down the top surface of the putter grip. The golfer addresses the ball as if to stroke the putter using only the right hand. Then, the golfer takes the left hand and uses it to stabilize the right hand and the putter. To do this, the golfer places their left hand over the interior wrist portion of the right hand behind the thumb of the right hand with the middle finger of the left hand resting on the styloid process of the right hand. The golfer presses the ring finger and the little finger of their left hand against the back of the right hand. The golfer also presses the palm of the left hand against the putter grip and squeezes the right hand with the left hand. The golfer then takes a full putting stroke with the above described grip.

13 Claims, 2 Drawing Sheets



U.S. Patent No.
5,616,089, "Method
of Putting"

- Business method?
"technique used in
athletics, instruction,
or personal skills" –
definition from
proposed legislation



KING & SCHICKLI, PLLC

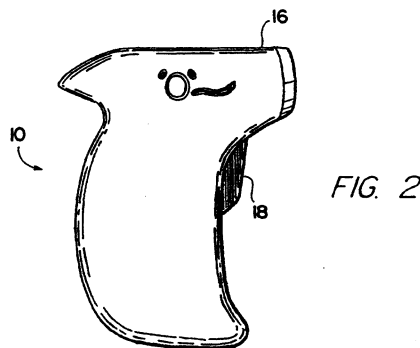
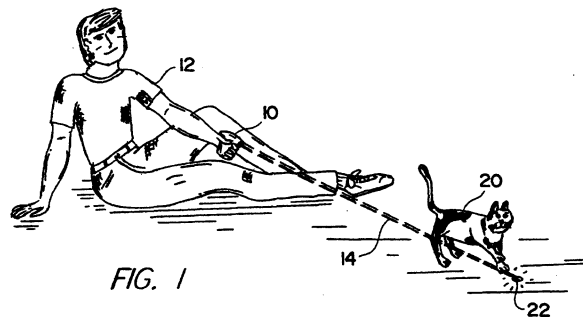
Patent, Trademark, Copyright & Unfair Competition Law

First Inventor Defense

U.S. Patent

Aug. 22, 1995

5,443,036



- Another Example
- U.S. Patent No. 5,443,036, "Method of Exercising a Cat":
 1. A method of inducing aerobic exercise in an unrestrained cat comprising the steps of:
 - (a) directing an intense coherent beam of invisible light produced by a hand-held laser apparatus to produce a bright highly-focused pattern of light at the intersection of the beam and an opaque surface, said pattern being of visual interest to a cat; and
 - (b) selectively redirecting said beam out of the cat's immediate reach to induce said cat to run and chase said beam and pattern of light around an exercise area.



KING & SCHICKLI, PLLC

Patent, Trademark, Copyright & Unfair Competition Law

First Inventor Defense



US006368227B1

(12) **United States Patent**
Olson

(10) **Patent No.:** US 6,368,227 B1
(45) **Date of Patent:** Apr. 9, 2002

(54) **METHOD OF SWINGING ON A SWING** 5,413,298 A * 5/1995 Perreault 248/228

(76) **Inventor:** Steven Olson, 337 Otis Ave., St. Paul, MN (US) 55104 * cited by examiner

(*) **Notice:** Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) **Appl. No.:** 09/715,198

(22) **Filed:** Nov. 17, 2000

(51) **Int. Cl. 7** A63G 9/00

(52) **U.S. Cl.** 472/118

(58) **Field of Search** 472/118, 119, 472/120, 121, 122, 123, 125

(56) **References Cited**

U.S. PATENT DOCUMENTS

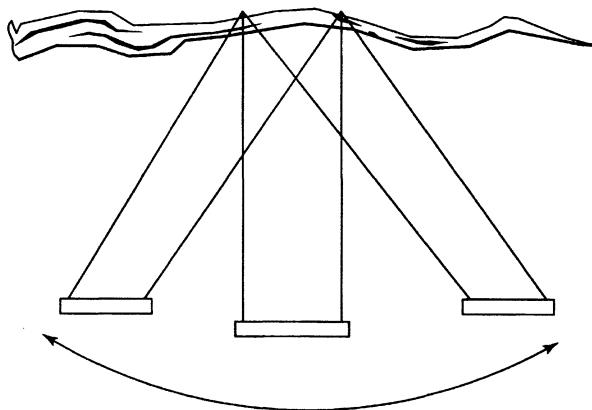
242,601 A * 6/1881 Clement 472/118

(74) **Attorney, Agent, or Firm**—Peter Lowell Olson

(57) **ABSTRACT**

A method of swing on a swing is disclosed, in which a user positioned on a standard swing suspended by two chains from a substantially horizontal tree branch induces side to side motion by pulling alternately on one chain and then the other.

4 Claims, 3 Drawing Sheets



- Yet another example
- U.S. Patent No. 6,368,227, "Method of Swinging on a Swing"
- Personal skills?



First Inventor Defense

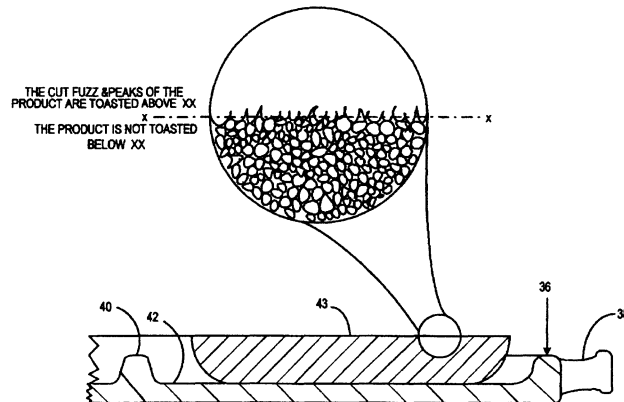


United States Patent [19] **Patent Number:** **6,080,436**
Lenahan [45] **Date of Patent:** **Jun. 27, 2000**

[54] **BREAD REFRESHING METHOD** 5,382,441 1/1995 Lantz et al. 426/241
 [76] **Inventor:** **Terrance F. Lenahan**, 246 Unity Dr., 5,472,721 12/1995 Eisenberg et al. 426/243
 Marietta, Ga. 30064-5446 6,013,900 1/2000 Westerberg et al. 219/405

[21] **Appl. No.:** 09/332,385 *Primary Examiner*—Nina Bhat
 [22] **Filed:** Jun. 14, 1999 *Attorney, Agent, or Firm*—Peter Vrabotes

[51] **Int. Cl.⁷** A21D 6/00 [57] **ABSTRACT**
 [52] **U.S. Cl.** 426/242; 426/496; 99/451; 219/725
 [58] **Field of Search** 426/241, 242, 426/496; 99/451; 219/725
 [56] **References Cited**
 U.S. PATENT DOCUMENTS
 5,049,398 9/1991 Saari et al. 426/20 3 Claims, 5 Drawing Sheets



- Yet another example
 - U.S. Patent No. 6,080,436, "Bread Refreshing Method"
1. A method of refreshing bread products, comprising:
 - a) placing a bread product in an oven having at least one heating element,
 - b) setting the temperature of the heating elements between 2500 F. and 4500 F., and
 - c) ceasing exposure of the bread product to the at least one heating element after a period of 3 sec. to 90 sec.



KING & SCHICKLI, PLLC
Patent, Trademark, Copyright & Unfair Competition Law

Problems/Considerations

- Identifying Business Methods
 - In many cases, client does not realize business method is patentable
 - One year after “public use” – may be too late to obtain patent
 - May want to simply keep as trade secret, if not previously disclosed



Problems/Considerations

- Examination – Quality Issues
 - Filings surged (but still less than 1%)
 - Primary Class – 705 – 1996 – 274 patents issued; 2001 – 877 patents issued; 2002 – 668 through 10/1/02
 - Not enough skilled examiners
 - But, examiners given 31 hours to examine applications in 705, as compared to 18 hours in other arts



Problems/Considerations

- Examination – Other issues
 - Prior art not well developed, difficult to locate
 - Traditional notions of obviousness sometimes hard to apply – does using a computer or the Internet to perform a well-known “brick and mortar” method somehow create a non-obvious invention?



Problems/Considerations



US006049811A

United States Patent [19] Patent Number: 6,049,811
 Petruzzi et al. [45] Date of Patent: Apr. 11, 2000

[54] MACHINE FOR DRAFTING A PATENT APPLICATION AND PROCESS FOR DOING SAME

[76] Inventors: James D. Petruzzi; Robert M. Mason, both of 13760 Noel, #820, Dallas, Tex. 75240

[21] Appl. No.: 08/756,444

[22] Filed: Nov. 26, 1996

[51] Int. Cl.⁷ G06F 17/21

[52] U.S. Cl. 707/507

[58] Field of Search 707/517-529, 707/507, 705/1

[56] References Cited

U.S. PATENT DOCUMENTS

5,623,681 4/1997 Rivette et al. 707/522

OTHER PUBLICATIONS

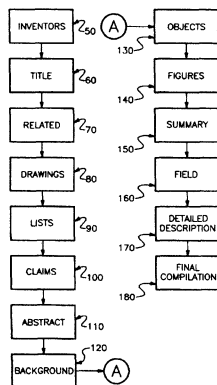
Pressman, Patent It Yourself, p. 8/1-8/20, Aug. 1996.
 Pressman, Software Engineering, A Practitioner's Approach, p. 98-111, 1982.

Primary Examiner—Anton Fetting

[57] ABSTRACT

A machine and method for drafting a patent application has a keyboard, mouse, display, printer, and a computer for receiving and transmitting data. The computer requests and stores information regarding the invention including, if appropriate: 1) qualities and benefits (QAB) of the invention over the prior technology; 2) primary elements (PE) of the invention that define the invention apart from prior technology; 3) secondary elements (SE) of the invention that may be important but not necessary to define over the prior technology; and 4) substitute elements (SUB) of the invention that may substituted or modified in an effort to avoid the primary and secondary elements but not depart from the invention. The QAB are requested and stored before the objects of the invention are drafted, the PE are requested and stored before the independent claims are drafted, the SE and SUB are requested and stored before the dependent claims are drafted, the independent claims are drafted before the summary of the invention is drafted, the independent claims are drafted before the dependent claims are drafted, the dependent claims are drafted before the abstract of the disclosure is drafted, and all claims are drafted before the detailed description of a preferred embodiment is drafted. The sections are drafted in a predetermined order prohibiting jumping ahead to draft a later section. At many sections, initial draft text, examples, samples, legal material, etc. are available to the user. A final patent application is compiled by combining the drafted sections with predetermined text.

18 Claims, 4 Drawing Sheets



- Another example
- U.S. Patent No. 6,049,811, "Machine for drafting a patent application and process for doing same."



KING & SCHICKLI, PLLC

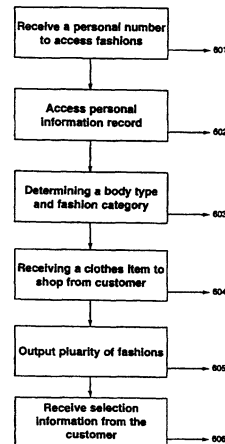
Patent, Trademark, Copyright & Unfair Competition Law

Problems/Considerations

C-44

| | | | |
|----------------------------------|---|---|----------------------|
| | | US005930769A | |
| United States Patent [19] | | [11] Patent Number: | 5,930,769 |
| Rose | | [45] Date of Patent: | Jul. 27, 1999 |
| [54] | SYSTEM AND METHOD FOR FASHION SHOPPING | 5,163,007 11/1992 Slatky | 364/470.03 |
| | | 5,495,568 2/1996 Beavin | 364/188 |
| | | 5,551,021 8/1996 Harada et al. | 707/104 |
| | | 5,680,314 10/1997 Patterson et al. | 364/470.03 |
| [76] | Inventor: Andrea Rose, 245 E. 63rd St., Apt. 319, New York, N.Y. 10021 | OTHER PUBLICATIONS | |
| [21] | Appl. No.: 08/726,674 | Sizing Up Clothing Sizes, Know How Magazine, Spring, 1994. | |
| [22] | Filed: Oct. 7, 1996 | <i>Primary Examiner</i> —Edward R. Cosimano | |
| [51] | Int. Cl. ⁶ | ABSTRACT | |
| [52] | U.S. Cl. | [57] The present invention provides a method of manual fashion shopping and method for electronic fashion shopping by a customer using a programmed computer, CD-ROM, television, Internet or other electronic medium such as video. The method comprises receiving personal information from the customer; selecting a body type and fashion category based on the personal information; selecting fashions from a plurality of clothes items based on the body type and fashion category; outputting a plurality of fashion data based on the selected fashions; and receiving selection information from the customer. | |
| [58] | Field of Search | | |
| [56] | References Cited | 45 Claims, 6 Drawing Sheets | |
| | U.S. PATENT DOCUMENTS | | |
| | 4,149,246 4/1979 Goldmas | 364/470.03 | |
| | 4,261,012 4/1981 Maloonia | 358/93 | |
| | 4,546,434 10/1985 Gioello | 364/400 | |
| | 4,626,344 12/1986 Collins et al. | 364/470.03 | |
| | 4,916,624 4/1990 Collins et al. | 364/470.03 | |
| | 4,916,634 4/1990 Collins et al. | 395/10 | |
| | 5,163,006 11/1992 Dezil | 364/470.03 | |

- Example of using computer or Internet to perform "old" process
- U.S. Patent No. 5,930,769, "Method of Fashion Shopping."



KING & SCHICKLI, PLLC

Patent, Trademark, Copyright & Unfair Competition Law


Problems/Considerations

- Enforceability of Business Method Patents
 - Methods of golfing, swinging, exercising cat
 - difficult to find infringer, prove infringement
 - Need direct infringer in United States – contributory/inducement of infringement requires knowledge - more difficult to prove; thus, in most cases, want claims directed at manufacturer/producer, not end user



Problems/Considerations

C-46


 US006143347A

United States Patent (19) [11] **Patent Number:** 6,143,347
Keithly et al. [45] **Date of Patent:** Nov. 7, 2000

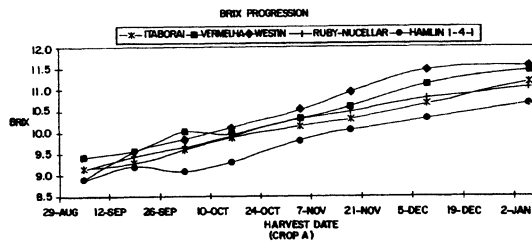
[54] **EARLY SEASON NOT FROM CONCENTRATE ORANGE JUICE AND PROCESS OF MAKING**
 [75] **Inventors:** James H. Keithly, Bradenton; Harold Pollack, St Petersburg; Thomas Taggart, Bradenton, all of Fla.
 [73] **Assignee:** Tropicana Products, Inc., Bradenton, Fla.
 [21] **Appl. No.:** 09/311,956
 [22] **Filed:** May 14, 1999
 [51] **Int. Cl. 7** A23L 2/02
 [52] **U.S. Cl.** 426/599; 426/616
 [58] **Field of Search** 426/616, 599

OTHER PUBLICATIONS
 Nelson et al. Fruit and Vegetable Juice Processing Technology, 3rd Ed. Avi Publishing Co, Westport, CT, pp. 41, 42 and 64, 1980.
 Pio, Junior and Sobrinho, Study of Some Characteristics of Fruit and Seeds of Various Kinds of Sweet Orange, *Citrus sinensis* (L.) Osbeck, Sao Paulo, Brazil (circa 1983).
 Road, Hendrix and Hendrix, *Quality Control Manual For Citrus Processing Plants*, vol. 1, pp. 22-31, Intercel, Inc., Safety Harbor, Florida (1986).
Primary Examiner—Helen Pratt
Attorney, Agent, or Firm—Cook, Alex, McFarren, Manzo, Cummings & Mebler, Ltd.

ABSTRACT
 Not from concentrate orange juice is provided which includes as a freshly squeezed orange juice component juice extracted from an early season round orange cultivar which has a color intensity in excess of that provided by Hamlin cultivars which are harvested at the same time as the early season cultivar, which is not a Hamlin cultivar. The juice extracted from such early season cultivar has sensory attributes which are at least as acceptable as Hamlin fresh juice. Preferred early season cultivars are within the Seleta family or are Westin cultivars or are Ruby Navel cultivars.

References Cited
U.S. PATENT DOCUMENTS
 3,227,562 1/1966 Houghtaling 426/599
 5,296,483 3/1994 Yokoyama et al. 504/326
 5,468,508 11/1995 Wu et al. 426/599
 6,037,863 12/1999 Chanchai et al. 426/599
FOREIGN PATENT DOCUMENTS
 288103 11/1988 European Pat. Off.

47 Claims, 12 Drawing Sheets



- Tropicana's U.S. Patent No. 6,143,347, "Early season not from concentrate orange juice and process of making"
- Claims both juice and blending method
- PTO "looking at"



KING & SCHICKLI, PLLC

Patent, Trademark, Copyright & Unfair Competition Law

Problems/Considerations

- Treated differently in different countries
 - Europe – Business methods in the Abstract are not patentable – must define structure, such as a programmed computer
 - Japan – parallel to the United States in some respects
 - Elsewhere – mixed bag



Benefits/Advantages

- Uncertainty provides patentee with large advantage in litigation
 - Barnes & Noble lost at preliminary injunction round and eventually settled case over “one-click” patent
 - E-Bay in lengthy dispute with individual owning patents on various aspects of online auction dating from 1995 – likely to settle




Method Patents – Special Case

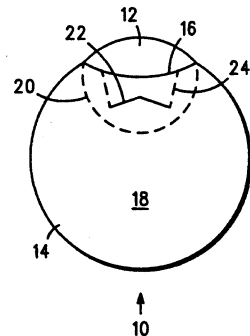
- Medical Treatment Steps or Surgical Techniques as “Business” Methods
- Patentable, but not enforceable *unless* the use of a patentable machine, manufacture, or composition is required
- 35 USC Section 287(c)

“With respect to a medical practitioner’s performance of a medical activity that constitutes an infringement . . . [of a patent], the provisions of sections 281, 283, 284, and 285 [basically, the remedy and damages provisions] of this title shall not apply against the medical practitioner or against a related health care entity.”



Method Patents – Special Case

| | | | |
|---|--|---------------|---------|
|  US005080111A | | | |
| United States Patent [19] | [11] Patent Number: 5,080,111 | | |
| Pallin | [45] Date of Patent: Jan. 14, 1992 | | |
| [54] METHOD OF MAKING SELF-SEALING EPISCLERAL INCISION | | | |
| [76] Inventor: Samuel L. Pallin, 10615 W. Thunderbird Blvd., Sun City, Ariz. 85351 | | | |
| [21] Appl. No.: 544,984 | | | |
| [22] Filed: Jun. 28, 1990 | | | |
| [51] Int. Cl.: A61F 9/00 | | | |
| [52] U.S. Cl.: 128/898; 606/107 | | | |
| [58] Field of Search: 606/107, 161, 166; 128/898; 623/6 | | | |
| [56] References Cited | | | |
| U.S. PATENT DOCUMENTS | | | |
| 4,607,617 | 8/1986 | Choyce | 606/107 |
| 4,619,657 | 10/1986 | Keates et al. | 606/107 |
| 4,702,244 | 10/1987 | Mazzocco | 606/107 |
| 4,706,666 | 11/1987 | Sheets | 606/107 |
| 4,773,415 9/1988 Ten 606/107 4,844,065 7/1989 Faulkner 606/107 4,959,070 9/1990 McDonald 606/107 | | | |
| Primary Examiner—John D. Yasko Assistant Examiner—William Lewis Attorney, Agent, or Firm—Harry A. Wolin | | | |
| [57] ABSTRACT | | | |
| A substantially self-sealing episcleral incision having an approximate central point 1.5 to 3.0 millimeters posterior to the limbus. Portions of the incision extending from the approximate central point extend laterally away from the curvature of the limbus. The configuration of the self-sealing incision allows the incision to seal as the eye is inflated following surgery and therefore requires no sutures for sealing. Accordingly, the probability of astigmatism is eliminated or greatly reduced and the reliance on sutures is eliminated. | | | |
| 29 Claims, 1 Drawing Sheet | | | |



- 287(c) came about as the result of a patent infringement action filed by Dr. Samuel L. Pallin against Dr. Jack A. Singer over U.S. Patent No. 5,080,111, which is directed to a patented surgical technique for use during cataract surgery.

C-50



KING & SCHICKLI, PLLC

Patent, Trademark, Copyright & Unfair Competition Law

Method Patents – Special Case

- Only applies to “medical practitioners” – defined in statute – licensed by state or acting under the direction of such person
- Exempts “related health care entity” also
- Does not apply to veterinary procedures (unless the animal is “used in medical research or instruction directly relating to the treatment of humans”)
- Query – why is a surgical technique any different from a medical device, drug, or method of doing business?

C-51



KING & SCHICKLI, PLLC

Patent, Trademark, Copyright & Unfair Competition Law

Internet/Software Patents

- The (Recent) Past
 - Software patentable subject matter, including method claims if concrete result produced
 - Examination difficulties – overworked Patent Examiners, limited prior art
 - Big consideration for inventors – if software is going to be obsolete in a short time, does it make sense to make investment in patent that might not issue for several years?



KING & SCHICKLI, PLLC

Patent, Trademark, Copyright & Unfair Competition Law

Internet/Software Patents

- Past and Recent Enforceability
 - Not many decisions upholding, but most tend to enforce or suggest enforceability – “one-click”
 - Litigation Rate – Patents in Class 705 issued since 1975
 - February 2000 – 53
 - December 2001 - 116



Internet/Software Patents

- Some trying to enforce “old” patents on new technology – e.g., British Telecom’s U.S. Patent No. 4,873,662 (filed in 1980) allegedly covering “hyperlinking” asserted against major ISP’s in the United States
- Prodigy recently obtained summary judgment of non-infringement - *British Telecomms. PLC v. Prodigy Communs. Corp.*, 2002 U.S. Dist. LEXIS 15521 (S.D.N.Y August 22, 2002)



Internet/Software Patents

- Past or Recent Enforcement Efforts
 - Activebuddy's U.S. Patent No. 6,430,602 covers method and system for interactively responding to instant messaging requests – sent licensing offers
 - News reports – targeted parties found anticipatory prior art dated years before the patent filing date in a matter of minutes using Internet search engine



Internet/Software Patents

- Past or Recent Enforcement Efforts
 - Since 1998, Microsoft accused of patent infringement in at least 35 patent infringement lawsuits
 - Only 7 suits in previous 22 years – lost only one (but settled most)
 - Microsoft – times are tough
 - Patentees – Microsoft not playing fair



Internet/Software Patents

- The Present
 - Economy down, number of filings up???
 - No more “submarine” patents – term now 20 years from filing – patentee’s delay reduces patent term
 - Automatic publication if foreign filing made
 - third parties can submit art to examiner – double-edged sword
 - Alternate forms of protection (copyright)



Internet/Software Patents

- The Future

- Filings expected to increase exponentially as transformation into “digital age” continues
- PTO must expand and grow to handle
- Prior art will become more readily available as PTO/EPO/JPO issue more patents
- Cases on obviousness that merely use software or Internet to perform well-known tasks needed to “raise bar.”



Fixing the “Problems”

- Many believe problems will fix themselves using existing legal concepts; e.g., reexamination
- Publication opens door to improvement – citation of prior art by others (but no *inter partes participation*)



Fixing the "Problems"

- PTO slowly getting "better"
 - Overall grant rate 72%
 - 2000 "business method" rate – 55%
 - 2001 rate – 33.6%
- "Second set of eyes" – Two QA Officers
- Presently sending Examiners on "field trips" to corporations and arming with corporate manuals on business practices

C-60



KING & SCHICKLI, PLLC

Patent, Trademark, Copyright & Unfair Competition Law

Fixing the “Problems”

- Other solutions – None attractive
 - Eliminate “presumption of validity” to lower burden of proof
 - Shorter term, expedited examination
 - No remedy for infringement
 - Opposition
 - Presumption of Obviousness (present in proposed legislation)
 - Compulsory licensing



Fixing the “Problems”

- Viable solution to “obviousness” problem – expand definition of “analogous art”
- Section 103 – “A patent may not be obtained . . . if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art *to which said subject matter pertains*” (emphasis added).



Fixing the “Problems”

- **Under standard, inventor is charged with “knowledge from those arts reasonably pertinent to the particular problem”**

- **Amazon’s “one click” patent – Claim 1**

A method of placing an order for an item comprising:

displaying information identifying the item; and

in response to only a single action being performed, sending a request to order the item along with an identifier of a purchaser of the item to a server system;

under control of a single-action ordering component of the server system, receiving the request;

retrieving additional information previously stored for the purchaser identified by the identifier in the received request; and

generating an order to purchase the requested item for the purchaser identified by the identifier in the received request using the retrieved additional information; and

fulfilling the generated order to complete purchase of the item

whereby the item is ordered without using a shopping cart ordering model.



Fixing the “Problems”

- '411 patent says single action required for ordering can be voice command
- Ordering room service? Analogous Art?
- Bar tab? Analogous Art?
- Can such events be cited by Examiner as “analogous art”? If so, patent might not have issued in the first instance



**PROTECTING AGAINST AND
PROSECUTING CYBERCRIME
(INCLUDING CYBERTERRORISM)**

Marisa J. Ford
Assistant U.S. Attorney, Criminal Fraud Section
Louisville, Kentucky

and

Kenneth J. Tuggle
Frost Brown Todd LLC
Louisville, Kentucky

Copyright 2002, Marisa J. Ford and Kenneth J. Tuggle

SECTION D



PROTECTING AGAINST CYBERCRIME

Protecting against cybercrime requires physical security, computer security and network security, robust systems, constant vigilance and persistent diligence. Cybercrime is not just a hardware problem or a software problem, it is a people problem too. Cybercrime threats are real and can cause significant damage if left uncontained. However, planning and prevention can do much to help you contain them. And the public and private domains hold significant resources to buttress your containment efforts.

THREATS

What threats exist and what resources are available to combat them? Probably the most common type of malicious software (“malware”) is the **virus**, a piece of code that enters your machine secretly, often as an email attachment or a download. Traditional viruses replicate within a machine, but need human intervention to spread. Newer malware, including Trojan horses (“**Trojans**”) and **worms** allow attacks of even greater scope.

Trojans infiltrate your machine and wait for an opportune time to open the city gates. A Trojan listens on a designated network port and waits for an external program to activate it, then takes control of the machine. Unlike viruses, Trojans do not replicate themselves.

Worms, conversely, do replicate, but unlike traditional viruses, worms do not need user assistance to move from machine to machine. Worms ride in on email attachments, word macros and other innocent looking code. Today, people are wary of email attachments they didn't request because an unfortunate number of attachments have contained viruses, worms, or other malware.

Defensive Devices

Fortunately, a number of defensive devices exist to help keep you safe and protected. **Anti-virus software** is one such device. Provided that its virus definitions are properly and frequently updated, anti-virus software will catch many known threats. In addition, you should consider a **firewall** of some sort. Firewalls are implemented in either software or hardware. You should periodically check for **downloadable patches** for your operating system and software at your vendors' website. Patches only remedy known flaws vulnerabilities. New vulnerabilities are constantly being uncovered. And, hackers seek them out through port scanning. Good fire walls can defeat such scans. **Configuration checks** are the next line of defense. Net browsers have a multitude of security settings that define which kinds of code can run, which sites can receive information from your cookies, etc. Programs exist to test your settings to find out how to fix them: e.g., Qualys's Free Browser

Checkout (<http://browsercheck.qualys.com>). Windows users can also try Microsoft Baseline Security Analyzer, a free download from Microsoft Technet that scans your system looking for misconfigured settings. Last, software and hardware firewalls exist to close off systems to scanning and entry. See PC Magazine, November 19, 2002, pgs. 99-112. Also see PC Magazine, November 19, 2002, pgs. 117-130. The earlier article deals generally with software firewalls. The second deals with small office security appliances.

Apart from these hardware and software defensive devices, you can adopt and execute a defensive strategy.

Defensive Strategies

Executing a defensive strategy involves at least six steps:

Preparation Evaluation Containment Eradication Recovery and Learning.

Preparation

Of these the most important is preparation. In accordance with near-universal principles, incidents always occur at the worst possible time. They result in confusion that is not conducive to intelligent decision making. You must already have a plan in place.

Before any incidents occur, form a Computer Security Incident Response Team (“CSIRT”) with the needed training, expertise and authority to handle problems. Usually, a CSIRT contains several groups: on-site groups to

implement responses at the affected locations; and a central command team to coordinate the action. Team members need to know exactly what their individual roles will be in the case of an incident and be prepared to execute them.

The CSIRT should include executive level management representatives who can understand the corporate ramifications of various decisions and can approve shutting down core business systems when needed. The CSIRT may also need a public relations specialist to act as the main contact with the press to help the company make the best public presentation, especially if it is publically traded. The CSIRT may also include a database administrator and a good programmer to craft any custom forensic tool needed for a precise analysis. Last, the CSIRT needs a project manager who can effectively coordinate the actions of all the technical members of the team. One member of the team must be designated as the central contact.

Prepare a Draft Incident Response Plan containing carefully thought-out checklists detailing the exact actions to take for each type of attack. The incident response plan also should outline the company's goals and objectives for handling incidents; its guidelines for determining the seriousness and impact of an attack; a reference detailing who should notify whom when an attack is in progress; information about any legal issues to be aware (of); a statement of any

rules one needs to follow for handling the labeling of evidence; and templates for keeping detailed records of everything that happens and every measure that is taken in response to the attack. Obviously, the plan must be based on thorough knowledge of the company's critical servers and applications and the business impact of lost, exposed or unavailable data. Have the plan approved by top management. Then, make sure each member of the CSIRT has a copy of the incident response plan and a call list with contact information for each team member, regularly updated.

Test the Plan and Keep It Updated. Find any gaps in it and mend them. Use any actual security incidents to improve the plan.

Develop a Support System. Identify and cultivate the right contacts at your local law enforcement agency and your internet service provider. Discuss with your local law enforcement contacts how to handle evidence that may be needed in court. Consult your ISP about how to collect any relevant data from its logs. You will need to provide date, time zone, time and activity data to help your ISP identify.

Evaluation

Evaluating an incident means detecting it, making a preliminary determination of its scope and initiating the response plan. Identify The Incident. Did an actual intrusion occur (or is it occurring)? Determine The

Scope Of The Incident. Is one system involved or multiple ones? One site or several? Is valuable information affected? Try to identify the intruder's entry point into your system.

Before taking any action Alert The CSIRT to avoid damage from inappropriate responses by the organization's own personnel that might leave systems unsecured, destroy evidence, etc. Start An Incident Log: a comprehensive, chronological recording of all observations, actions, which actors acted, where and why.

Containment

Secure the Area to limit the damage as much as possible. Backup Affected Systems before altering them to preserve evidence for analysis and prosecution. Examine all Systems Logs for clues and analysis. Disconnect the Affected Systems from the Network to prevent the problem from spreading or recurring.

Eradication

Analyze the Attack. Where did it come from and how was it executed? Protect the Systems. Place your fire wall in a new location. Move some systems to new IP addresses. Add new software or install OS patches, but do not reconnect any affected systems to the network until you know you can

prevent another intrusion. Clean Up the Mess by removing viruses or reinstalling the system from scratch, and restoring lost or contaminated data.

Recovery

Restore Affected Systems from backups or from scratch. Install the latest software patches when you do. Continue Monitoring for additional attacks.

Learning

Prepare an Incident Report soon after an attack while the information is fresh. Include the lessons learned, identify the known costs and summarize findings for management. Evaluate how your CSIRT teams performed. Implement changes to be better prepared to repel or avoid the next attack.

Other Threats

Consider some potential sources of attack. A PriceWaterhouseCoopers survey suggested that the greatest threat was from insiders such as current and former employees, on-site contractors, consultants and OEM's, vendors, suppliers and even strategic partners. Other potential threats come from "outsiders" such as hackers or "crackers," competitors, shareholders/speculators, the media and Governments, e.g. Echlon and Carnivore.

Many companies fail to plug well known technological holes which account for a great number of the successful break-ins. The SANS Institute

(Cert.org) is a center of Internet Security Expertise located at the Software Engineering Institute operated by Carnegie Mellon University. Among other things, it tracks security holes in operating systems, e-mail browsers and other common software. More specifically, CERT/CC studies internet security vulnerabilities, provides instant response services to sites that have been the victims of attack, publishes a variety of security alerts, does research in wide area network computing and develops information and training to help companies improve security at their sites. Treat yourself to a visit to the SANS Institute website at cert.org.

Also, consider denial of service (“DoS”) attacks. A DoS attack “floods” a network with bogus information or information requests that prevents legitimate network traffic thereby disrupting connections between two machines, preventing access to service or preventing a particular individual from accessing a service or disrupting service to a specific system or person. However, service overloading and message flooding are but two of several ways that DoS attack may occur.

Writing in the Richmond Journal of Law and Technology, Jeff Nemerofsky states:

There are several ways a denial of service attack may occur—service overloading and message flooding are but two –and these attacks may be directed against either a user, a host computer, or a network. These

attacks have a vernacular all their own and can be categorized as “fork bombs,” “malloc bombs,” “SYN flood” and “mail bombs,” with specific names such as “Ping of Death,” “Teardrop,” “Boing,” “New Tear” and “IceNewk.” For instance, one attack paints a huge black window on the user’s screen in such a way that the user can no longer access the remainder of their screen.

6 J.L. & Tech. 23 (Spring 2000)

REMEDIES

The Computer Fraud And Abuse Act

In response to these and other threats, Congress enacted the first Computer Fraud and Abuse Act in 1984 and has amended it from time to time thereafter, in 1986, 1994 and 1996. In its present form, the Act provides:

(a) Whoever—(5)(A) through means of a computer used in interstate commerce or communications, knowingly causes the transmission of program, information, code, or command to computer or computer system if- (i) the person causing the transmission intends that such transmission will- (I) damage, or cause damage to, a computer, computer system, network information, data, or program; or (II) withhold or deny, or cause the withholding or denial, of the use of a computer, computer services, system or network, information, data, or program; and (ii) the transmission of the harmful component of the program, information, code, or command- (I) occurred without the authorization of the persons or entities who own or are responsible for the computer system receiving the program, information, code, or command; and (II)(a) causes loss or damage to one or more other persons of value aggregating \$1,000 or

more during any 1-year period; . . . shall be punished .

...

In 1998, Robert Morris, a 23 year old first year graduate at Cornell University's Computer Science program created a computer program later known as the internet "worm" or "virus." Morris intended to release the worm into university, government or military computers around the country to demonstrate the inadequacies of the then current security measures. However, after releasing his worm, Morris discovered it was actually infecting many other machines eventually causing computers at over 6000 educational institutions and military sites around the country to cease functioning. *U.S. v. Morris*, 928 F.2d 504 (2nd Cir. 1991)

Morris was prosecuted and found guilty of violating the Computer Fraud and Abuse Act, Section 1030 (a)(5)(A) which prohibited intentional, unauthorized access to federal computers and sentenced to three years probation, four hundred hours of community service, fined \$10,500 and the cost of his supervision. *Id.* at 506

Morris claimed that the statutory language "intentionally accesses a Federal interest computer without authorization, and by means of one or more instances of such conduct, alter, damages, or destroys information in any such Federal interest computer, . . ." required the Government to prove that he intentionally accessed the Federal computer and intentionally altered

information or prevented its use. The 2nd Circuit agreed with the District Court that the intent required applied only to the act of accessing the system, not the alteration of information or prevention of authorized use, and let Morris' convictions stand. *Id.* at 510-11.

In 1994, Congress amended the 1986 Computer Fraud and Abuse Act to broaden the Federal laws that related to computer "worms" and "viruses." Coverage of the Act was expanded to include computers used in interstate commerce. The requirement of an unauthorized access was removed so that company insiders and authorized users could be held liable and certain types of reckless conduct and intentional acts were deemed criminal.

Then in 1996, Congress further expanded the 1994 act to include computers in the private sector, called protected computers, as well as those in the government domain. Today, the 1999 statute covers protected computers, or computers no longer strictly under government domain.

Not unexpectedly, America Online, Inc. has been involved in a number of cases involving the Computer Fraud and Abuse Act and other statutes. For example, in *America Online, Inc. v. LSGM, Inc., et al.*, 46 F.Supp. 2nd 444 (E.D.Va. 1998), AOL sued website operators and their principals alleging that they sent unauthorized and unsolicited bulk e-mail advertisements to AOL customers. The district court held that the operators' use of providers' internet

domain name violated Lanham Act prohibitions on false designations of origin, operators' use of domain name constituted dilution and operators violated Computer Fraud and Abuse Act and the Virginia Computer Crimes Act. Moreover, the operators' conduct amounted to trespass to chattels under Virginia law. Specifically, AOL estimated that defendants in concert with their "site partners" transmitted more than 92 million unsolicited and bulk e-mail messages advertising their pornographic websites to AOL members from approximately June 17, 1997 to January 21, 1998. Indeed, defendants admitted that they sent approximately 300,000 e-mail messages a day at various intervals from their Michigan offices. Further, defendants admitted to maintaining AOL memberships to harvest or collect e-mail addresses of other AOL members, to using the AOL Collector and e-mail Pro/Stealth Mailer extractor programs to collect e-mail address of AOL members and to using software to evade AOL's filtering mechanisms. Defendants also forged the domain information "aol.com." in the address line of e-mail messages sent to AOL members and committed a number of other violations of AOL's Terms of Service.

According to the court, the defendants violated 18 U.S.C. §1030(a)(2)(C) of the Computer Fraud and Abuse Act which prohibits individuals from "intentionally accessing a computer without authorization or exceeding authorized access, and thereby obtaining information from any protected

computer if the conduct involved interstate or foreign communication.” Also, defendants exceeded authorized access in violating the Computer Fraud and Abuse Act. Similarly, defendants impaired computer facilities by their conduct in violation of the Computer Fraud and Abuse Act damaging AOL’s computer network, reputation and good will. Also see *Cyber Promotions, Inc. v. America Online, Inc.*, 948 F.Supp. 436 (E.D. Pa. 1996); *America Online, Inc. v. National Healthcare Discount, Inc.*, 121 F.Supp. 2nd 1255 (N.D. Iowa 2000); *America Online, Inc. v. Greatdeals.net, et al.*, 949 F.Supp. 2nd 851 (E.D. Va. 1999); and *America Online, Inc. v. IMS, et al.*, 24 F.Supp. 2nd 548 (E.D. Va. 1998).

CONCLUSION

As this short discussion shows, defensive devices, defensive strategies and network and computer security are vital steps to protect oneself from hackers, crackers, snoopers, downloaders, tamperers, spoofers, jammers or flooders and virus mongers. Here, an ounce of prevention is worth many pounds of cure.

Also, legal remedies exist. The Computer Fraud and Abuse Act as presently drawn provides both civil and criminal protection and remedies against people who violate it in any of the several ways the Act forbids. The USA Patriot Act allows one to seek the assistance of law enforcement authorities and, in appropriate circumstances, permits them to enlist the

assistance of internet service providers. Finally, where theft of trade secrets are at issue, the Economic Espionage Act can provide a remedy.

Mr. Kenneth J. Tuggle
Frost Brown Todd LLC
400 W. Market Street, 32nd Floor
Louisville, Kentucky 40202-3363
(502)568-0269

revised 10/31/2002 3:43 PM
025:pw/skn
LOUIMDMS/201908.1



CYBER-TERRORISM
&
CRITICAL
INFRASTRUCTURE
PROTECTION

MARISA J. FORD
 DEPARTMENT OF JUSTICE
 U.S. Attorney's Office
 Western District of Kentucky



AGENDA

- What is "Cyber-Terrorism" and Critical Infrastructure Protection?
- Applicable Federal Statutes
- National Security Law Issues and Information Sharing



WHAT IS THE CRITICAL
INFRASTRUCTURE

- We use portions of our infrastructure to:
 - communicate
 - manage industrial activities
 - conduct business
 - perform scientific research
- Portions of our infrastructure are considered critical to the day-to-day functioning and the safety and well-being of society





WHAT IS THE CRITICAL INFRASTRUCTURE

- Critical Infrastructure:
 - Telecommunications
 - Banking and Financial Systems
 - Electrical Power Grids
 - Oil and Gas Pipelines
 - Transportation Networks
 - Water Distribution Systems
 - Emergency Services
 - Government Operations
 - Medical and Health Care
 - Food Supply



CRITICAL INFRASTRUCTURE PROTECTION

- Prevent conventional criminals, terrorists, hostile nation-states from interrupting these services
- Prepare and assist in the reconstitution of systems that are downed or attacked
- Investigate attacks on the critical infrastructure



WHAT IS CYBER-TERRORISM?



WE KNOW WHAT CONVENTIONAL TERRORISM LOOKS LIKE.



WHAT IS CYBER-TERRORISM?

WHAT WOULD AN ACT OF CYBER-TERRORISM LOOK LIKE?

WE DON'T KNOW.

AND HOPEFULLY WE WON'T FIND OUT.



CYBER-TERRORISM & CIP: SHOTS ACROSS THE BOW

- 1997 Cyber Attack on Florida 911 System
- 1998 "Solar Sunrise" intrusions into over 500 gov't installations, military, and civilian systems
- 1998 Telephone Switch Hack closes an Airport
- 2001 Hackers protesting U.S./China conflict enter US electrical power systems
- Recent worms



WHAT IS CYBER-TERRORISM?

- Cyber-Terrorism Is Distinct from other computer crime
- Cyber-Extortion
 - Many cases involving financial institutions and e-commerce retailers
- Cyber-Espionage
 - Attempts to exploit access to vulnerable networks for intelligence purposes
- Other Malicious "Hacking"
 - Many institutions are the subject of malicious hacking



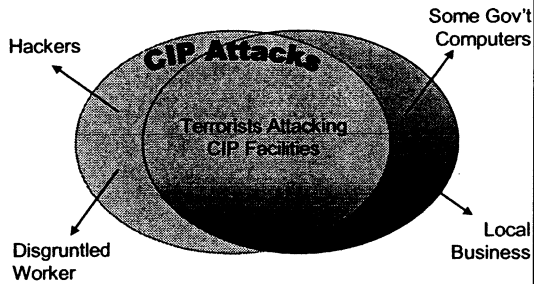


DEVELOPING A DEFINITION OF CYBER-TERRORISM

- Based on 18 U.S.C. 2331:
 - An act involving use of a computer;
 - That is dangerous to human life;
 - That is intended to:
 - intimidate or coerce a civilian population; or
 - influence the policy of a government by coercion or intimidation
 - 2332b(G)(5)(B) limits this to certain 1030 offenses.



CIP AND CYBER-TERRORISM





FEDERAL STATUTES IN CIP/CYBER-TERRORISM CASES





**FEDERAL STATUTES IN
CIP/CYBER-TERRORISM
CASES**

- Terrorism Statutes
 - 18 U.S.C. 2332b
- Computer Intrusion Statutes
 - 18 U.S.C. 1030(a)(5)
- RICO Statute
 - 18 U.S.C. 1961
- Threat
 - 18 U.S.C. 875(c)
- Sentencing Guidelines
 - 3A1.4



**ACTS TRANSCENDING
NATIONAL BOUNDARIES
18 U.S.C. 2332B**

- An offense under 2332b must:
 - be an act that "transcend[s] international boundaries" and
 - Kills, maims any person within the United States; or
 - creates a substantial risk of serious bodily injury to another person by destroying or damaging any structure, conveyance, or other "real or personal property" in the U.S. in violation of State or U.S. law.
- Includes threats, attempts, and conspiracies
- Death eligible or 25 years



**ACTS TRANSCENDING
NATIONAL BOUNDARIES
18 U.S.C. 2332B**

- An offense under 2332b must:
 - be an act that "transcend[s] international boundaries" and
 - Kills, maims any person within the United States; or
 - creates a substantial risk of serious bodily injury to another person by destroying or damaging any structure, conveyance, or other "real or personal property" in the U.S. in violation of State or U.S. law.
- Includes threats, attempts, and conspiracies
- Death eligible or 25 years

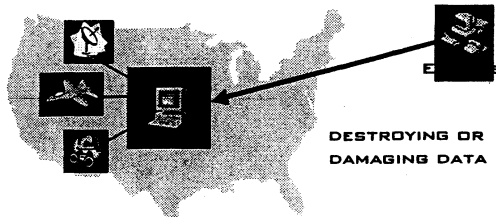


**ACTS TRANSCENDING
NATIONAL BOUNDARIES**
18 U.S.C. 2332B

- An offense under 2332b must:
 - be an act that "transcend[s] international boundaries" and
 - Kills, maims any person within the United States; or
 - creates a substantial risk of serious bodily injury to another person by destroying or damaging any structure, conveyance, or other "real or personal property" in the U.S. in violation of State or U.S. law.
- Includes threats, attempts, and conspiracies
- Death eligible or 25 years

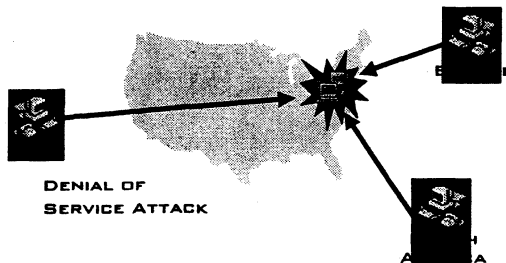


**ACTS TRANSCENDING
NATIONAL BOUNDARIES**
18 U.S.C. 2332B





**ACTS TRANSCENDING
NATIONAL BOUNDARIES**
18 U.S.C. 2332B





**ACTS TRANSCENDING
NATIONAL BOUNDARIES**
18 U.S.C. 2332B

- Limitations of section 2332b
 - Is erasing or altering data damage or destruction of "real or personal property"?
 - Does the "damage" have to be direct or does foreseeable resulting damage count?
 - Is a Denial-of-Service attack damage to "real or personal property"?
 - Must be an international incident



COMPUTER INTRUSION
18 U.S.C. 1030(A)(5)(A)(iii)

- Knowingly causes transmission of program, info, code, command, and intentionally causes damage without authorization to a "protected computer," and
 - loss to 1+ persons or affecting 1+ "protected computer" aggregating to at least \$5,000.
 - Impairment of medical exam, diagnosis, treatment, or care of 1+ person.
 - Physical injury to any person.
 - a threat to public health or safety.
 - Damage affecting a computer system used by a gov't entity for administration of justice, national defense, or national security.



RICO STATUTE
18 U.S.C. 1961 ET. SEQ

- Certain 1030 offense are now RICO predicates
- 1030 offenses where damage is:
 - Impairment of medical exam, diagnosis, treatment, or care of 1+ person
 - Physical injury to any person
 - a threat to public health or safety
 - Damage affecting a computer system used by a gov't entity for administration of justice, national defense, or national security
- A terrorist group that is a RICO enterprise and conducts its business through a pattern of acts of cyber terrorism is subject to prosecution under RICO



THREATS
18 U.S.C. 875(c)

- Whoever transmits in interstate or foreign commerce any communication containing any threat to kidnap any person or any threat to injure the person of another, shall be fined under this title or imprisoned not more than five years, or both.



SENTENCING GUIDELINES
3A1.4

- §3A1.4. TERRORISM:
 - (a) If the offense is a felony that involved, or was intended to promote, a federal crime of terrorism, increase by 12 levels; but if the resulting offense level is less than level 32, increase to level 32.
- Application Note 1:
 - The offense level increases if the offense involved, or was intended to promote, a federal crime of terrorism. "Federal crime of terrorism" is defined at 18 U.S.C. § 2332b(g)



SENTENCING GUIDELINES
3A1.4

- This provision should be used judiciously...



- See US v Leahy, 169 F.3d 433 (7th Cir.)



NATIONAL SECURITY LAW
ISSUES



NATIONAL SECURITY
POLICY

- Missteps in the past have resulted in limits being placed on use of intelligence authorities
- Law, Policy, and Regulation control how information can be used and shared
- Some of those were relaxed as a result of the USA PATRIOT Act
 - FISA and Title III Limitations
 - Information Sharing



FOREIGN INTELLIGENCE
SURVEILLANCE ACT
50 U.S.C. 1801 ET SEQ.

- FISA v. Title III
 - FBI's National Security Division v. Criminal Investigations Division
 - Not a 4th Amendment search requiring "Probable Cause"
 - Obtained from the FISA Court at Main Justice
 - Restrictions on use for criminal investigations
 - Oversight by Office of Intelligence Policy and Review (OIPR)





FISA AND TITLE III

- Restrictions on disclosure and use of FISA information
 - "Primary Purpose" Test
 - July 1995 FISA Guidelines
- Restrictions on Use of Title III information for intelligence purposes
 - 2000 OLC Opinion



FISA AND TITLE III

- "Significant Purpose" is to gain foreign intelligence.
- 18 USC 2517 now states:
 - Any investigative or law enforcement officer, or attorney for the Government, may disclose such contents to any other Federal law enforcement, intelligence, protective, immigration, national defense, or national security official to the extent that such contents include foreign intelligence or counterintelligence



FISA AND TITLE III

- How will these issues come up?
 - FISA Authority is being used by FCI agents just like Title III wiretaps are used by CID agents
 - Increasingly, national security and criminal investigations are going to intersect
 - May need to share Title III info
 - Internal Security Section at Justice oversees criminal use of the FISA statute



INFORMATION SHARING



- FISA and Title III Information
- Grand Jury
- Duty to turn over any Foreign Intelligence Information



INFORMATION SHARING
GRAND JURY MATERIAL

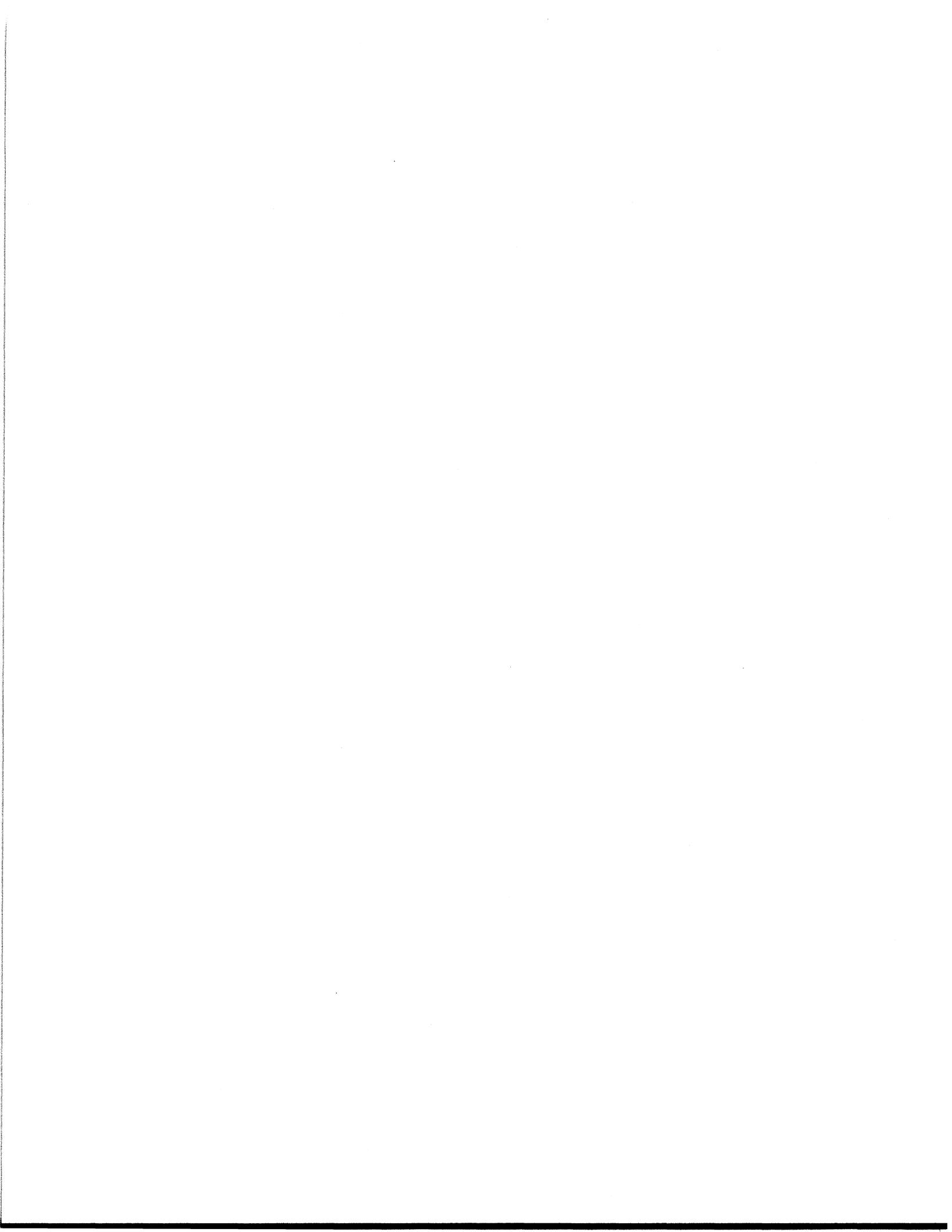
- May disclose to federal law enforcement, intelligence, protective, immigration, national defense, or national security officials in performance of his official duties when matters involve foreign intel or counterintel. FRCP 6(c)(i)(v)
- Must file notice that information was disclosed and the entities to which disclosure was made. FRCP 6(c)(ii)



**WE'RE FROM THE
GOVERNMENT, WE'RE
HERE TO HELP YOU.**



- U.S. Attorney's office: (502) 582-5930
- E-Mail: marisa.ford@usdoj.gov



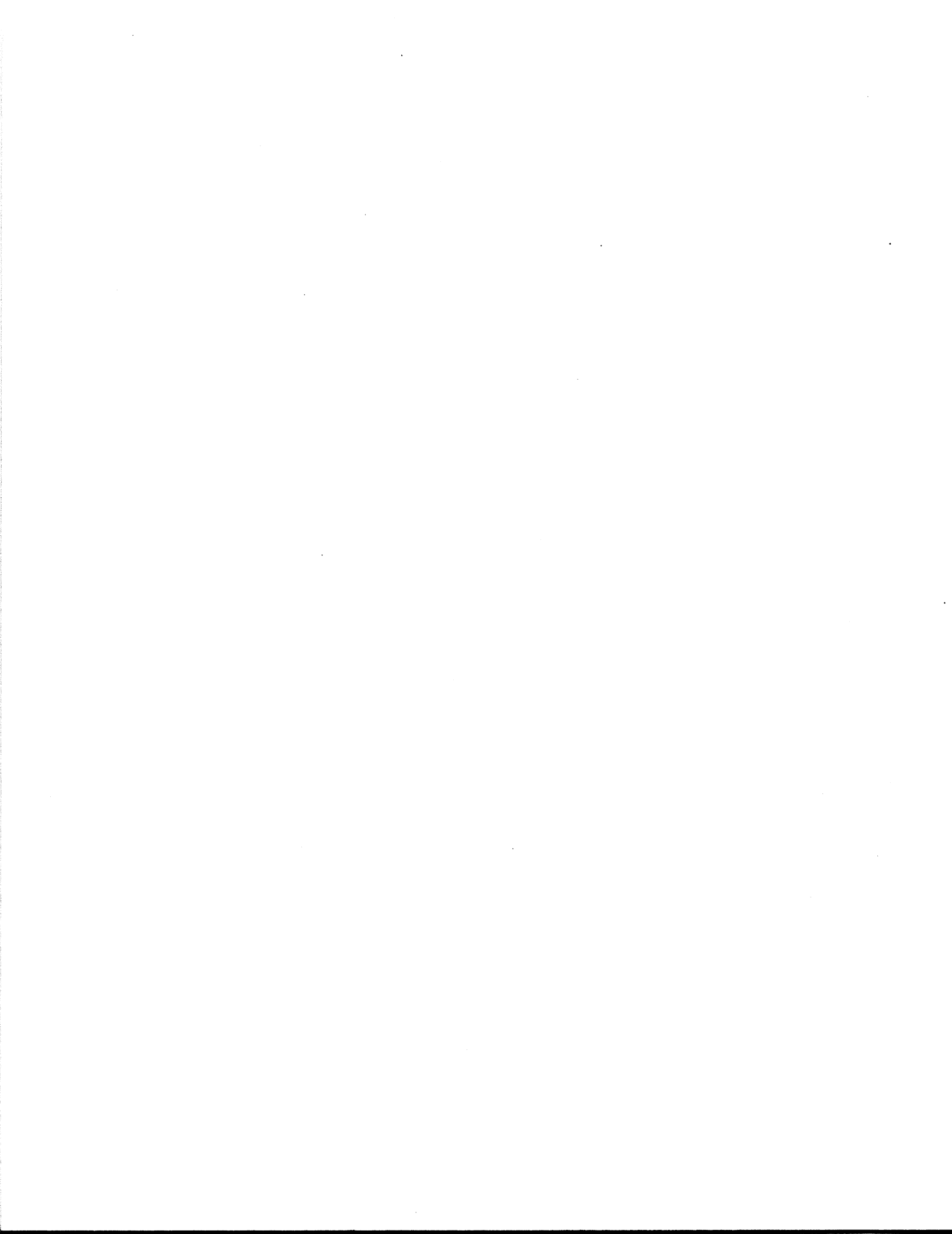
**FINANCING ISSUES AND INTELLECTUAL PROPERTY
DEVELOPMENT:**

The Intersection Between Credit and Property Rights

*Raymond T. Nimmer
Leonard Chiles Professor of Law
University of Houston Law Center
Houston, Texas*

Copyright 2002, Raymond T. Nimmer

SECTION E



COMMERCIAL FINANCE LAW
&
INTELLECTUAL PROPERTY

Raymond T. Nimmer
Leonard Childs Professor of Law
University of Houston Law Center

(Adapted from Nimmer & Dodd, Licensing Law (to be published 2003 West Publ.))
All Rights Reserved

Table of Contents

| | | | |
|---|--|-------------|-------------|
| I. | Introduction... | E-1 | |
| II. | Sources of Credit Law for Information Assets..... | E-1 | |
| | [1]. Federal Property Rights Systems: State Law Interface | E-2 | |
| | [2]. State Law Systems: Revised Article 9 and Other Law | E-3 | |
| III. | Defining the Collateral or Asset | E-5 | |
| | [1]. Statutory Nomenclature and Classification | E-6 | |
| | [2]. Software, Computer Programs, Data and the Like | E-8 | |
| PART A. SECURED LENDING AND | | | |
| INTELLECTUAL PROPERTY RIGHTS AS ASSETS | | | E-11 |
| IV. | Scope of Article 9: Intellectual Property Rights | E-11 | |
| | [1]. General Application of Article 9: Security Interest | E-11 | |
| | [i]. Personal Property | E-12 | |
| | [ii]. Security Interest | E-13 | |
| | [2]. Application of Particular Article 9 Rules: Partial Exclusions | E-14 | |
| V. | Creating a Security Interest: Intellectual Property Rights | E-16 | |
| | [1]. Required Writing and Description | E-16 | |
| | [2]. New Developments and Technology | E-17 | |
| VI. | Filing, Perfection and Registration: Intellectual Property Rights | E-19 | |
| | [1]. Nature of the Options | E-20 | |
| | [2]. Criteria for Preemption | E-21 | |
| | [3]. Copyrights | E-22 | |
| | [4]. Patents | E-25 | |
| | [5]. Trademarks | E-28 | |
| | [6]. Trade Secrets | E-29 | |

| | | |
|--------------|--|-------------|
| VII. | Priority Issues: Intellectual Property Rights | E-30 |
| | [1]. Underlying Ownership Rules and Priority | E-31 |
| | [2]. Priority Among Transfers | E-32 |
| | [i]. Copyrights | E-33 |
| | [ii]. Patents and Federal Trademarks | E-34 |
| VIII. | Enforceability Issues: The Nature of the Rights | E-37 |
| | [1]. Trade Secrets | E-38 |
| | [2]. Trademarks | E-38 |

PART B. LICENSES AND OTHER CONTRACTS AS COLLATERAL**E-39**

| | | |
|-------------|--|-------------|
| IX. | Character of Contract-Based Financing | E-39 |
| X. | Licensor's Interest as Collateral: Cash Flow from Contracts | E-40 |
| | [1]. What Law Applies: Federal Law | E-40 |
| | [2]. What Law Governs: State Law | E-42 |
| | [3]. Perfecting an Interest | E-44 |
| | [4]. Contractual Restrictions on Transferring Cash Flow | E-44 |
| XI. | Licensee Interest: Licensed Rights as Collateral | E-45 |
| | [1]. Assignability in General | E-45 |
| | [2]. Revised Article 9: Creating Interests in Licensee Rights | E-46 |
| XII. | Priority Issues and Licenses | E-48 |

PART C. BANKRUPTCY ISSUES**E-51**

| | | |
|--------------|---|-------------|
| XIV. | Rights and Goodwill As Assets | E-51 |
| XV. | Sales of Rights in Bankruptcy | E-54 |
| XVI. | Contract Rights: General | E-56 |
| XVII. | Executory Contracts | E-56 |
| | [1]. Licenses as Executory Contracts: Generally | E-56 |
| | [2]. Effect of Bankruptcy Termination Clauses | E-58 |
| | [3]. Employment Contracts | E-58 |
| | [4]. Non-Competition Agreements | E-58 |
| | [5]. Assumption of Licensee's Interest in License | E-59 |
| | [6]. Effect of Rejecting a License in a Licensor Bankruptcy | E-61 |
| | [7]. Royalties to be Paid To Retain Rights | E-61 |
| XVI. | Debtor's Use of Licensed IP After Filing Bankruptcy | E-62 |
| XIX. | Automatic Stay | E-63 |
| XX. | Infringement Actions | E-64 |

Commercial Finance Law and Intellectual Property

Raymond T. Nimmer
Leonard Childs Professor of Law
University of Houston Law Center

(Adapted from Nimmer & Dodd, Licensing Law (to be published 2003 West Publ.))
All Rights Reserved

I. Introduction

The information age heightens the value of informational assets. This affects what are the ordinary focal points for credit transactions. There result a number of issues about how credit law interacts with these new assets.

This paper focuses on secured lending relating to informational subject matter and concludes with a brief overview of selected bankruptcy issues. We will not deal with the full details of secured financing law or with consumer credit legislation. Rather, we focus on several significant legal issues in this and in related forms of financing.¹ This is a context in which significant questions lack clear answers and which, like many topics in licensing law, is experiencing significant change. Many of the difficult issues entails resolving conflicts between federal and state law which, for purposes of financing transactions often take diametric approaches. Currently, the most significant changes are in the enactment of a complete revision of UCC Article 9, and in promulgation of new standards for lease and unsecured financing in UCITA.

II. Sources of Credit Law for Information Assets

Credit financing here is characterized by two conceptually difficult characteristics. One relates to practice issues, while the other relates to an interaction between federal and state law.

As a matter of practice, asset-based financing in intellectual property and related fields often follows different traditions and terminology than other types of financing. Some of this involves the use of terminology and techniques associated with conveyancing. While

¹ In addition to the questions addressed in this chapter, which deal primarily with creating, perfecting and obtaining priority in an interest, there are issues regarding foreclosure that we do not discuss here. These issues have generated virtually no litigation in intellectual property law. As a general matter, foreclosure is governed under state law, Article 9 of the UCC, although the results of foreclosure proceedings must conform to federal intellectual property law transfer rules when applicable. See *Lilly v. Terwilliger*, 796 P2d 199 (Mont. 1990). See also *Chesapeake Fiber Packaging Corp. v. Sebro Packing Corp.*, 143 Bankr. 360 (D. Md. 1992) (assignment of patent application permitted further assignment in the event of termination for material breach as part of financing arrangement). Because of massive changes in foreclosure law under new Article 9, anyone involved in this field must re-evaluate their forms and procedures.

other fields of asset-based financing have used Article 9 terminology of “security interest” since the mid-1960’s, it remains common to describe some intellectual property financing agreements as “conditional assignments.” The form of agreement may nominally entail an assignment with a condition subsequent, reverting the asset back to the assignor in the even of breach (e.g., non-payment or the like).² The assignor in such structure is often the lender and, thus, the entire deal may involve an initial transfer to the lender with a conditional assignment back.

Other financing issues are handled differently in the information asset area than in other contexts because of substantive differences in the recording systems and in the underlying substantive property law. This includes, for example, rules in trademark law that prohibit “assignments in gross” and raise questions about whether a security interest offends that substantive law rule.³

Beyond terminology issues, then, there is a fundamental structural problem. Secured lending is governed by an interaction of federal and state law, but the contours of what is governed by federal and what issues are governed by state law are not clear.⁴ This problem arises most often in transactions associated with “federal intellectual property”, such as copyright, patent, and federal trademarks. Pure trade secret and state law trademark financing in concept does not present a federal-state issue.⁵

[1]. Federal Property Rights Systems: State Law Interface.

The primary federal intellectual property rights systems (copyright, patent, trademark) do not contain extensive coverage of toward asset-based financing, although the statutes may contain references to “mortgages” or security interests.⁶ Yet, each of the statutory systems does contain substantive rules that affect the use of intellectual property assets as the subject matter of asset-based financing. In cases of conflict, of course, these federal rules prevail over contrary state law rules. The difficulty comes in determining when a conflict exists and whether the conflict creates a preemptive, rather than a parallel rule system.

² See Raymond T. Nimmer, *Commercial Asset-Based Financing* (1988). See also *Chesapeake Fiber Packaging Corp. v. Sebro Packing Corp.*, 143 Bankr. 360 (D. Md. 1992) (assignment of patent application permitted further assignment in the event of termination for material breach as part of financing arrangement).

³ See *Roman Cleanser Co. v. National Acceptance Co.*, 802 F2d 207 (6th Cir. 1986) (holding that a security interest in a trademark was not an assignment in gross). See generally McCarthy on Trademarks § 18.7.

⁴ See, e.g., *Muldo v. Matsco (In re Cybernetic Servs., Inc.)*, 52 USPQ 2d 1693 (9th Cir. BAP 1999); *Broadcast Music Inc. v. Hirsch*, 41 USPQ2d 1373 (9th Cir 1997); *In re Avalon Software, Inc.*, 209 BR 517 (Bankr. D. Ariz. 1997); *In re Peregrine Entertainment, Ltd.*, 116 Bankr. 194 (CD Cal. 1990).

⁵ Determining when or whether the trade secret financing is purely a state law issue is not always a straightforward question. If, for example, a trade secret is embodied in a writing in a form that creates a copyrightable work, arguably there are two distinct rights based claims in this asset (confidentiality of information, copyright exclusive rights). See, e.g., *In re Avalon Software, Inc.*, 209 BR 517 (Bankr. D. Ariz. 1997).

⁶ For example, the Copyright Act defines a “transfer of copyright ownership” to include: “an assignment, mortgage, exclusive license, or any other conveyance, alienation, or hypothecation of a copyright or of any of the exclusive rights comprised in a copyright, whether or not it is limited in time or place of effect, but not including a nonexclusive license.” 17 USC § 101. Section 261 of the Patent Act also refers to mortgages in reference to its priority of rights rules. 35 USC § 261.

The points of potential conflict include the following issues:

- The federal statutes contain *registration or recording rules* premised on a property-law focus on the property as the organizing features of the records-keeping system, rather than focusing on a party-based approach focus as in Article 9 on secured financing. The issue is to what extent federal filing rules over-ride state law rules as applied to security interests and, to the extent that they do, how does a lender or other party reconcile two functionally different filing systems in an efficient manner?
- The federal statutes contain *priority rules* based on a different conceptual structure than that used to resolve priority of rights issues under state credit laws, including Article 9. The issue created is to what extent the priority of rights rules in the federal statutes over-ride the different rules in state law?
- The federal statutes and case law establish standards for *creating enforceable transfers* of intellectual property. These differ from rules associated with other types of asset-based financing collateral, especially goods. The issue concerns how these different standards interact with state law rules about creating enforceable security interests?
- Federal law places limits on *what rights are transferred* and what rights are withheld in ordinary transactions (e.g., non-exclusive licenses). The questions are to what extent these rules defeat ordinary forms and formats of secured lending under state law.

[2]. State Law Systems: Revised Article 9 and Other Law

The dominant, relevant state law applicable to financing assets is Article 9 of the Uniform Commercial Code. Article 9 covers all secured lending in personal property with several defined exceptions that are not relevant here.⁷ Effective in July, 2001, a new substantially revised version of Article 9 became effective in most states, working significant changes in applicable law relevant to intangibles financing. For purposes of this discussion, we treat the uniform version of Article 9 in existence before 2001 as the “original” Article 9, and the 2001 revision as “revised” Article 9.

Article 9 relies on a single concept of “security interest” that covers a range of previously differently described financing frameworks.

- Although the term “security interest” ordinarily refers to a lending transaction, the scope of Article 9 is not limited to transactions that are formally described as loan

⁷ The exceptions differ between what we here describe as “original Article 9” and the 2000 version, which we here describe as “revised Article 9. See UCC § 9-104 (Original); UCC § 9-109 (Revised).

transactions – substance controls over form. A conditional assignment that entails a secured loan transaction in fact will be treated as a security interest.

- “Security interest” is broadly defined in the UCC as any property right taken to assure the performance of any obligation by the other party.⁸
- Additionally, Article 9 applies to sales or absolute assignments of certain intangible assets, such as accounts and payment streams associated with other assets. Under revised Article 9, this picks up many transactions in which payment (royalty) streams are transferred for current value, whether by way of a lien or by way of an assignment.

Article 9 contains elaborate priority and other rules, many of which are relevant to information-based financing, but uses a simplified system of recording and simplified rules for creating a security interest with minimal formalities. Both were changed from prior law by transition to Revised Article 9.

- The primary place to file and, thus, perfect, a security interest is the debtor’s location.⁹ The rule governs, of course, only to the extent that federal law does not require filing (recording or registration) in a different location.

Among the many changes made by revised Article 9 were numerous changes targeted to licensing and intellectual-property. The reason stems from a confluence of simple facts. First, a goal of Article 9 was to expand the maximal availability of commercial values for use for asset-based financing.¹⁰ This supposedly frees up value to provide capital and other support for business. Second, intangible assets have become important forms of value in the modern economy. Thus, the law revision focused in part on these assets.

As we discuss later, there are many contexts in which this effort appears in the language of Revised Article 9. These include:

- Redefining the term “account” to include contractual rights to payment coming from a license and, thus, covering virtually all transactions in such payment rights.¹¹
- Invalidating in part contract terms that prohibit transfer of a payment (royalty) stream.

⁸ UCC § 1-307(37) (1990 Official Draft).

⁹ UCC §§ 9-301; 307 (Revised).

¹⁰ Interestingly, for various reasons, this premise was not followed with respect to consumer-related financing. In that context, indeed, many of the innovations of Article 9 (revised) are expressly excluded from application to consumer assets and several other changes are made to reduce the easy availability of consumer assets as collateral. See, e.g., UCC §§ 9-108 (description of collateral); 9-109(d)(13) (consumer deposit accounts) (Revised)

¹¹ UCC § 9-102(a)(2) (Revised).

- Invalidating in part contract terms or the terms in other law that prevent a lender from creating and perfecting an interest in a non-exclusive license.¹²
- Reworking the language on deference to other filing rules to limit the extent of deference to that mandated by the other law.
- Rules dealing directly with computer programs as assets and distinguishing between programs customarily embedded in goods which are treated as goods, as compared to other programs which are treated as “software”, an intangible asset.¹³
- Creating an idea of licensee in the ordinary course.

The ultimate effect of these and other rules remains to be seen, but it is clear that financing issues are different under revised Article 9 in contrast to practice and law under original Article 9.

Of course, while Article 9 dominates state law regarding secured finance, there are other sources of state law that may need to be considered. For example, most states have adopted Article 2A of the UCC, dealing with leases of goods. Article 2A contains specific provisions validating what it described as a “finance lease.”¹⁴ This is a financing format in which the financier obtains the particular goods for purpose of leasing them to an identified lessee as a financial accommodation. The lessee has picked out the goods to be leased and the financier “purchases” them at the lessee’s instructions. In such transactions, under Article 2A, the finance lessor is treated in a manner consistent with its actual role in the transaction – as a lender, rather than as a true lessor – for purposes of warranties and the like.

Additionally, UCITA contains limited provisions dealing with the position of a creditor other than a secured lender with reference to license interests in computer information transactions. These provisions deal with both lease-based lending and a form of unsecured lending.

III. Defining the Collateral or Asset

Under Article 9, important issues about the enforcement and the proper approach to creating or perfecting a security interest hinge on describing the collateral that is the subject matter of the transaction. Filing and other rules often hinge on the type of collateral involved. It is also the case that, especially when the transaction involves parties who come to the issue primarily from a commercial finance, rather than from an intellectual property background, parties also frame both the security agreement and the financing state (in stat records) in terms of the so-called collateral classifications found in Article 9 (other original and revised).

¹² UCC § 9-408 (Revised).

¹³ UCC § 9-102(a)(75) (Revised).

¹⁴ UCC § 2A-103 (1998 Official Text).

[1]. Statutory Nomenclature and Classification

Article 9 sets out various “collateral classifications” or “collateral types” and frames many rules around the type of collateral involved. The primary distinction of significance involves separating goods, intangibles, and intangibles represented by a significant writing (such as a promissory note). We will not discuss intangibles represented by a significant writing, but concentrate on the other two categories.

Both general categories (goods and intangibles) involve various subcategories and classifications. The important point for modern practice is that, reflecting the increasing perceived value of intangibles as assets, revised Article 9 alters the definitions or categories that existed under original Article 9 and creates several new categories relevant to intellectual property assets and licensing.

Under original Article 9, the analytical framework involves first distinguishing between goods and intangibles. “Goods” includes “all things which are movable at the time the security interest attaches...”¹⁵ Within the category of goods, a particular item is classified as inventory, equipment, farm products, or consumer goods largely based on the manner in which the debtor uses the item. Within the context of intangibles, the two further categories of importance to us were “accounts” and “general intangibles,” defined in the following manner:

- “Account means any right to payment for goods sold or leased or for services rendered which is not evidenced by [a significant paper such as a negotiable] instrument or chattel paper.”
- “General intangible means any personal property (including things in action) other than goods, accounts, chattel paper, ... instruments ...”¹⁶

As this indicates, “general intangible” was a background, or catchall category that included all collateral not covered by a more specific classification. Most intellectual property rights and licenses, however, fell within the definition of “general intangible.” This included rights under a license, either rights to use the licensed subject matter or rights to collect royalties under the license.

Revised Article 9 was drafted at a time when the value of informational assets was clearly understood. While Revised Article 9 retains the differentiation between goods and intangibles, it makes significant changes in each definition that affect information asset financing. Some pertain to computer programs as collateral, which we address in a subsequent subsection. Beyond that, revised Article 9 alters several intangibles classifications.

It defines the term “account” to *expressly include* rights to payment resulting from a license, lease or assignment of property.¹⁷ For a commercial lawyer, this classification

¹⁵ UCC § 9-105(1)(h)(Original).

¹⁶ UCC § 9-106(Original).

reflects a more comfortable and intuitive classification. Coupled with other changes, it places most rights to payment flowing from unsecured commercial transactions within a single category. As we discuss later, this affects the scope of Article 9 since, subject to some narrow exclusions, it places all transactions (sales or security interests) in which the subject matter involves a payment stream arising from other transactions within Article 9.¹⁸ Previously, sales of rights to payment arising out of licenses or assignments were governed under other law.

Revised Article 9 also creates a new sub-category within the class of “general intangibles.” This is a “payment intangible”, defined as “a general intangible under which the account debtor’s principal obligation is a monetary obligation.”¹⁹ This does not include contractual rights to royalties under a license. Subject to preemption and various stated exclusions, however, sales of and security interests in a payment intangible is within the scope of revised Article 9.

To understand how these classifications work together, consider the following illustrations:

Illustration 14.1. Assume that Debtor owns a patent, which it has licensed various people to use in return for stated running royalties. One of these people is Licensee. Under original Article 9, in a loan to Debtor, a security interest in the patent or in the proceeds of the licenses to Debtor are general intangibles.

In Illustration 14.1, we are dealing with intangibles and not with interests in goods. Under original Article 9, in a loan to Licensee, the contract rights under the license are general intangibles. In contrast, under revised Article 9: 1) in a loan to Debtor, the patent is a general intangible, while the license royalties are accounts, and 2) in a loan to the Licensee, the contract rights under the license are general intangibles. Under both versions of Article 9, sales of general intangibles are not within the scope of Article 9, while sales of accounts (both versions) and sales of payment intangibles (revised Article 9) are within that scope.

Illustration 14.2. Assume that Debtor owns the copyright to a motion picture. It enters into licenses with various theaters for showing performances of the motion picture. Debtor has also made many thousands of copies of the motion picture on CD’s which it plans to sell to retail distributors. It has, in fact, already sold ten thousand copies to Block Video.

Illustration 14.2 presents an issue that has presented conceptual difficulty for the financial community and courts dealing with financing questions in information assets. In a loan to Debtor, the copyright is a general intangible and the right to payment in the licenses with the theaters are accounts under Revised Article 9.

¹⁷ UCC § 9-102(a)(2)(Revised).

¹⁸ UCC § 9-109(Revised).

¹⁹ UCC § 9-102(a)(61)(Revised).

Now consider the tangible copies in Illustration 14.2. For copies that remained owned by the Debtor, one can view a tangible copy as goods or as an asset involving intangible rights. Indeed, both descriptions might reasonable apply and, in fact, both aspects could serve as collateral in a loan to Debtor for these copies. The difference in terms of what one claims as collateral can be immense. The copy, stripped of intellectual property rights associated with it, may be valueless and in any event is clearly of less value that the combined copy and copyright. On the other hand, it is not clear that an interest in a copyright gives one any security interest in a particular copy. The security interest might relate to either the intellectual property (intangible) or the tangible embodiment (e.g., goods). The choice alters what a creditor must do to perfect its interest²⁰ and affects the rights that the lender has in the event of default.²¹

For copies that have been sold to a third party (not the copyright or patent owner), doctrines of first sale and patent exhaustion clarify the issue. The buyer obtains no rights in the underlying copyright or patent and, thus, cannot use them as collateral. The collateral, rather consists of the copy and the right of the copy owner to further transfer that copy. The issue then arises whether the copies (when made) should be treated as tangible or intangible collateral for purposes of Article 9. As we see below, under original Article 9, there were cases in analogous contexts that go in conflicting directions. Revised Article 9 does not resolve this question for purposes of motion pictures or sound recording, but it does resolve the question for computer programs. The program are general intangibles. This is because it is the intangible (information), not the medium containing it that constitutes the value a purchaser acquires. In Illustration 14.2, then, in the hands of Block Video, the copies might be goods, but if the information is in digital form, the motion picture might be considered a "computer program" and thus a general intangible or, perhaps, treated as such by analogy to programs.

On the other hand, had Debtor delivered a copy to Block Video under a license giving it the right to make thousands of copies for sale, Block Video would most likely not be the owner of the copy. Its asset would be a license to make copies. Those license rights are general intangibles because we are not then dealing with rights to payment.

[2]. Software, Computer Programs, Data and the Like

The distinction between an interest in goods and an interest in intangibles often creates problems in information asset-based lending. The issue potentially arises in any case where the security agreement provides for less than a comprehensive grant of a interest in all of the debtor's assets (e.g., an interest in debtor's "inventory" where significant value resides

²⁰ See *In re Information Exch., Inc.*, 98 Bankr. 603 (Bankr. ND Ga. 1989).

²¹ At some level, one can wonder whether a security interest in a copy that has not been sold to a third party gives the lender any significant rights at all in the event of a default, since both a patent and a copyright give that rights owner control over the ability to sell the copy until a first sale occurred. Although there has been no reported litigation on this, however, the better view would be that, if the copyright (or patent) owner created the security interest in the copy, there is an implied license in the event of default and foreclosure for the lender to sell the copy in satisfaction of the debt. See *McCoy v. Mitsubishi Cutlery, Inc.*, 67 F.3d 917, 920 (Fed.Cir.1995) ("Whether express or implied, a license is a contract governed by ordinary principles of state contract law.").

in an underlying patent, trademark or copyright),²² or where the lender has followed procedures of perfecting or enforcing an interest based on a conclusion that the collateral is of one type and it in fact turns out to be characterized by a court as being of a different type requiring a different approach to perfecting the interest.

This issue is often encountered in cases involving data, text or code. The security interest might relate to either the intellectual property (intangible) or the tangible embodiment (e.g., goods). The choice alters what a creditor must do to perfect its interest and what rights it has in the event of default.

*In re Bedford Computer Corp.*²³ held that software would be considered tangible, rather than intangible property because the “technology cannot exist independent from the actual hardware components to which it gives operational life.” This requires use of state law for perfection and priority, but also tends toward the view that the security interest does not cover intellectual property rights. One may have a lien against one copy of source code, but not in the copyright interest that involves a right to make further copies of the code. Obviously, this leaves the lender with less position than if the lien related to both the copy and the copyright.²⁴

In contrast, *In re Information Exchange, Inc.*²⁵ reached a different result in reference to computer tapes that contained a debtor's data base. The creditor took possession of the computer tapes. It argued that possession perfected the security interest without any filing. If the database were tangible, this would be correct. The court, however, held that the security interest was in an intangible. It emphasized the actual character of the transaction and the source of the value it entailed, rather than the form in which the value was held. As the court noted, it was “not the computer tape itself which is actually in issue ... but the information and programming which is recorded on the tape.” Information is an intangible, treated under the UCC as a general intangible in which a security interest can be perfected only by filing.

The comparison of these cases shows the uncertainty that can arise in understanding exactly what constitutes the collateral when Article 9 interacts with the world of intellectual property rights. Revised Article 9 addresses this problem with respect to one type of intangible collateral – computer programs – and by doing so provides appropriate guidance with respect to other types of digital information as collateral. Whether its method of treating

²² See, e.g., *United States v. Antenna Systems, Inc.*, 251 F. Supp. 1013, 1016 (D.N.H. 1966) (Security interest in inventory, work in progress, contract rights, and equipment of a software company did not cover “blueprint and technical data produced when the company's engineering staff designed a product.”). The reader should note, however, that use of an agreement that refers simply to “all assets” creates problems entirely unassociated with the subject matter of this book. Such descriptions have been held to be overly broad and therefore inadequate under Article 9. Revised Article 9 makes this rule explicit as applied to a security agreement. UCC § 9-108(c)(Revised).

²³ *In re Bedford Computer Corp.*, 62 Bankr. 555 (Bankr. DNH 1986).

²⁴ The district court in *In re C Tek Software, Inc.*, 117 Bankr. 762 (DNH 1990), also treated software as a tangible. That case dealt with the impact on a creditor's lien of the movement of tangible copies of source code from one state to another, an action that may require refileing under the general rules of the UCC for some goods. In *C Tek*, the security interest covered both the source code and all ownership rights in the software, thus seeming to expressly cover copyright interests.

²⁵ *In re Information Exch., Inc.*, 98 Bankr. 603 (Bankr. ND Ga. 1989).

the distinction works well in practice or not remains to be seen, of course, since there has been no reported case law under revised Article 9.

Revised Article 9 treats a computer program ordinarily as a general intangible, rather than goods, even if contained on a tangible medium. Revised Article 9 provides that the term “goods” does not include a “computer program embedded in goods that consist solely of the medium in which the program is embedded.”²⁶ Instead, with an enumerated exception, computer programs along with any supporting information transferred with it are defined as “software” and expressly defined as a general intangible. This also should control the designation of the medium that holds the program since the medium has no value independent of its content and any approach other than considering the two together would create hopeless classification and enforcement problems, but the statute does not clearly answer that question.²⁷

Revised Article 9, however, treats some computer programs as goods. This exception involves a computer program embedded in goods if the goods are not simply the medium in which the program is embedded and if:

- (i) the program is associated with the goods in such a manner that it customarily is considered part of the goods, or (ii) by becoming the owner of the goods, a person acquires a right to use the program in connection with the goods.²⁸

Comments to revised Article 9 do not give illustrations of this bifurcated treatment, but the general parameters are relatively clear.

- Programs not embedded in goods or embedded solely on a medium of affixing them (e.g., a diskette or a CD) are general intangibles.
- Programs customarily or actually separately licensed apart from the sale or lease of the goods in which they are embedded are also general intangibles.
- If, however, the program is customarily treated as part of the goods and in which it is embedded or is sold in a manner that the buyer of the goods has a right to use the program in those goods, the program is treated as goods for purposes of Article 9.

Thus, a program that operates a toy robot that is sold to the general public and not separately licensed would be goods for purposes of Article 9, while a program embedded in a computer and separately licensed is a general intangible. A program provided on a diskette or CD is a general intangible, regardless of whether it was sold or licensed to the transferee-debtor.

²⁶ UCC § 9-102(a)(44)(Revised).

²⁷ See *Antenna* case. See also the definition of “computer information” in UCITA § 102 (2000 Official Text).

²⁸ UCC § 9-102(a)(44)(Revised).

Article 9 does not define the term “embedded” or the term “computer program.” One might rely on the definition of computer program in the Copyright Act, but there is no reference to that Act in this statute. Alternatively, the term might be construed in light of other state law, such as UCITA. Also left unanswered is whether digital products that are representations or copies of motion pictures or sound recording are covered by this concept. The argument that they should be included is simple: the digital medium is the same for programs and has the same effect (instructing a computer how to operate) and, furthermore, as with programs, the value lies in the intangibles, not the diskette or CD.

Part A. Secured Lending and Intellectual Property Rights as Assets

IV. Scope of Article 9: Intellectual Property Rights

The scope of Article 9 is defined by two analyses. The first involves the defined affirmative scope and limitations contained in the Act itself. The second concerns the preemptive influence of federal law which, by potentially preempting certain applications of Article 9, in effect narrows the scope of that statute. With respect to both, however, we need further to distinguish between issues of scope which ask whether Article 9 applies at all to a particular transaction, and questions which ask, assuming that Article 9 has some application to a given transaction, does the Article 9 rule on the particular question at issue control or does other law govern?

In this section, we focus on those questions as they relate to intellectual property issues. We discuss contract and contract rights issues in a subsequent part of this chapter.

[1]. General Application of Article 9: Security Interest

Both original and revised Article 9 apply broadly to any transaction, regardless of form, intended to create a security interest in personal property.²⁹ Article 9 also applies to sales of certain contractual rights. Revised Article 9 expands this to include, in relevant part, “a sale of accounts, chattel paper, payment intangibles, or promissory notes.”³⁰ Each of these, which may not be familiar to parties lacking extensive experience with Article 9, is a defined term. Both in its definition of “accounts” and in the new term “payment intangibles”, revised Article 9 greatly expands the scope of its application into intellectual property licensing arrangements.

It is clear that the intent of the affirmative statement of scope is to be broad and to apply regardless of the form or label adopted by the parties for their transaction. The scope of Article 9 relevant to intellectual property rights (as compared to contract payment rights), is largely controlled by two terms: “security interest” and “personal property.”

²⁹ UCC § 9-102(a)(Original); UCC § 9-109(a)(Revised).

³⁰ UCC § 9-109(a)(3)(Revised).

[i]. Personal Property

The UCC does not define “personal property.” However, various comments to both versions of Article 9 make clear that the intent includes copyright, patent, trademark and similar rights. Comments to revised Article 9 dealing with the content of one of the Article 9 collateral types (“general intangibles”) comment:

[This] is a residual category of personal property, including things in action ... Examples are various categories of intellectual property ... As used in the definition ... “things in action” includes rights that arise under a license of intellectual property, including the right to exploit the intellectual property without liability for infringement.³¹

To an intellectual property lawyer, the device of including licensed rights within a concept of “things in action” seems out of place. Since the concept seems to deal with contractual collateral, however, we will return to that problem later.

The Comment makes clear the drafters’ intent to cover intellectual property and associated forms of “personal property.” Indeed, the idea that intellectual property rights are a form of personal property is commonplace.³²

The issue that will strike the intellectual property bar as interesting about this focus on personal property concerns the idea of *property* itself. Most traditional fields of intellectual property law have been held to create property rights in their particular subject matter. However, what of information that falls outside these fields and that designation? Does Article 9 apply only to subject matter that would be considered to be property? For example, if a factual database were used as collateral for a loan or similar transaction, would Article 9 apply if the database were not copyrightable and were not held in a manner that constitutes it to be a trade secret?

We should also note that, in the comment, the reference to rights created under a license refers to rights held by a licensee under a license. In some aspects of intellectual property law and practice, a non-exclusive licensee is not treated as holding a property right, but as being merely the beneficiary of a promise to not sue. Whether such position elevates into a “property” right for purposes of Article 9 might be questioned, but it is clear that the licensee at least has a contractual interest and contract rights are adequate in modern law for setting financing arrangements.

More generally, the unique concepts of property limitations under intellectual property law might indicate that some transactions are not covered. Yet, it is not likely that a court would or should reach that conclusion on the scope of Article 9. The purpose of the statute is to cover all transactions that engage a security interest as a focus and that deal with valuable collateral. The formal conclusion that data is or is not property does not bear on

³¹ UCC § 9-102, cmt. 5d (Revised).

³² See, e.g., 35 USC § 261 (“Subject to the provisions of this title, patents shall have the attributes of personal property.”).

achieving that goal. Indeed, if one sought a technical justification for describing an uncopyrighted database as personal property, one could find it in the numerous state criminal laws that expressly so state for purpose of criminal theft and similar prosecutions.

[ii]. Security Interest

The second element of the scope of Article 9 relevant to intellectual property rights refers to a transaction that creates a “security interest.” Revised Article 9 defines “security interest” to mean:

An interest in personal property or fixtures which secures payment or performance of an obligation. The term also includes any interest of a consignor and a buyer of accounts, chattel paper, a payment intangible or a promissory note in a transaction that is subject to Article 9.³³

The definition does not depend on the form of a transaction, but the function of the property interest created by the transaction.³⁴ While there is no case law directly on point, a conditional assignment of rights in intellectual property should qualify as a security interest if the conditions involved rights that secure payment or another obligation. The same holds true for an “exclusive license” under the same conditions and analysis.

This result seems unsurprising if the primary purpose of the transaction centers on securing performance of credit repayment obligations under a loan or a credit purchase related to the intellectual property where the effect of the transaction is to convey to the transferee essentially all rights in the intellectual property on payment of all obligations.³⁵ Some risk exists, however, that the language of Article 9 might cover more broadly a reversionary right in a license or assignment (e.g., a reversion if the licensee’s use exceeds the exclusive license scope). That would be a misapplication of Article 9, even if one could argue that such conditions are nominally within the language, since the purpose of Article 9 remains on property-based assurances of the performance under credit obligations and the remedies or other rules of Article 9 are suited solely to the context of a credit transaction and enforcing payment through sale or other disposition of the collateral. Those remedial provisions are not appropriate to ordinary license breach and have appropriately never been applied to that context.

³³ UCC § 1-201(37) (2000 Official Text).

³⁴ See UCC § 9-102, cmt. 3b (Revised) (“Whether an agreement creates a security interest depends not on whether the parties intend that the law *characterize* the transaction as a security interest, but rather on whether the transactions falls within the definition of “security interest” in Section 1-201.”).

³⁵ In a marginally analogous context, there has been extensive judicial and legislative activity regarding when or whether a transaction characterized as a lease of goods was in a fact a sale of the goods subject to a security interest. As the law eventually evolved in that context, a critical issue in making the distinction involves whether the economic nature of the transaction in effect conveyed all relevant rights in the leased goods to the lessee as a practical matter, or whether the lessor retained a significant residual interest (e.g., retained value after the transaction was fully performed). See UCC § 1-201(37) (1990 Official Text).

[2]. Application of Particular Article 9 Rules: Partial Exclusions

If a transaction falls within the affirmative scope of Article 9, there remain questions about whether or to what extent Article 9 governs a particular issue in the transaction. Frequently Article 9 does not govern the entire relationship.

One way in which this occurs comes directly from the focus of Article 9 itself. The provisions of Article 9 deal with the creation, perfection and enforcement of security interests and with validating or invalidating certain other aspects of a contractual relationship associated with those functions. This leaves many issues untouched and, therefore, subject to other law. The clearest example concerns warranties or other assurances of the quality of the subject matter. These issues are not addressed in Article 9; other law controls. Similarly, Article 9 does not discuss standards for delivery or performance, issues of cure, questions of repudiation, or in transactions other than sales, issues about where or whether title transfers. On all of these, other law governs.

Article 9 focuses on issues associated with the relationship between the interest in personal property and the obligation it secures. Within that scope, the general rule is that Article 9 controls over other state law, unless it expressly defers to other law, such as on issues of perfection of a security interest in an asset covered by a state certificate of title statute.³⁶

There are two parts of this selected deference or exclusion that affect secured lending in intellectual property assets and, perhaps, also to interests in license contract rights. The first is that Article 9 does not govern where a federal law or regulation preempts. Revised Article 9 states this premise in the following terms:

This article does not apply to the extent that ... a statute, regulation, or treaty of the United States preempts this article³⁷

This language narrows the deferential language in original Article 9. That language excluded original Article 9 coverage for any security interest subject to a law of the United States to the extent that the law "governs the rights of parties to and third parties affected by transactions in the particular types of property."³⁸ Under revised Article 9, deference requires preemption; that is, there is no state law deference based on the mere fact of federal coverage unless the federal coverage is preemptive in effect, in which case, of course, state law has no choice but to give way to federal law.

For intellectual property assets, the most important potentially preemptive federal laws relate to copyright, patent and trademark. Both original and revised Article 9 contain rules specifically referring to deference in regard to filing or recording rules. The relevant language in revised Article 9 provides:

³⁶ See, e.g., UCC §§ 9-303; 9-311(a)(2)(Revised); UCC §§ 9-302(3)(b).

³⁷ UCC § 9-109(c)(1)(Revised).

³⁸ UCC § 9-104(a)(Original).

[The] filing of a financing statement is not necessary or effective to perfect a security interest in property subject to ... a statute regulation or treaty of the United States whose requirements for a security interest's obtaining priority over the rights of a lien creditor with respect to property preempt [the section requiring filing in state records to perfect an interest.]³⁹

The term "perfect" or "perfection" in Article 9 refers to placing the security interest into the best possible position with respect to the rights of third parties in the relevant property. Under the foregoing rule, for property covered by such a preemptive statute, compliance with the relevant federal rules is the only way to perfect the interest.

Once again, the language in revised Article 9 narrows language in original Article 9 by merely stating the truism: a federal preemptive law preempts Article 9 which, after all, is merely state law despite its national importance. The language in original Article 9 had stated:

The filing of a financing statement ... is not necessary or effective to perfect a security interest in property subject to ... a statute or treaty of the United States which provides for national or international registration ... or which specifies a place of filing different from that specified in this Article for filing of the security interest.⁴⁰

While this language required merely that there be a federal registration system applicable to the subject matter, the revised Article 9 language requires a registrations system of a particular type (e.g., giving priority over a judgment lien creditor) and that the system be preemptive, rather than concurrent in nature.

The change from original to revised Article 9 language embodies a state law policy change, moving in a direction more favorable to the treatment of secured interests under state law. In this regard, it is interesting that, while the comments to original Article 9 describe the Copyright Act registration rules in illustrating a system that displaces Article 9, the comments to revised Article 9 do not cite the Copyright Act. Yet, one doubts that secured lenders or others relying on a security interest will act differently under original Article 9, at least until definitive judicial ruling signal a true and definitive change in law. The risk that copyright preempts state law filing remains strong and a change in Article 9 comments cannot alter that effect.

Under revised Article 9, Article 9 rules are displaced by federal law only if the federal rules preempt Article 9 rules. Revised Article 9 states this rule twice – recognizing displacement to the extent that federal law generally preempts, and also if a federal registration rule of a particular type preempts the state rule.

³⁹ UCC § 9-311(a)(1)(Revised).

⁴⁰ UCC § 9-302(3)(a)(Original).

V. Creating a Security Interest: Intellectual Property Rights

The threshold legal issue in asset-based financing in any context entails how one creates an enforceable interest.⁴¹ The basic theme of secured lending focuses on property interests created by agreement. Thus, the core questions center on creating an enforceable agreement, what formalities or other requisites apply, and what law governs concerning them?

[1]. Required Writing and Description

Both versions of UCC Article 9 require a signed writing that describes the collateral in order to establish an enforceable security interest unless the creditor is in possession of the collateral.⁴² Consistent with modern law and UCITA, Revised Article 9 describes this requirement as an *authenticated record*, changing prior law only to the extent that electronic signatures and records are permitted.

This state law requirement corresponds to requirements under patent and copyright law that transfers of interests in those rights must be in writing.⁴³ The federal act requirement does not apply to all contracts involving copyrights or patents, but is more narrow. The language in the Copyright Act is as follows:

A transfer of copyright ownership, other than by operation of law, is not valid unless an instrument of conveyance or a note or memorandum of the transfer, is in writing and signed by the owner of the rights conveyed.⁴⁴

The requirement under this federal rule arises only if the transaction entails a transfer of "copyright ownership." The technical issue thus presented concerns whether a security interest in a copyright entails a "transfer of copyright ownership." This is a defined term in copyright law.⁴⁵ It generally has been held to apply to security interests.

The Patent Act similarly provides that "Applications for patent, patent, or any interest therein, shall be assignable in law by an instrument in writing."⁴⁶ As a general rule, the term "assignment" involves a transaction that transfers title.⁴⁷ The requirement of a written

⁴¹ We are following a traditional commercial lending structure here in differentiating between issues that define the rights between the parties (creditor and debtor) to the agreement and issues that focus on the rights of the creditor, through its property interest, against third parties. The latter issue, discussed below, concerns how one *perfects* a security interest and what *priority* that perfected interest has against third parties.

⁴² UCC § 9-203(Original); UCC § 9-203(b)(Revised).

⁴³ 17 USC § 204(a); 35 USC § 261. The federal electronic signature statute presumably allows the writing requirement to be satisfied by an electronic record or signature.

⁴⁴ 17 USC § 204(a).

⁴⁵ 17 USC § 101.

⁴⁶ 35 USC § 261.

⁴⁷ See *In re Cybernetic Services, Inc.*, 52 USPQ2d 1683 (BAP 9th Cir. 1999); *Rite-Hite Corp. v. Kelley Co.*, 56 F.3d 1538, 1551 [35 USPQ2d 1065] (Fed. Cir. 1995) (assignment is the conveyance of title in patent Law); *Public Varieties of Miss., Inc. v. Sun Valley Seed Co.*, 734 F.Supp. 250, 252 (N.D. Miss. 1990) (assignment is "a conveyance which transfers the entire bundle of common law rights residing in a patent">cq>).

agreement is absolute and in the nature of a statute of frauds.⁴⁸ A security interest under modern practice does not require a transfer of title and, thus, arguably falls outside this standard in cases where title was not conveyed.⁴⁹ We will have more to say about this standard later.

In part because of the over-riding Article 9 requirement and in part because of questions about the scope of the federal writing requirements, preemption or deference issues between state and federal law here are seldom debated on the question of whether there was an adequate writing.

The writing must adequately describe the subject matter and the fact that a transfer occurred. As a general rule, practitioners approaching the issue from an intellectual property perspective tend to describe a copyright, patent or trademark in formal, specific terms referencing the registration numbers. In part this is caused by the traditional focus of those fields, but in part it is caused by the registration systems that copyright, trademark, and patent law implement. For example, the Copyright Act provides that a recordation of a document pertaining to a transfer of copyright ownership. In contrast, commercial finance practice often relies on general UCC categories. When they adequately encompass the particular rights involved, such more generic descriptions ordinarily suffice.

Of course, as we have seen earlier, misconceptions about what actually comprises the collateral are not uncommon. Thus, for example, in *United States v. Antenna Systems, Inc.*,⁵⁰ the court held that a security agreement extending to inventory, work in progress, contract rights, and equipment of a software company did not cover "blueprint and technical data produced when the company's engineering staff designed a product." The court described the visual reproductions of "engineering concepts, ideas and principles [as] general intangibles" under the U.C.C. The court suggested that ideas dominate intellectual property, making the tangible embodiment of the ideas inseparable from the ideas themselves. Thus, the fact that these were in tangible form did not control their classification.

[2]. New Developments and Technology

Article 9 allows the creation of an interest in current and after-acquired property with minimal formality.⁵¹ This approach facilitates so-called revolving loan financing, a situation

⁴⁸ See *Valente-Kritzer Video v. Pinckney*, 881 F.2d 772 (9th Cir. 1989). Compare *Great S. Homes, Inc. v. Johnson & Thompson Realtors*, 797 F. Supp. 609 (MD Tenn. 1992) (exclusive copyright licensee had standing to bring infringement action even though license agreement was oral when complaint was filed).

⁴⁹ See *In re Cybernetic Services, Inc.*, 52 USPQ2d 1683 (BAP 9th Cir. 1999). Compare *Waterman v. MacKenzie*, 138 U.S. 252, 11 S.Ct. 334, 34 L.Ed. 923 (1891) (Patent mortgage was an assignment where mortgage was created by transferring ownership of the patent, subject to defeasance upon payment of a loan.).

⁵⁰ *United States v. Antenna Systems, Inc.*, 251 F. Supp. 1013, 1016 (D NH 1966). See also *Chemical Bank v. Communications Data Servs., Inc.*, 765 F. Supp. 1401 (SD Ia 1991) (refusing to resolve whether a subscription list was "goods" or "general intangibles" but treating the list as goods by applying U.C.C. 9-310); *Dabney v. Information Exch., Inc. (In re Information Exch., Inc.)*, 98 BR 603, 604 (Bankr. ND Ga. 1989) (computer information and programming are general intangibles not goods).

⁵¹ The agreements here may be couched expressly in the form of a security agreement like that used in UCC generally or, especially when drafted by lawyers whose specialty lies in intellectual property law, in terms of a "collateral assignment." The form does not control the substance of the agreement. See generally Nimmer,

in which both the debtor and the creditor understand that the collateral basis for the transaction will be a shifting, rather than a fixed set of assets.

That approach does not fit easily into the framework of intellectual property law. In that law, determinations about ownership are made based not solely on derivation of the subsequent work or invention, but on who contributed the creative work product and whether that contribution was authorized and not an infringement. Furthermore, in federal intellectual property regimes, registration systems and the rights flowing from them tend to be organized in terms of specific patents, trademarks or copyrights, rather than in reference to the debtor, thereby making it more difficult to simply follow a premise that a single agreement or registration automatically covers entirely separate works or inventions.

In *In re C Tek Software, Inc.*⁵² a lender had a security interest in various assets, including a particular computer program developed to the level of version 3.7. Subsequent to the security interest being created, a third party was given an exclusive license to develop, enhance, and market the program. After the licensor defaulted, the lender sought to foreclose on the software copyright, including the copyright on the then-current version of the program (4.1). The court, however, ruled that the secured party's lien was limited to the version in existence at the time of the loan. The enhancements could be identified separately from that earlier version and were not within the lien.

Significantly, in this case, the copyright in the derivative work was held by the licensee who was not a party to the loan agreement. Even if the security agreement by its own terms extended to new versions of the software, in this case that new version was not and had never been owned by the debtor. Nor had the licensee given the debtor permission to encumber licensee's property. If the derivative work were developed and owned by the debtor, however, a different result might arise, at least under revised Article 9. Article 9 gives a lender an automatic interests in any identifiable proceeds of its original collateral. While original Article 9 treats proceeds as referring largely to property received on sale, lease or other disposition of collateral, Revised Article 9 uses a broader concept that includes "rights arising out of collateral."⁵³

In contrast to *C Tek* the court in *Chesapeake Fiber Packaging Corp. v. Sebro Packing Corp.*⁵⁴ held that a security interest in a patent application extended to the patent issued as a result of the application enforcing the intent and language of the transaction. This approach parallels modern commercial financing law. No clear reason exists to disregard an interpretation of a financing contract (security agreement, assignment, or license) that reflects modern commercial expectations and one suspects that the modern commercial view will prevail.

C Tek involved a failure to make the security interest extend to new property defined in a manner consistent with copyright law. A related problem occurs if the lien attaches to technology only in its current state or only to new property. The difficulty entails identifying

Commercial Asset-Based Financing ch.22 (1988).

⁵² *In re C Tek Software, Inc.*, 127 Bankr. 501 (Bankr. DNH 1991).

⁵³ UCC § 9-102(a)(64) (revised).

⁵⁴ *Chesapeake Fiber Packaging Corp. v. Sebro Packing Corp.*, 143 Bankr. 360 (D. Md. 1992).

the encumbered technology separate from the other technology of the debtor or its new versions. The court in *Bedford Computers*⁵⁵ invalidated an ownership claim to “new software” because the alleged owner who had financed the development could not separate its technology from other software. The critical step involves establishing and enforcing a method of tracing or identifying the specific collateral. Absent a means for that, it may be that no security interest exists because the secured party failed to provide a reasonable description of the collateral.

VI. Filing, Perfection and Registration: Intellectual Property Rights

Whether a security interest is effectively created affects various issues. Primarily, however, it sets out the existence of enforceable rights against the debtor. With reference to rights against third parties, under Article 9 and federal intellectual property law, an enforceable security interest is merely a precondition for having rights, but further steps must occur to establish protection or priority of rights against third parties to the extent permitted under the applicable law. Article 9 refers to these added steps as steps that relate to “perfecting” the security interest, terminology that we follow in this chapter even though the same language does not appear in federal intellectual property law, where the statutes tend instead to refer to the validity of the interest as against certain third parties.

Although there are several exclusions from this requirement, for most collateral relevant to this discussion, to perfect an interest, Article 9 requires either filing of a financing statement in a relevant state office or taking possession of the collateral to perfect the interest.⁵⁶ Taking possession is not a permitted means of perfecting a security interest in true intangibles, such as general intangibles and accounts, which include intellectual property rights and license rights under both versions of Article 9.⁵⁷ On the other hand, either filing or taking possession suffices for perfecting a security interest in goods. Filing under Article 9, of course, ordinarily requires filing in a state office, while recordation rules under federal laws relevant to intellectual property ordinarily require recording in a federal office.

State law filing systems under Article 9 are ordinarily indexed according to the debtor’s name, rather than to the collateral, except in atypical cases where a title system exists, such as in state laws relating to certificates of title in motor vehicles. Importantly, however, for ordinary collateral, revised Article 9 changes the rules as to which office in which state provides the location for filing. For most cases, the filing location under revised Article 9 will be at the debtor’s location, which for corporations is at the debtor’s place of incorporation,⁵⁸ rather than at the location of the collateral or the transaction that creates it.

A basic theme in the Article 9 rules focuses on requiring a creditor to take steps that law treats as giving constructive notice to third parties of the creditor’s interest, but a further justification for the Article 9 rules centers on the creditor’s ability to plan a transaction: augmented by knowing both how and where one checks to determine what prior interests

⁵⁵ In re *Bedford Computer Corp*, 62 Bankr. 555 (Bankr. DNH 1986).

⁵⁶ UCC § 9-302 (Original); UCC §§ 9-308-316 (Revised).

⁵⁷ See discussion of collateral categories in ¶ 14.--.

⁵⁸ UCC §§ 9-301; 307 (Revised).

exist and what steps one need to take in order to set the priority of the interest against subsequent parties.⁵⁹

Under either version of Article 9, once one correctly determines the nature of the collateral, location of the collateral or debtor, and the name of the debtor, guidance on how to perfect an interest becomes relatively straightforward to the extent that Article 9 governs:

- General intangibles (e.g., intellectual property, including trade secrets): filing is required and is to be made in designated state records in the debtor's location and under the debtor's name as described in Article 9.
- Goods: filing or possession may perfect; filing is to be made under the debtor's name; which state's records govern depends on whether original or revised Article 9 applies.

This state law system sets the background for the preemption and practical issues that affect asset-based financing of intellectual property assets. Mostly, these issues focus on the involvement of federal intellectual property regimes. As we have seen, original Article 9 and revised Article 9 each contain two provisions that expressly defer to federal registration or filing systems when they are applicable to personal property collateral. The two versions of Article 9 do so in different language, with revised Article 9 limiting its deference to federal systems to the extent they preempt state law, while original Article 9 leaves open the potential of broader deference to federal filing systems.

[1]. Nature of the Options

As we consider these issues, an important practical question needs to be set out as the background for discussion. The filing systems (federal and state) use conceptually different frameworks. The federal systems are based on a property-rights model, akin to real estate records. They register interests based on the work (the property). In part, at least, this is because of the primary function of the systems, which includes tracking title in intellectual property. In contrast, Article 9 records require filing based on the debtor's name. That is because they track primarily a credit-lien process that does not purport to concern itself with recording or tracking title in an asset, but focuses on giving a limited picture of the credit status of the particular debtor.

The two systems optimally support structurally different types of financing. To understand this, consider the following illustration:

Illustration 14.3. ABB Productions creates a copyrighted motion picture (titled: Race Times), having obtained all relevant rights from all relevant persons. ABB is a corporation located in California. It has produced two hundred other motion pictures. To support production of Race Times, ABB seeks financing from Bank 1. Bank 2 also gives ABB general financing for its overall business operations.

⁵⁹ Raymond Nimmer, Ingrid Hillinger & Michael Hillinger, *Secured Financing* (1999).

What Bank 1 must do to determine the priority of its interest differs significantly depending on whether copyright rules apply or whether the Article 9 system applies. To determine whether other interests will compete with its interest in the designated motion picture, if the copyright work-based filing system controls, Bank 1 need only confirm that there are no other interests of record in that copyright. There is no need to search or clear rights in the other motion pictures or in the general financing records applicable to the debtor, ABB, or to determine the scope of any interest lenders who financed the two hundred other motion pictures took. One might well argue that a work-based title system is thus the most efficient for financing that focuses on specific works, since the system narrows those to whom the lender must look for finding and negotiating away conflicting interests. In our illustration, a debtor-based system might require clearing the interests of two hundred entities and still determining whether the debtor (ABB) owned the copyright in the particular work.

In contrast, a debtor-based filing systems seems better suited to the support of financing based on the general assets of a debtor. We can see this from the perspective of Bank 2, which is a general asset lender. Its lending approach benefits from a single, debtor-based filing system since, under that system, it can determine which prior lenders makes claims with respect to which assets of the debtor from a single search and a resulting series of inquiries. A work-based system, in contrast, requires the general lender to search for and determine interests in all of the copyright works individually, in Illustration 14.3 this means a search of over two hundred different records systems. One can easily observe that a debtor-based system better supports lending against general assets.

There are ways to blend the two, of course, and there are limits on the effects we have mentioned. But the relevant point is that the choice of which system dominates does not merely pertain to a question of where to file, but affects the process and methodology of asset-based lending.

[2]. Criteria for Preemption

In determining whether or to what extent federal rules on filing or priority displace state law, ultimately requires both a federal preemption analysis and an analysis of state law which, in some cases, may defer to federal law even if the federal law does not in fact preempt state law on the issue. Quite obviously, under U.S. law, if it chooses and if it operates within a scope of federal law competence, any federal law can preempt state law regardless of what the state law says to the contrary. That simple federalism principle is sometimes not fully considered in discussion of the interaction of federal and state law in the realm of asset-based financing. The question of whether a federal filing or priority (or other) system displaces state law is not initially a question of what Article 9 rules provide, but a question of what federal law mandates.

The standards under which preemption occurs focus on several characteristics of the federal rule and the overall system in which it applies, as these relate to the particular state rule about which preemption arguments arise. For our purposes, we can state three relevant approaches to federal preemption of state law, without delving deeply into the intricacies of each:⁶⁰

1. State law is preempted if federal law entirely occupies a field and the state law attempts to intrude into that field. (*field preemption*)
2. State law is preempted if a federal law expressly provides for such preemption and the federal law deals with a topic to which federal law appropriately can be applied. (*express preemption*)
3. State law is preempted if a state law is inconsistent with and impedes the achievement of federal policy as expressed in federal law or regulation. (*conflict preemption*)

In context of asset-based financing and the registration and priority rules of Article 9 and federal law, these three preemption analyses have been only sporadically and incompletely evaluated. Instead, courts and commentators often focus on the language of Article 9 itself, and the scope of its “deference” to federal law. But, of course, that is backwards. The proper discussion is to ask 1) does federal law preempt contrary state law on this particular issue, and if it does not then 2) does state law nevertheless defer to federal rules?

It is on this latter point that there exists a difference at least in the language of revised and original Article 9. Revised Article 9 makes it quite clear that it defers to federal systems of registration and priority only to the extent those systems are preemptive, while the language of original Article 9, at least as to filing and perfection rules, permits a broader interpretation, finding deference based on the mere existence of an applicable federal recordation system.

[3]. Copyrights

Section 205 of the Copyright Act provides:

Any transfer of copyright ownership or other document pertaining to a copyright may be recorded in the Copyright Office ... Recordation of a document in the Copyright Office gives all persons constructive notice of the facts stated in the recorded document, but only if –

(1) the document, or material attached to it, specifically identifies the work to which it pertains so that, after the document is indexed ... it would be revealed by a reasonable search under the title or registration number of the work; and

⁶⁰ See *Saridakis v. United Airlines*, 166 F.3d 1272, 1276 (9th Cir. 1999); *In re Cybernetic Servs. Inc.*, 239 BR 917 (Bankr. 9th Cir. 1999).

(2) registration has been made for the work.⁶¹

The section goes on to set out priority rules with respect to “conflicting transfers” and based in part on the timing of filing in the federal system in a manner that gives constructive notice to third parties.

The first question relevant to preemption is whether this rule applies to security interests in copyright. There are two aspects about the scope of this recordation statute that have significance in this context. Initially, Section 205 permits recording of any “transfer of copyright ownership” or of a document pertaining to copyright. A “transfer of copyright ownership” means:

An assignment, mortgage, exclusive license, or any other conveyance, alienation, or hypothecation of a copyright or of any of the exclusive rights comprised in a copyright, whether or not it is limited in time place or effect, but not including a nonexclusive license.⁶²

The term “hypothecation” expressly brings security interests within the copyright law filing system, at least for works that have been registered with the Copyright Office.⁶³

The fact that Section 205 permits recording security interests in registered copyrights suggests that its rules, rather than those of state law govern in such cases. This is buttressed by the fact that copyright law provides that no state law can create rights equivalent to those under copyright law, a statement that borders on an express “field preemption” within the scope of copyright in addition to the express preemption embodied in Section 205 itself.⁶⁴ The official comments to original Article 9 use the Copyright Act to illustrate an alternative filing system which would render a U.C.C. filing unnecessary or ineffective.⁶⁵ That language does not appear in the comments to revised Article 9, but this does not appear to alter the preemptive effect of federal legislation dealing with recording, notice and, ultimately, with priority issues concerning security interests in a manner differently than does Article 9.

Several courts have properly held that the Copyright Act supersedes UCC filing requirements to perfect security interests in copyrights and this rule should continue to govern under revised Article 9.⁶⁶ Notice that a conclusion that copyright law governs this issue affects not only where a registration occurs (federal as compared to state), but also what is filed

⁶¹ See 17 U.S.C. 205(a) (1988).

⁶² 17 USC § 101.

⁶³ See Black's Law Dictionary 742 (6th ed. 1990) (“Hypothecate” means: “To pledge property as security or collateral for a debt. Generally, there is no physical transfer of the pledged property to the lender, nor is the lender given title to the property; though he has the right to sell the pledged property upon default.”). See also *In re Cybernetic Services, Inc.*, 52 USPQ2d 1683 (BAP 9th Cir. 1999).

⁶⁴ 17 USC § 301.

⁶⁵ U.C.C. § 9-302 cmt. 8 (Original). Notice the absence of any reference to the Patent Act and the Lanham Act.

⁶⁶ See *Official Unsecured Creditors' Comm. v. Zenith Prod., Ltd. (In re AEG Acquisition Corp.)*, 127 B.R. 34, 40-41 (Bankr. C.D. Cal. 1991) (discussing perfection of a security interest in three films under a conditional sales contract), *aff'd*, 161 B.R. 50 (BAP 9th Cir. 1993); *In re Avalon Software, Inc.*, 209 B.R. 517 (B.C. D. Ariz, 1997); *National Peregrine, Inc. v. Capitol Fed. Savs. & Loan Assoc. (In re Peregrine Entertainment, Ltd.)*, 116 B.R. 194, 198-204 (CD Cal. 1990) (UCC filing does not perfect an interest in copyright).

(document specifically describing the title or the work or its registration number) and what priority rules apply.

The case law, however, is not consistent on a what rule governs security interests in copyrightable works for which no copyright registration occurred. As indicated above, under Section 205, federal recording does not give constructive notice to third parties unless "registration has been made for the work." Section 205 provides priority rules, but only with respect to works that are recorded in a manner that gives constructive notice under the statute. This leaves open whether the recording system preempts state law for unregistered works.

Several courts have held that state law filing does not perfect an interest in an unregistered copyrightable work because the federal recording rule controls. In *In re Avalon Software, Inc.*,⁶⁷ for example, a Bankruptcy Court held that, in the absence of a filing in Copyright Office records, a security interest was not perfected in software and other copyrightable works. The basic approach of the court was that Copyright Act rules completely preempt state filing and perfection rules, even for works lacking a copyright registration. This point is significant in that, in the absence of a registration, no Copyright Office filing can occur. The court emphasized that, if a creditor undertakes to obtain a security interest in a copyrighted work, it must comply with both the Uniform Commercial Code and federal copyright law. That is, in order for a security interest to attach, UCC compliance is necessary.

As to perfection rules, relying on UCC 9-302 in original Article 9, the court held that perfection requirements are different if the property is subject to a federal statute which requires central filing in another registry or location. The Bank had argued that if Avalon did not register its copyrightable material or software, perfection must be made under the UCC for such works. The court expressly rejected this argument. This would leave unregistered copyrights essentially unavailable for financing.

Under the *Avalon* approach, the burden is on the creditor to ensure registration and proper filing. Without so doing, it holds an unperfected security interest, invalid in bankruptcy, and has no means of avoiding this. In contrast, in *Aerocon Engineering, Inc. v. Silicon Valley Bank*⁶⁸ the court held that state law governs perfection of interests in unregistered copyrights. The *Aerocon* court concluded that there was no federal preemption here because the federal rules do not establish a means to perfect or to determine the priority of an unregistered copyright. While *Avalon* considered this as placing a burden on the creditor to ensure that steps were taken to qualify under federal law, the Ninth Circuit in *Aerocon* regarded the omission as leaving the perfection and priority issue to state law. Thus, there was no field preemption, conflict preemption or express preemption, since nothing in the Copyright Act precludes perfecting interests under state law in unregistered copyrights.

⁶⁷ *In re Avalon Software, Inc.*, 209 B.R. 517 (Bankr. Ariz. 1997).

⁶⁸ *Aerocon Engineering, Inc. v. Silicon Valley Bank*, -- F.3d -- (9th Cir. 2002) (no preemption of state law regarding unregistered copyrights).

The *Aerocon* approach does not mean that a creditor can safely ignore copyright recording. Whether or not a copyrighted work is registered, of course, does not reflect an inherent character or quality of the work, but a discretionary choice by the copyright owner. Registration of the work can occur at any time and, even under *Aerocon*, that step would make federal law applicable and preemptive.

[4]. Patents

Patent rights are created under the Patent Act and issued by the Patent Office. Thus, by their nature, patents their ownership and control are focused around a governmental registry and issuance system such as does not exist in copyright law where federal registration is not a precondition to holding a copyright. This would seem to indicate that the likelihood of preemption should be greater under patent law than under copyright. Buttressing that idea, the Patent Act provides that:

[a]n assignment, grant or conveyance shall be void as against any subsequent purchaser or mortgagee for a valuable consideration, without notice, unless it is recorded in the Patent and Trademark Office within three months from its date or prior to the date of such subsequent purchase or mortgage.⁶⁹

Federal regulations authorize (but do not require) recording of a “mortgage, lien [or] encumbrance” in a patent.⁷⁰

Yet, the impact of these patent law rules on state law concerning filing and priority of security interests is seemingly less than under copyright law. There are two reasons for this. The first concerns the scope of the rule itself. Notice that this patent law recording-priority rule deals only with assignments, grants and conveyances. These words are not necessarily self-defining, but one way of approaching the preemption issue is to ask whether a security interest falls within this language. If not, then one could argue that there is no preemption of a topic that is not addressed in the Patent Act and that, therefore, unless Article 9 nevertheless defers to the federal filing system, state law governs perfection of such a security interest.

Once this question is directly addressed, the tendency has been to focus on the term “assignment.” As a general matter, in most contexts, this term in patent law involves the transfer of title to the patent (e.g., I assign the patent to you).⁷¹ The traditional importance of title affects the relationship with Article 9 since, unlike former methods of personal property financing which may have involved title-based mortgages and the like,⁷² when adopted in the early 1960’s, Article 9 specifically eschewed any reliance on questions of title, dealing instead with a concept of a security interest as a form of personal property interest not

⁶⁹ 35 USC § 261 (1988).

⁷⁰ 37 C.F.R. 1.331(b) (1992); see also 37 C.F.R. 1.131(b) (1992) (permitting recordation of liens that “affect the title of the patent or invention to which it relates”).

⁷¹ See *In re Cybernetic Services, Inc.*, 52 USPQ2d 1683 (BAP 9th Cir. 1999); *Rite-Hite Corp. v. Kelley Co.*, 56 F3d 1538 (Fed. Cir. 1995) (“assignment” is the conveyance of legal title in patent); *Public Varieties of Miss., Inc. v. Sun Valley Seed Co.*, 734 F.Supp. 250, 252 (N.D. Miss. 1990).

⁷² See *Waterman v. MacKenzie*, 138 U.S. 252 (1891).

connected to title concepts. Article 9 security interests in patents usually leave title in the debtor or simply do not address the location of title. Because the federal recording system for patents arguably requires only the recording of transfers of title, Article 9 filing may not be preempted.⁷³

That conclusion was reached by the Bankruptcy Appellate Panel in *In re Cybernetic Services, Inc.*⁷⁴ The question there was whether a security interest filed only in state records was enforceable against the trustee in bankruptcy of the debtor. The court there focused on the title-related connotations of the term "assignment" and essentially concluded that, by not referring to security interests, the patent rule left the field of filing and perfecting security interests regarding patents to other law, even though administrative rules might permit recording a security interest in federal records, this was not a statutory mandate and did not establish a preemptive effect for the patent rule.

The court also held that Article 9 Section 9-302 did not require deference to the federal filing system by the state law filing system here. The court noted:

[The] Patent Act is not sufficiently comprehensive to exclude state methods of perfecting security interests in patents. The Patent Act does not include security interests within any of the scope or definition provisions. Security interests in patents are not assignments governed by the mandatory recording records provision of Section 261 of the Patent Act. Because the Patent Office records security interests on a discretionary basis and such recording does not provide constructive notice, the Patent Act registration system is insufficient to provide the sole method of perfecting security interests in patents.

The *Cybernetic* conclusion has been followed by other courts. For example, in *City Bank & Trust Co. v. Otto Fabric, Inc.*,⁷⁵ the District Court held that "the failure of the [Patent Act] to mention protection against lien creditors suggests that it is unnecessary to record an assignment or other conveyance with the Patent Office to protect [a lender's] security interest against [a lien creditor]."⁷⁶ The court also held that a U.C.C. filing perfects a security interest in a patent.

⁷³ The administrative rules regulating the function and operation of the Patent Office are consistent with the conclusion that the focus of the Patent Act recording provisions is transfers of title. 37 C.F.R. 3.11(a) provides that "assignments," accompanied by a cover sheet, will be recorded, and that "other documents" affecting title will be recorded at the discretion of the Commissioner. Assignments are defined as transfers by a party of all or part of its right, title and interest in a patent or patent application. 37 C.F.R. 3.1. The terms "security interest" and "lien" are not included in the C.F.R. provisions on patents.

⁷⁴ *In re Cybernetic Services, Inc.*, 52 USPQ2d 1683 (BAP 9th Cir. 1999).

⁷⁵ *City Bank & Trust Co. v. Otto Fabric, Inc.*, 83 B.R. 780, 782 (D. Kan. 1988) (because Congress has not expressly required the filing of an assignment with the Patent Office to perfect a security interest in a patent, notwithstanding amendment to the Patent Act following the advent of modern commercial law, the Act leaves open the area of protection against the interests of lien creditors). See also *Holt v. United States*, 13 UCC Rep. Serv. 336 (D.D.C. 1973) (35 U.S.C. Section 261 applies only where title has been conveyed, not to creation of a security interest); *In re Transportation Design & Technology, Inc.*, 48 B.R. 635, 639 (Bankr. S.D. Cal. 1985).

⁷⁶ *Id.*

A second approach that gives state filing efficacy for patents centers on the second part of the recording-priority rule in Section 261. That second part concerns against whom the patent conveyance is made ineffective if not recorded in the federal system. The conveyance is void only against a "subsequent purchaser or mortgagee for a valuable consideration". The court in *Chesapeake Fiber Packaging Corp. v. Sebro Packaging Corp.*,⁷⁷ concluded that federal law preempts state law filing systems, at least in part, but that Section 261 did not resolve the question of priority between a security interest and a judgment lien creditor (or trustee in bankruptcy). The competing claimant was not a bona fide purchaser and, therefore, could not claim priority over the secured creditor. The court reasoned that the priority provisions in federal patent filing give priority only to bona fide purchasers, not to all subsequent claimants against an unrecorded interest. Under this approach, state law recording perfects against a judgment lien creditor, but may (or may not) give protection against other parties.⁷⁸

The net effect of these rulings is that an ordinary Article 9 security interest appears to be considered outside the scope of federal preemption and, even under original Article 9, state law deference in cases of patents. Perhaps left unanswered, however, is the appropriate treatment of a security device that utilizes a conditional assignment of title, rather than a straightforward security interest. Does the format employed alter the applicable law where, in this context, the format does nominally involve a transfer of conditional title? Conditional assignments are treated, for purposes of state law, as simple security interests under the doctrine that substance prevails over form. Yet, the reason why there exists no preemption of filing rules for security interests rests in the fact that they do not deal with title, while a conditional assignment does. The better rule would seem to be that a federal law system designed to record and trace title to patents should govern when the parties deal in a transaction that conveys title, albeit conditionally and even though for other purposes state law will treat that conveyance of title as a security interest.

If the cases are taken at their face value, we have a records system for patents that splits the idea of title (federal) from the idea of security interest (Article 9). That bifurcation creates numerous conceptual and practical problems. Some concern the question of priority between an ownership transfer (federal records) and a security interest (Article 9), a topic we discuss later. But even beyond technical priority questions, the split is cumbersome and creates uncertainty. It contrasts to the rules developed for interfacing with other title-based records systems, such as certificates of title for automobiles, where the perfection of the security interest must ordinarily be made on the document that traces (records) title. In part this is because, even if we claim that the separate security interest system can be independent, in fact a lender or other party is forced to deal with both systems when they are split. Thus, for example, a lender could not safely lend against a specific patent without confirming ownership of that patent, an exercise that requires reference to the federal records on ownership. Logically, the two systems need to be joined into one and, since federal law is not likely cede control of patent ownership to the state systems, that one should be the patent records system.

⁷⁷*Chesapeake Fiber Packaging Corp. v. Sebro Packaging Corp.*, 143 B.R. 360, 368 (D. Md. 1992), *aff'd*, 8 F.3d 817 (4th Cir. 1993). See also *In re Transportation Design & Technology, Inc.*, 48 B.R. 635, 639 (Bankr. S.D. Cal. 1985).

⁷⁸*In re Transportation Design & Technology, Inc.*, 48 B.R. 635, 639 (Bankr. S.D. Cal. 1985).

One commentator argues that the approach of *Otto Fabric*, which focuses on priority, rather than filing, strikes an appropriate balance - giving at least some efficacy to the state law filing as against non-voluntary transferees.

There is much wisdom in the balance struck by *Transportation Design* and *Otto Fabric*. Together, the cases recognize that Section 261 of the Patent Act is not a secured financing statute in the modern sense, its use of the word "mortgagee" notwithstanding. Rather, it is concerned with ownership or title transfers, not the security interests of commercial financiers. The lineage of Section 261 is traceable back into the nineteenth century, and the statute is hopelessly out of touch with the notice filing concept incorporated in Article Nine of the U.C.C. which was not widely enacted until 1955 through 1965. The Patent Act says nothing about the priority of either security interests or judgment liens. Thus, it makes good sense to leave this issue to the state law of Article Nine where it is specifically and carefully addressed. ... Similar caution is appropriate before determining that Article Nine has been preempted if the question arises whether section 261 governs a dispute between competing security interests. Once again, a security interest in an asset is not the equivalent of title to the asset. A secured party is not an assignee or a mortgagee. Only Article Nine contains an extensive treatment of secured party priority.⁷⁹

[5]. Trademarks

Trademark rights can arise under either federal or state law.

State law trademarks are, for purposes of secured financing, clearly covered under Article 9. Both original and revised Article 9 classify trademarks as general intangibles. Under original Article 9, license interests arising from trademarks are also general intangibles. As we have seen earlier, however, under revised Article 9, a right to receive money stemming from a license of intellectual property will be treated as an account.

The federal trademark system is the Lanham Act. Federal law provides for registration and recording of assignments under the Lanham Act. Section 10 of that Act provides:

An assignment shall be void as against any subsequent purchaser for valuable consideration without notice, unless the prescribed information reporting the assignment is recorded in the Patent and Trademark Office within 3 months after the date of the subsequent purchase or prior to the assignment.⁸⁰

The Act mandates a recording only with respect to assignments but permits recording of other instrument related to trademarks at the Commissioner's discretion.

⁷⁹ 1C Peter F. Coogan et al., *Secured Transactions Under the Uniform Commercial Code* Section 25.08 [3] [b] [iii] (1999).

⁸⁰ 15 USC § 1060 (1988).

This trademark rule is similar to section 261 of the Patent Act, but even more clearly focused on registration of "assignments" and priority with respect to purchasers. As in the patent context, the concept of an "assignment" generally encompasses all rights in the trademark, including title.⁸¹ If a transaction does not transfer title, several courts have held that a UCC filing perfects the interest because, unlike in an assignment, a security interest does not deal with title.⁸² This pattern seems to state established law and creates many of the same problems pointed out in our prior discussion of security interests in patents. A different result may occur when the parties utilize a title-based format, such as a conditional assignment which, while merely a security interest under state law, does entail a conveyance of title.

In trademark financing, an additional complication arises because of peculiarities of the substantive law of trademarks regarding "naked licenses" and "assignments in gross." To avoid abandoning the trademark, the owner of the mark (perhaps the lender in a collateral assignment) may be required to monitor use of the trademark to avoid ensure quality retention.⁸³ Similarly, the ordinary rule holds that a transfer of a mark cannot occur unless the transfer includes relevant accompanying goodwill of the business.⁸⁴ In *Roman Cleanser*, the Sixth Circuit examined this issue related to the trademark of certain cleaning products. The court held that the sale of the mark along with the formulas and customer lists was sufficient without including the equipment used to make the products.⁸⁵ A security interest holder must record not only its interest in the trademark but also its interest in the "goodwill" in order to be able to foreclose on its interest.⁸⁶

[6]. Trade Secrets

Trade secret rights to control the use and disclosure of confidential information arise under state law. Thus, as a matter of principle, Article 9 filing and priority rules govern. Trade secret rights also fall within the category of "general intangibles."⁸⁷ As we have seen earlier, however, under revised Article 9, a right to receive money stemming from a license of intellectual property will be treated as an account.

One recurring difficulty in discussing financing based on trade secrets as collateral is in distinguishing the secrets from the tangible property. Courts have difficulty in drawing this distinction. The proper inquiry should *not* be with respect to the tangibility of the collateral but with the nature of the proprietary rights claimed. If the lender wishes as part of its collateral to

⁸¹ *Acme Valve & Fittings Co. v. Wayne*, 386 F. Supp. 1162, 1165 (S.D. Tex. 1974).

⁸² See, e.g., *Joseph v. 1200 Valencia, Inc. (In re 199Z, Inc.)*, 137 B.R. 778, 782 (Bankr. C.D. Cal. 1992) (distinguishing the statutory copyright language of *Peregrine* from the language of the Lanham Act); *In re Chattanooga Choo-Choo Co.*, 98 B.R. 792, 796, 798 (Bankr. E.D. Tenn. 1989) (holding that a U.C.C. filing perfects a security interest in trademarks and priority governed by Article 9); *In re C.C. & Co.*, 86 B.R. 485, 487 (Bankr. E.D. Va. 1988); *Creditors' Comm. of TR-3 Indus. v. Capital Bank (In re TR-3 Indus.)*, 41 B.R. 128, 131 (Bankr. C.D. Cal. 1984); *Roman Cleanser Co. v. National Acceptance Co. (In re Roman Cleanser Co.)*, 43 B.R. 940, 946 (Bankr. E.D. Mich. 1984), *aff'd* on other grounds, 802 F.2d 207, 209 (6th Cir. 1986); See *Red Barn, Inc. v. Red Barn Sys., Inc.*, 322 F. Supp. 98 (ND Ind. 1970).

⁸³ See *E. & J. Gallo Winery v. Gallo Cattle Co.*, 967 F.2d 1280, 1290 (9th Cir. 1992).

⁸⁴ 15 USC § 1060 (1988). See *Green River Bottling Co. v. Green River Corp.*, 997 F.2d 359, 362 (7th Cir. 1993).

⁸⁵ 802 F.2d at 209.

⁸⁶ *Marshak v. Green*, 746 F.2d 927, 931 (2d Cir. 1984).

⁸⁷ See *United States v. Antenna Sys., Inc.*, 251 F. Supp. 1013, 1016 (D.N.H. 1966).

control the right to disclose or use the information, the claim covers intangible assets describable as trade secrets. If the lender wishes as part of its collateral to obtain possession of existing copies, the claim covers goods.

The difficulties involved are compounded because of the possible role of copyright law as an intervening source of rights with respect to some trade secret information. While trade secrets are not embodied in a tangible medium in a form that permits copyrightability, some and many can be so expressed. When for example, secret information is expressed in a memorandum that qualifies under copyright law for copyright protection, what framework for establishing a security interest governs: Article 9 state law, or the preemptive provisions of copyright law?

Properly understood, the answer lies in what aspects of the information the lender desires to control as part of its collateral. Copyright law deals with making and distributing copies, while trade secret law deals with enforcing confidentiality even in contexts of restricted disclosure and use. Only one court has directly addressed the problem. The court in *In re Avalon Software, Inc.*⁸⁸ properly recognized that, whether registered or not, many trade secret materials are also copyrighted works under current law. The court went on to conclude that an unregistered computer program (a copyrighted work) could be perfected on as collateral only through the device of complying with federal copyright law, a result later rejected by the Ninth Circuit. The *Avalon* court, however, deviated from its own rule in part, holding that state law filing covered customer lists (not asking whether the list was copyrightable) and also covered manuals associated with the software products. The manuals certainly are copyrighted works.

A rule that leaves to state law the issue of perfection of a security interest in an unregistered copyright avoids this problem. However, that rule leaves the choice between state and federal law to the discretionary actions of the debtor (or other copyright owner) on whether it registers or does not register its copyright.

VII. Priority Issues: Intellectual Property Rights

The importance of recording regimes (whether federal or state) lies in the fact that recording fixes or establishes the strength of a transfer as against designated other parties, while failure to file leaves the transferee more exposed to potential claims from such persons. Most often, the act of recording (as contrasted to complying with an applicable statute of frauds) does not affect rights between the two parties involved in the particular transfer. That is certainly true with respect to Article 9, which does not require filing an interest to establish its position with respect to the debtor and its individual creditor. Instead, recording issues typically relate to the relationship between the recorded (or unrecorded) interest and third parties with claims to the same property. Article 9 describes this as a question of *priority* of rights.

Priority issues often relate to licenses. We discuss that question later. The focus here centers on priority in intellectual property rights themselves. In the realm of using intellectual property rights as collateral, there are two distinct priority questions. One relates to priorities

⁸⁸ *In re Avalon Software, Inc.*, 209 B.R. 517 (BC D Ariz 1997).

linked to the underlying distribution of rights themselves, and the other relates to priority among transfers of the underlying rights.

[1]. Underlying Ownership Rules and Priority

For secured lenders, one potential source of conflict and an important priority question comes from the relationship between the creditor's interest in intellectual property and the underlying distribution of initial ownership created under intellectual property law without any transfer having to occur.

Intellectual property regimes contain their own unique rules of ownership. Indeed, the difference between ownership in intellectual property law and ownership concepts in other fields of personal property constitutes one important difference that affects financing practice. For example, intellectual property ownership does not hinge on physical possession or, often, on whether property was created using the financial resources of a particular person. Indicia of ownership, if any, are often far more obscure than in tangible goods or contract rights. A recitation of the ownership concepts in various areas of intellectual property law would go well beyond our scope.

However, a basic general principle relevant to lenders is important: an interest (e.g., security interest) sought or obtained in intellectual property ordinarily can only attain a status consistent with the rights that the transferee (debtor) has a right to control. While copyright, patent and trademark law, as well as Article 9, provide recording-based priority rules, all of these deal with priority of rights among transfers or transactional interests. None deal with the rights of the underlying property owner, except as they have been transferred. As a result, an interest property recorded as the first record of a transfer may be entirely ineffective as against a true underlying owner of an property right. Consider the following illustration:

Illustration 14.4. Client Company hires software developer to create an inventory control program for Client. The contract does not specify who owns the program. Client has possession of the only copies of the software. Lender makes a loan to Client, including in the collateral, the copyright in software. It may even demand that Client register the copyright to clarify where Lender should file.

In this illustration, a proper state or federal filing of the security interest (or both) would suggest that Lender has a priority interest in the software. It does not. At most, it has a security interest in the tangible copies, but it has no interest in the copyright since that interest is owned by the software developer. The facial assurances that the recording systems coupled with the Client's possession of a copy suggest are entirely incorrect. Client (debtor) cannot give an interest in what it does not own and the software developer's failure previously to record its interest does not alter its ownership rights.

A second illustration may further underscore the conceptual problems.

Illustration 14.5. Scientist, working with various other employees of Company 1, develops an important new method of processing residue from nuclear energy plants. The process is not patented, but is used by Company 1 for competitive advantage. Unknown to it, however, Company 2 discovers the same process. Later, Scientist leaves Company 1 and creates her own company (Company 3) based in part on the process she developed. Assume that the arrangement between Scientist and Company 1 was not sufficient to preclude her subsequent use of the process she developed.

Some forms of intellectual property can be co-owned by parties who have worked together or, even, by parties entirely unaware of each other. In such cases, a security interest obtained in the intellectual property by dealing only with one such party does not ordinarily bind the other. A lender providing a secured loan to Company 1 in the prior illustration cannot take an enforceable lien in the valuable process that supersedes the ownership rights of Company 2 and the Scientist. The filing systems do not deal with that risk.

[2]. Priority Among Transfers

While one can solve issues about where to file or record simply by complying with all of the potentially applicable recording laws, the same cannot be said to be true with respect to rules of priority. In intellectual property, federal and state law systems use entirely different and conflicting *priority* rules.

Both original and revised Article 9 contain elaborate priority rules, the details of which are ordinarily irrelevant to intellectual property licensing. For present purposes, the Article 9 rules can be reduced to three premises:

1. A first-filed security interest ordinarily has priority on current and after-acquired collateral over a subsequently filed security interest or a subsequent buyer of the collateral unless the first filed interest consents to the subsequent transaction (*first to file rule*).
2. A first-filed security interest can be ousted from priority over some after-acquired collateral by a person who finances the debtor's acquisition of the collateral and complies with stated notice-giving steps (*purchase priority*).
3. A first-filed security interest can be ousted from priority by a buyer of goods that acquires the goods from the debtor in a sale in the ordinary course of the debtor's business (*buyer in ordinary course*).

None of these rules hinge priority on whether the second party had actual notice of the first interest (as compared to constructive notice). None of the state law rules conform to rules in federal intellectual property law. None.

Federal rules in trademark, patent and copyright law determine priorities based on grace periods, actual notice, and bona fide purchase. The relevant issue thus becomes one of determining when one rule (federal or state) governs or when the other rule (federal or state) applies. As we have seen, this involves determining when federal law preempts and, if it does not, determining when state law defers to federal law. A simple premise is that, if federal law provides one result, state law cannot provide a different result in the same context.

Priority rules can be conceived of as defining a relationship the parameters of which are defined by answering two questions: “what type of parties are involved” and “what rule governs between those parties?”

[i]. Copyrights

The Copyright Act rule differs from patent and trademark law. Section 205 of the Copyright Act provides:

As between two conflicting transfers, the one executed first prevails if it is recorded, in the manner required to give constructive notice under subsection (c), within one month after its execution in the United States or within two months after its execution outside the United States, or at any time before recordation in such manner of the later transfer. Otherwise the later transfer prevails if recorded first in such manner, and if taken in good faith, for valuable consideration or on the basis of a binding promise to pay royalties, and without notice of the earlier transfer.⁸⁹

This rule governs between “transfers” of copyright. A transfer includes a security interest, an assignment of copyright, and an exclusive license of a copyright, but does not include a non-exclusive license.⁹⁰

For conflicts between such claims, this federal rule controls and sets out a rule of “first created” subject to a grace period “first-to-file” concept. Thus, if my transfer occurs before yours and I file within one month after it, you are subordinate to my interest even if you file first, paid value, and had no notice of my interest. A first-created transfer is also senior to a subsequent transfer if not recorded within one month, so long as it records first.

The idea of “first-created” as governing priority interacts awkwardly with the filing rules that lenders have used for other types of property since the 1960’s adoption of Article 9. Yet, viewed from a property-rights perspective, it has merit. If a rights owner has already transferred its rights (in whole or in part) to another person, the subsequent transferee starts with the notion that what was once transferred can no longer be conveyed to another person. The grace period and recording rule can be seen as exceptions to the basic theory that an owner cannot effectively transfer again what it already gave away.

There may be potentially significant limits on this first-created, grace period rule.

⁸⁹ 17 USC § 205(d).

⁹⁰ 17 USC § 101.

It is not clear whether the copyright rules apply to unregistered copyrights. One can read the priority rule as only dealing with priorities between interests in registered copyrights, since registration is a precondition for constructive notice under the Copyright Act and the stated rule refers to that effect as a factor in determining relative rights. On the other hand, one can read the federal rule as applying to all copyright interests, whether or not in a registered copyright, and giving precedence to interests in *registered* copyrights. The plain language of the statute supports this latter result. Thus, the *Peregrine* court held that the Copyright Act rule preempts the UCC rules. That is too broad, but for types of disputes actually dealt with in Section 205, copyright law controls. Clearly, the Copyright Act controls in a conflict between a recorded interest in a registered copyright and other transfers of that registered copyright.

Section 205 gives no guidance to settle disputes where neither transferee records its transfer in federal records. State law should apply. As to conflicting security interests, Article 9 gives precedence to the first to be created or perfected.⁹¹

Section 205 does not resolve a conflict between two interests in an unrecorded copyright.⁹² Article 9 should govern under the rules set out above.

Section 205 may not settle disputes in which one conflicting party is a bankruptcy trustee or judgment lien creditor in a registered copyright. In such cases, arguably, the interests acquired by the bankruptcy estate do not entail a transfer of copyright ownership as measured by the terms of the Copyright Act, but focus on the rights of a creditor obtaining rights through involuntary, judgment-enforcement processes.

[iii]. Patents and Federal Trademarks

Federal patent and trademark law contain priority rules that are similar to each other. They provide, respectively, as follows:

Patent:

An assignment, grant or conveyance shall be void as against any subsequent purchaser or mortgagee for a valuable consideration, without notice, unless it is recorded in the Patent and Trademark Office within three months from its date or prior to the date of such subsequent purchase or mortgage.⁹³

Trademark:

An assignment shall be void as against any subsequent purchaser for valuable consideration without notice, unless the prescribed information reporting the assignment is recorded in the Patent and Trademark Office within 3 months after the date of the subsequent purchase or prior to the assignment.⁹⁴

⁹¹ UCC § 9-312 (original).

⁹² 17 USC § 205(c)(2).

⁹³ 35 USC § 261.

⁹⁴ 15 USC § 1060 (1988).

We suspect that the word “void,” were it written today, would refer to a lack of priority, but nevertheless federal law literally voids the loser’s interest (as compared to merely rendering it subordinate), suggesting that the interest has no role or influence in respect to the senior interest.

Both trademark and patent rules deal with *assignments* and both provide that an assignment is void against designated subsequent parties if it is not recorded within three months of the assignment or before the subsequent transaction. The term “assignment” focuses on transfers of essentially all rights; it is like a sale. As we have seen, several courts have held that the term does not refer to a security interest in that modern security interests do not involve a transfer of title, at least before the occurrence of default and foreclosure.

Both rules give assignments priority over a subsequent “purchaser” of the patent or trademark. Neither statute defines “purchaser.” But that term is defined in the UCC. There, it includes any person that acquires an interest in property by a voluntary transfer, including by buying or obtaining a security interest in it.⁹⁵ It is not clear whether that UCC concept applies in these federal statutes.

Putting that issue aside momentarily, we have a “clear” rule: as a matter of federal law, an assignment of a trademark or patent has priority over a subsequent purchaser of the trademark or patent if there was a recording of the assignment within the three-month grace period or in any event before the recording of the conflicting “purchase.” Arguably, then, both statutes control a conflict between a transfer of ownership (assignment) and a security interest or other voluntary transfer of the former owner’s trademark or patent (purchase). This is consistent with the title law idea that, if a person has already sold property, it cannot thereafter defeat or subvert that transfer by giving a further purported interest to another person. The ownership rules trump lender rules within the scope of these statutes in reference to intellectual property rights.

Having defined that basic premise, however, we also need to recognize the uncertainty left by the mismatch of language between federal and state law and, more importantly, between the two federal statutes. These otherwise similar statutes use different language in significant respects. The differences in language suggest differences in law.

The patent law rule refers to an “assignment, grant or conveyance,” while the trademark rule refers merely to an “assignment.” The term “assignment” apparently does not include a modern security interest (although it may include a transaction set up as a conditional assignment), but what of the other words in the Patent Act. Quite clearly, unless we assume that the language means nothing, the patent rule covers transfers that are not covered by the trademark rule. What transfers are these? Reported cases do not answer that question. However, the reference to a “grant” or “conveyance”, when juxtaposed to “assignment,” suggests that the federal rule at least encompasses exclusive licenses or like transactions that are short of an actual assignment of the patent but may entail property rights transfers. On the other hand, a similar logic suggests that the more limited trademark language does not go beyond actual and complete assignments.

⁹⁵ UCC § 1-201 (1998 Official Text).

The structure of both priority rules is similar in that they define a particular type of claim (e.g., assignment) and treat its position as against designated other claims. Looking at the second part of the two rules, the statutes also use different language in describing against whom a filed assignment prevails. The patent rule refers to rights *against* “any subsequent purchaser or mortgagee”, while the trademark rule refers only to rights “against” a subsequent purchaser. Once again, while the patent rule is broader, the meaning of the difference has not been articulated in case law.

Taking the statutes in reverse order, the federal trademark rule clearly resolves conflicts between assignments (transfers of ownership) and subsequent purchases; it does so based on *federal* filing. Thus, an assignment with a federal filing made within the grace period takes priority over any intervening assignment in a trademark. Another assignee is clearly a “purchaser.” Yet, the term “purchaser” goes further. One view, consistent with commercial usage is that a “purchaser” is any person who acquires an interest by a voluntary transaction. Under that reading, any such voluntary transaction, including the creation of a security interest, would seem to be subject to the federal rule that an assignee takes precedence if created or recorded first or within the terms of the priority statute. Courts that have held that UCC filing perfects a security interest in a trademark also often hold that the priority disputes addressed were governed by Article 9. While that may be true for conflicts not dealt with in federal law, it is not true for priority conflicts between assignments of a trademark and conflicting interests of purchasers as that term is used in federal law. The crux of the issue is whether the term encompasses a secured lender. It should be noted, however, that even if “purchaser” includes a secured party, the federal rule *does not* cover priority conflicts among two secured parties since the federal act deals only with the rights of an assignee against designated purchasers.

The patent law rule is broader than the trademark rule. Clearly, it addresses the priority of assignments (and grants and conveyances) among themselves (e.g., the priority of rights between two assignments of the same patent.⁹⁶ It also addresses rights of an assignee as against a purchaser *or* a mortgagee of the patent. If “purchaser” broadly covers any voluntary transferee, then the term mortgagee is redundant and inoperative, since mortgages are voluntary transactions. Ordinarily, one should not interpret a statute in a manner that renders a part of the statute inoperative. This argues for reading “purchaser” in a more narrow manner, perhaps limited to assignees and exclusive licenses, treating the term as roughly equivalent to “buyer.” Under such an interpretation, the federal priority rule does not apply to conflicts between an assignee and a security interest. But that interpretation conflicts with the traditional concept that “buyers” of this type of property are described as “assignees” of the title to the patent.

How to cut through this is not entirely clear since we are dealing with language that is not readily connected to modern usage and is not specifically defined in the statute or dispositive case law. However, the basic structure of both statutes indicates an intent to govern priority of rights between a title-based transfer of the patent or the trademark in conflict with rights of other claimants. Without doing damage to the structure of the federal law, one view would simply treat the references to “purchasers” as indicating that the federal rule governs the

⁹⁶ Thomas v. Topco Acquisitions, Inc., 776 F. Supp. 431, 435 (ED Wis. 1991) (Even if the last purchaser of an interest was not recorded, it has priority over prior unrecorded interests.).

rights of a title transferee as against all other voluntary transferees, including security interests. That view leaves lesser or different transfers governed by other law.

Neither statute expressly treats the position of either an assignment, or a security interest, in reference to rights acquired by enforcing judgments, such as through a judicial lien, garnishment or the like. The importance of deciding what are the rules for such potential conflicts resides primarily in reference to dealing with the status of such claims in the event of a bankruptcy filing. Among the effects of a bankruptcy filing is that the bankruptcy trustee or the debtor in possession obtain the rights of a judgment lien creditor as of the date of the filing.⁹⁷

One inference is that federal silence on the issue does not transfer the topic to state law, but merely leaves the question governed by a first created rule - that would elevate an unrecorded interest over a judgment lien creditor. That result would give special treatment to such interests that does not arise under any state law. It is not an appropriate inference.

In contrast, some reported cases treat the failure of the Patent Act to expressly address priority between voluntary transfers and judgment liens as indicating an intent to leave that issue to state law. Two trial court decisions hold that either filing in the patent office or under state law protects a lender against judgment lien creditors because such parties do not qualify as the bona fide *purchasers* that the federal priority rule specifically addresses.⁹⁸ But the language of neither the federal statutes nor the state law support a conclusion that creates parallel systems from the fact of federal silence. Actually, U.C.C. section 9-302 may render the state law filing "ineffective." The secured parties' interests would then be unperfected unless federally filed.

The most reasonable conclusion, at least with respect to a security interest in conflict with a judgment creditor is simply that federal law does not apply at all. A federal registration and filing is not relevant. The issue is entirely outside the scope of federal law and entirely within the scope of state law.

VIII. Enforceability Issues: The Nature of the Rights

While one can become entranced by the federal-state relationships that define problematic questions about financing based on ownership rights pertaining to intellectual property, those conflicts may be less important than are issues which require a lender (and debtor) to understand the nature of the basic property rights and how they integrate with lending practice.

In many respects, intellectual property is not a property right that can merely be simply defined and used as collateral without paying attention to what needs to be done to actually acquire and enforce the property itself or even recognizing what is covered or not covered by the property right.

⁹⁷ 11 USC § 544(a).

⁹⁸ See *City Bank & Trust Co. v. Otto Fabric, Inc.*, 83 BR 780 (D. Kan. 1988); *In re Transportation Design & Technology, Inc.*, 48 BR 635 (Bankr. SD Cal. 1985).

The issues are most clearly applicable in dealing with trade secrets and trademarks. In both cases, the property right is defined not only by identifiable subject matter, but by the relationship between that subject matter and either the overall business of the debtor or the network of confidential relationships which exists in reference to that subject matter.

[1]. Trade Secrets

While trade secrets are property, the information involved as an alleged trade secret is treated as property only in reference to the associated confidential and similar interests that are established with respect to it. A piece of information is not, in itself, a protected trade secret that constitutes property. It becomes a trade secret and a valuable property in reference to lending transactions only in reference to actual and enforceable conditions of confidentiality associated with it. That fact has significance for potential lenders.

Consider the following illustration:

Illustration 14.6. Debtor company manufactures rings for high school and college graduates. It uses an automated process to make the rings which gives it a substantial cost and price advantage over competing companies. The automated process consists of a number of elements that are not generally known. Most Debtor employees have agreed to non-disclosure and confidentiality agreements about Debtor's process. Lender makes a loan to Debtor based on Debtor's tangible assets and its trade secrets. It properly files in state and federal record systems.

When the collateral consists in whole or in part of information whose value derives from its secret character, interests in that "property" have value only if they encompass the ability to control and enforce that confidentiality. In Illustration 14.6, for example, the value or *existence* of any lien on a secret process hinges not on the subject matter (information), but on the information *and* control of its secret nature. To effectuate the lien requires assuring the enforceability of confidentiality restrictions *and* ensuring that the lender controls them in the event of default. For example, in the illustration, does the lender acquire an enforceable right to insist on compliance with employee confidentiality and non-disclosure agreements about the alleged secret process? If not, there may be no property covered by the lien as to that subject matter or, at least, at most a property interest whose value can be undermined at any time by persons against whom the lender has no resulting cause of action.

[2]. Trademarks

A trademark exists only in reference to enforceable rights in a name, symbol or other enforceable mark because it is associated with a property or business activity used in commerce.⁹⁹ When split from that connection, the trademark "right" may expire.

Because of this relationship, issues associated with security interests in trademarks include questions about whether creating or enforcing the interest of the lender does or does not create a context in which the underlying right expire and, thus, the value of the collateral ends

⁹⁹ McCarthy on Trademarks, §§ 2.15; 18.1 et. seq. (1999).

because of the security interest. Trademark law doctrine prohibits transfers that separate the goodwill or underlying business activity from the mark itself. In reference to assignments, this doctrine is described as involving an “assignment-in-gross”, the effect of which may be to abandon the mark itself.¹⁰⁰ In context of trademark licensing, a similar concept involves so-called “naked licenses” under which the licensor fails to retain and exercise the right to control the quality of the licensee’s performance under the mark.¹⁰¹

These doctrines obviously have significance in reference to licensing practice, but they are also important in reference to secured lending. An early issue, now largely resolved, concerned whether creating a security interest in a mark constitutes an “assignment-in-gross”? Both logic and the result reached in the reported cases indicate that it does not. The basic rationale is that merely creating an interest does not in itself separate the mark from the goodwill of the business or the quality control of the mark owner. Indeed, under modern financing practice, creating a security interest in such an intangible is likely to have virtually no effect on the use of the mark in commerce. The rationale applies regardless of whether the parties style their transaction as a simple security interest or as a conditional assignment.¹⁰² At most, the transaction involves a promise to assign or transfer in the future under stated conditions and that promise does not constitute a present assignment-in-gross.¹⁰³

This rationale, however, does not protect the transfer that might occur when an actual default and foreclosure occurs. Typically, at this point in the credit transaction, default results in an actual sale (assignment) of the collateral and *this* transfer must comply with the underlying rules about ensuring a continuity of connection between the mark and the underlying goodwill.¹⁰⁴ Because of this, creating a security interest that covers only the mark and not any of the business or business assets associated with the goodwill symbolized by the mark leaves the creditor in a position from which it cannot effectively foreclose its interest without creating an invalidating assignment-in-gross.¹⁰⁵

Part B. Licenses and Other Contracts as Collateral

IX. Character of Contract-Based Financing

Intellectual property rights provide one direct focus for financing, but an alternative basis lies in using the contract rights that may arise with respect to intellectual property and, most specifically, rights associated with licenses or assignments of information and intellectual property. Commercial use of contract rights as collateral has widespread application in modern financing. When brought into the context of licensing law, however, the nature of the contracts,

¹⁰⁰ See, e.g., *Marshak v. Green*, 746 F2d 927 (2d Cir. 1984); *Pepsico, Inc. v. Grapette Co.*, 416 F2d 285 (8th Cir. 1969); *Ph. Schneider Brewing Co. v. Century Distilling Co.*, 107 F2d 699 (10th Cir. 1939).

¹⁰¹ *McCarthy on Trademarks* § 18.48 (1999). See generally *Dawn Donut Co. v. Hart’s Food Stores, Inc.*, 267 F2d 358 (2d Cir. 1959); *Kentucky Fried Chicken Corp. v. Diversified Packaging Corp.*, 549 F2d 368 (5th Cir. 1977).

¹⁰² See, e.g., *In re Roman Cleanser Co.*, 802 F2d 207 (6th Cir. 1986) (trademark security interest not an assignment in gross). See also *Restatement (Third) of Unfair Competition* § 34, comment e (1995).

¹⁰³ See *Gaia Technologies, Inc. v. Reconversion Technologies, Inc.*, 93 F3d 774 (Fed. Cir. 1996); *Li’l Red Barn, Inc. v. Red Barn Systems, Inc.*, 322 F. Supp. 98 (ND Ind. 1970), *aff’d*, 174 USPQ 193 (7th Cir. 1972).

¹⁰⁴ See, e.g., *In re Roman Cleanser Co.*, 802 F2d 207 (6th Cir. 1986).

¹⁰⁵ See generally *Simensky, Enforcing Creditors’ Rights Against Trademarks*, 79 *Trademark Rep.* 569 (1989).

the rights they create, and the background of federal law in which they occur all combine to make the lending practice here unique.

To set the context for the following discussion, it is important to clearly indicate the nature of the financing structure in the context of contract-based financing. In broad terms, this breaks down into two distinct financing practice formats.

- The first deals with the transferor's use for financing purposes of rights it acquires under a contract, most frequently this focuses on the transferor's (licensor) right to receive payments from the transferee (licensee). The financing arrangement occurs when the right to receive payment is transferred to a third party (lender, buyer) as a means of converting a future payment into present cash.
- The second format occurs where the transferee (licensee) is the debtor. In this context, the licensee will use its contractual rights as a basis for obtaining funding from a third party (lender). Sometimes, the contract rights may be the only collateral, but more often they form one part of the collateral, perhaps having significance primarily because the licensed rights are important to maintaining the value and operational capacity of other property.

These two different formats entail markedly different legal issues.

X. Licensor's Interest as Collateral: Cash Flow from Contracts

Cash flow from contracts can come from a variety of underlying agreements. When the cash obligations arise from the sale of goods or services, state law (most often Article 9) governs. For cash flow from licenses or assignments, whether treated in the agreement as a form of royalty or as a deferred purchase price payment, also presents potentially significant and valuable collateral. In dealing with that collateral, however, several legal issues arise that are relatively unique to this context.

[1]. What Law Applies: Federal Law

As we have seen, the three primary federal intellectual property rights regimes have recording or filing rules that apply to certain transactions relating to intellectual property rights. The better view is that none of these statutes applies to interests taken in contractual obligations or rights, such as a right to receive royalty payments. The statutes, by their own terms and by their context deal only with interests in the intellectual property; the right to payments resulting from a transaction in reference to that property is not equivalent to a property right in the intellectual property.

This result seems perfectly clear with respect to patent and trademark law, where the recording rules deal with "assignments" or other conveyance of the property. It should also be clear with respect to copyright law where the recording statute deals only with transfers of copyright ownership.¹⁰⁶ These statutes deal with recording title to the property and not with

¹⁰⁶ 17 USC 101.

priority of rights in contractual obligations, even if associated with use or conveyance of the property. But in the copyright context, two lower court rulings place this simple conclusion under a cloud.

Among other issues, the court in *In re Peregrine Entertainment, Ltd.*,¹⁰⁷ dealt with questions about proper filing of security interests in the contract rights (licenses) associated with the intellectual property. Without substantial discussion or sufficient analysis, it held that one must file in the Copyright Office to perfect a security interest in a nonexclusive license involving a copyrighted work. *Peregrine* was followed on this issue by *In re Avalon Software, Inc.*¹⁰⁸ After holding that copyright law governed filing regarding unregistered or registered copyrights, the court extended this analysis to include the proceeds of those copyrights. This included all licenses from the software (as compared to service contract receivables). If the claim to these contract rights had been solely as proceeds, the court's conclusion here would be a follow-up from its analysis of the copyright-state law interface. In fact, however, the security interest also claimed the contract rights as direct collateral. While the court did not discuss this, by wrongly extending the copyright analysis to the contract rights, it in effect indicates that one must perfect on licenses and on license proceeds in the Copyright Office, a decision consistent with the *Peregrine* case, but at odds with the scope and character of copyright filing structure which deals solely with property rights transfers. Of course, as we have seen, a later court rejected the *Avalon* analysis as applied to unregistered copyrights and, presumably, would also have rejected that court's analysis concerning license proceeds, at least with respect to licenses of unregistered copyrights.¹⁰⁹

The better view is that, while recording in federal records may be necessary to ensure priority or validity of rights in the underlying intellectual property when a transfer occurs, that filing has no association with establishing or enforcing the interests of a third party transferee of the cash flow that comes from a transfer. Thus, the Ninth Circuit in *Broadcast Music Inc. v. Hirsch*¹¹⁰ reached the better result when it held that a contractual assignment of royalties to creditors need not be recorded under the Copyright Act. As the court analyzed this case, even though the assignment conveyed the significant beneficial interest associated with the copyright, the contract was not an assignment of the copyright, but of a contractual right to receive royalties. That being true, state law controlled and, in this case, did not require a filing to fully enforce the assignment.

This result creates a bifurcation of legal coverage that is common in relationship to title-based systems. Simply stated, the effect of a transaction in reference to establishing ownership or other property interests in the underlying intellectual property itself is governed by the property-rights law, while the effect of a transfer of the *contract* and rights under it to a third party is otherwise governed by other law.

¹⁰⁷ *In re Peregrine Entertainment, Ltd.*, 116 Bankr. 194 (CD Cal. 1990).

¹⁰⁹ *Aerocon Engineering, Inc. v. Silicon Valley Bank*, 244 BR 149 (Bankr. ND Cal. 1999) (no preemption of state law regarding unregistered copyrights).

¹¹⁰ *Broadcast Music Inc. v. Hirsch*, F3d 41 USPQ2d 1373 (9th Cir 1997) (assignment of royalties to creditors need not be recorded under copyright act provisions; this was not assignment of a copyright even though it, in effect, conveyed beneficial interest in the copyright).

[2]. What Law Governs: State Law

A wrong holding that federal law applies to some transfers of contractual rights associated with copyrights, patents or trademarks would, of course, create preemption questions like those discussed earlier. For present purposes, however, we will assume that perfection and enforcement of interests in contractual rights to receive royalty or other payments are governed by state, rather than federal law.

Given this assumption, the basic question of applicable law thus becomes a question of whether the transaction is governed by Article 9 or by general state common law and statutes. The answer to this question changed dramatically under Revised Article 9, with the effect of placing most forms of cash flow financing associated with licenses under the governance of Article 9.

Subject to two relevant exceptions we will discuss shortly, original Article 9 applies to security interests in accounts and general intangibles, and to sales of accounts and chattel paper.¹¹¹ Since this version of Article 9 defines accounts to include only rights to receive payment for the sale of goods or services, payments made pursuant to a license of information are treated as “general intangibles”, rather than accounts.¹¹² The effect is that, under original Article 9, transactions involving financing of a licensor (or assignor) based on the cash flow from licenses is within Article 9 if the transaction entails a security interest, but not if the transaction involves a sale of the contract rights to a third party.

Of course, the reason why this is significant comes from the fact that, in cash-flow based financing, sales and security interests are often treated as interchangeable since negotiated agreements can use either framework to achieve the same or at least similar economic results. Because of this commercial reality, one goal of revised Article 9 was to expand the coverage of transactions involving sales of cash flow as a form of financing. It does so in two ways, both of which affect practice in reference to intellectual property contract rights.

Initially, as discussed earlier, Revised Article 9 redefines the term “account” to expressly include rights to payment for “property that has been or is to be sold, leased, licensed, assigned or otherwise disposed of”.¹¹³ This expressly covers licenses. It yields more than just a change in language.¹¹⁴ The scope of Revised Article 9, like that of original Article 9 includes sales of accounts.¹¹⁵ That term now includes transactions that entail a sale of cash flow rights

¹¹¹ UCC § 9-102 (Original).

¹¹² UCC § 9-106 (Original). See *In re SSE International Corp.*, 198 B.R. 667 (Bankr. W.D. Pa. 1996) (settlement agreement that represented amounts due under license agreement was a general intangible for purposes of Article 9; it was not covered by a security agreement referring to “accounts”).

¹¹³ UCC § 9-102(a)(2) (Revised).

¹¹⁴ The language change, however, is also important for practice after July 2001, the effective date of Revised Article 9 because it means that security agreements that refer solely to “accounts” after that date may include in their scope the proceeds of licenses, while agreements that refer solely to “general intangibles” after that date may not include licenses. Compare *In re SSE International Corp.*, 198 B.R. 667 (Bankr. W.D. Pa. 1996) (settlement agreement that represented amounts due under license agreement was a general intangible for purposes of Article 9; it was not covered by a security agreement referring to “accounts”).

¹¹⁵ UCC § 9-109(a)(3) (Revised).

arising out of license agreements. The term also includes property that has been assigned, thus arguably also bringing within Article 9 any transaction that involves a sale of a cash flow right arising out of an assignment of a copyright, patent or the like.

The second expansion involves the term “payment intangible.” This term means a general intangible in which “account debtor’s principal obligation is a monetary obligation.”¹¹⁶ Revised Article 9 applies to security interests in and sales of payment intangibles.

The assumption under Revised Article 9 should be that all transactions involving monetary obligations are within the scope of Article 9 unless pulled out by an express exception or by a misapplied concept of preemption. Under original Article 9, it might have been better practice to make that same assumption, but as a matter of law original Article 9 does not apply to sales of monetary obligations arising out of a license or assignment of intellectual property. Indeed, this latter conclusion was one factor that resulted in one court holding that an assignment of contract royalty rights was outside Article 9 and was perfected without the need for recording in either federal or state systems.¹¹⁷

The broad coverage in both versions of Article 9 of financing based on contract rights is cut back in limited fashion by state-law exceptions from the scope of Article 9 unrelated to federal preemption issues. The exceptions, as stated in Revised Article 9 are as follows:¹¹⁸

- A sale of accounts or payment intangibles as part of a sale of the business out of which they arose.
- An assignment of accounts or payment intangibles which is for the purposes of collection only.
- An assignment of a right to payment to an assignee that is also obligated to perform under the contract.
- An assignment of a single account or payment intangible to an assignee in full or partial satisfaction of a preexisting debt.

These exceptions take the entire transaction out of Article 9, leaving questions about priority, enforceability and other matters to general common law or other applicable statutes. They replicate exceptions under original Article 9.¹¹⁹ The obvious purpose is to keep Article 9 applicability away from certain transactions that are not involved in financing the transferor-debtor.

¹¹⁶ UCC § 9-102(a)(61) (Revised).

¹¹⁷ Broadcast Music Inc. v. Hirsch, 41USPQ2d 1373 (9th Cir 1997).

¹¹⁸ UCC § 9-109(d) (Revised).

¹¹⁹ UCC § 9-104(f) (Original).

[3]. Perfecting an Interest

For transactions to which it applies, both original and revised Article 9 typically require filing in relevant state records systems in order to perfect an interest in contract rights to receive payment, whether characterized as accounts or general intangibles.¹²⁰ Both versions of Article 9 contain elaborate rules delineating which office in which state is the appropriate place to file. Under Revised Article 9, filing with respect to corporate debtors will typically be in the state where the corporation is incorporated, while under original Article 9, the appropriate state for filing with respect to corporate debtors ordinarily is the state in which the debtor's chief executive office is located.¹²¹

Both versions of Article 9, however, permit some interests to be perfected without filing. The relevant rules are substantially the same in both versions. Revised Article 9 provides:

[No filing is required to perfect an interests in] an assignment of accounts or payment intangibles which does not by itself or in conjunction with other assignments to the same assignee transfer a significant part of the assignor's outstanding accounts or payment intangibles¹²²

This rule, of course, permits the creation of hidden, unrecorded interests that will have priority under Article 9 over later transfers.¹²³

[4]. Contractual Restrictions on Transferring Cash Flow

As a general rule, parties to a contract have the right to contractually limit the persons with whom they are willing to deal. Nevertheless, for transactions within the scope of Article 9, that right is precluded with respect to transfers of payment rights.

Under Article 9, terms that require consent, that prohibit, or otherwise condition the right of the party receiving payments to transfer that right to another party are generally rendered unenforceable and without any effect.¹²⁴ This rule applies even if the remainder of the contractual relationship is nontransferable because of the personal nature of the services required of the transferor or for other reasons.

This rule of invalidation originated in original Article 9. Its impact on licensing and related practice, however, will be far more significant under revised Article 9 because of the broader scope of revised Article 9, including its application to sales of the right to receive payments under a license. The comments to the relevant Article 9 provision indicate that clauses conditioning transfers of payments streams are entirely ineffective, but they invite the courts to recognize that other terms affecting the handling of cash within a relationship are not

¹²⁰ UCC §§ 9-308(a); 9-310(a) (Revised).

¹²¹ UCC § 9-307(e) (Revised); UCC § 9-103(3) (Original).

¹²² UCC § 9-309(2) (Revised); UCC § 9-302(1)(e) (Original).

¹²³ Revised Article 9 also provides that no filing is required to perfect a *sale* of a payment intangible. The apparent distinction between a sale and an assignment is not explained in the statute.

¹²⁴ UCC § 9-406(d) (Revised); UCC § 9-318 (Original).

rendered invalid even if they may make assignment of a right to a cash flow difficult. For example, a requirement that the licensor set-aside funds received in a form of reserve would be enforceable, even though it might make any transfer of the right to payment valueless.

XI. Licensee Interest: Licensed Rights as Collateral

The circumstances become materially more complicated if a lender obtains a security interest in technology or processes that the debtor holds under a license from a third party. The threshold question in such cases centers on whether the debtor (licensee) holds any transferable interest to which the security interest can attach.

[1]. Assignability in General

As a basic premise, while modern financing law does not depend on questions about title or ownership, for something of value to serve as collateral for a loan, that something must in principle be transferable, at least to the extent that admits of the creation of a security interest.

As a general rule, the assignability of a license or similar contract will be judged under state law. State law ordinarily permits transfers of a contract right without consent of the other party unless the transfer will have a material, adverse effect on the other party or the contract itself precludes transfer. This rule governs many contracts pertaining to information and intellectual property rights. In the absence of contrary contractual terms, it ordinarily precludes transfer only special cases such as where the transfer would expose confidential material or would jeopardize a party's expectation that a particular individual or group would actually perform the contract in the sense that the contract is of a personal nature and "the performance depends upon a special relationship, special knowledge, or a unique skill, upon which the other party is entitled to rely."¹²⁵ The court in *In re Sentry Data, Inc.*,¹²⁶ applying Minnesota law, concluded that the exclusive license to market software did not create such a relationship, because performance of the contract did not depend on special action by the licensee and did not involve any obligation to protect trade secrets, but merely an obligation to market a product.

An entirely different background rule governs a licensee's interest in a nonexclusive license of federal intellectual property. In this context, cases routinely conclude that the licensee's contractual interest is *not* transferable unless the licensor consents to the transfer.¹²⁷ Applying a federal law policy derived by case law, rather than statute, courts routinely emphasize that a nonexclusive license is a limited conveyance that does not establish sufficient rights to enable the transferee to make a reconveyance without permission of the licensor. This result flows in part from the concept that a non-exclusive license is personal in nature.¹²⁸ In

¹²⁵ *In re Rooster*, 100 BR 228 (Bankr. ED Pa. 1989)(Pennsylvania law).

¹²⁶ *In re Sentry Data, Inc.*, 87 BR 943 (Bankr. ND Ill. 1988).

¹²⁷ See *Unarco Indus., Inc. v. Kelley Co.*, 465 F.2d 1303, 1306-07 (7th Cir. 1972), cert. denied, 410 U.S. 929 (1973); *PPG Industries, Inc. v. Guardian Industries Corp.*, 597 F.2d 1090 (6th Cir.), cert. den., 444 US 930 (1979); *Harris v. Emus Records Corp.*, 734 F.2d 1329, 1332-33 (9th Cir. 1984) (copyright); *In re Alltech Plastics, Inc.*, 71 B.R. 686, 688-89 (Bankr. W.D. Tenn. 1987) (patent).

¹²⁸ See *Gilson v. Republic of Ireland*, 787 F.2d 655, 658 (D.C.Cir.1986) ("It is well settled that a non-exclusive licensee of a patent has only a personal and not a property interest in the patent and that this personal right cannot

addition, as described by the court in *Everex Systems, Inc. v. Cadtrax Corp. (In re CFLC, Inc.)*,¹²⁹ a case dealing with a non-exclusive patent license, allowing "free assignability ... of nonexclusive patent licenses would undermine the reward that encourages invention because a party seeking to use the patented invention could either seek a license from the patent holder or seek an assignment of an existing patent license from a licensee. In essence, every licensee would become a potential competitor with the licensor-patent holder in the market for licenses under the patents." The rule against transferability is a preemptive federal law rule.¹³⁰

[2]. Revised Article 9: Creating Interests in Licensee Rights

While the rule against transferability rests on a federal law policy and cannot be changed by state law, Revised Article 9 purports to provide a state law financing rule that allows some use of licensee interests as collateral even without the assent of the licensor.

These new provisions are premised on a purported distinction between transfer on the one hand and the mere creation or perfection of a security interest on the other. Section 9-408 of Revised Article 9 *invalidates* both contractual restrictions and rules of law that preclude or condition the creation or perfection of a security interest in a general intangible, including a license. The provision regarding any contrary rule of law reads as follows:

A rule of law, statute, or regulation that prohibits, restricts, or requires the consent of a government [or an] account debtor to the assignment or transfer of, or creation of a security interest in, a ... general intangible, including a contract, permit, license, or franchise between an account debtor and a debtor, is ineffective to the extent that the rule of law ...

- (1) would impair the creation, attachment, or perfection of a security interest;
or
- (2) provides that the creation, attachment, or perfection of the security interest may give rise to a default, breach, right of recoupment, claim, defense, termination, right of termination, or remedy ...¹³¹

be assigned unless the patent owner authorizes the assignment or the license itself permits assignment."); *Stenograph Corp. v. Fulkerson*, 972 F.2d 726, 729 n. 2 (7th Cir.1992) ("Patent licenses are not assignable in the absence of express language."); *Rock-Ola Manufacturing Corp. v. Filben Manufacturing Co.*, 168 F.2d 919, 922 (8th Cir.), cert. dismissed, 335 U.S. 855-6, 69 S.Ct. 134, 93 L.Ed. 403 (1948); *E.I. du Pont de Nemours & Co. v. Shell Oil Co.*, 498 A.2d 1108, 1114 (Del.1985) (rights conveyed by nonexclusive patent license are personal to licensee and not susceptible to sublicensing unless specific permission given).

¹²⁹ *Everex Systems, Inc. v. Cadtrax Corp. (In re CFLC, Inc.)*, 89 F.3d 673 (9th Cir. 1996).

¹³⁰ But see *Institut Pasteur v. Cambridge Biotech Corp.* (The court did not contest the relevance of the basic federal policy, but noted that Chapter 11 presumes a continuation of the prior debtor, albeit under a different legal structure. Viewed in this manner, in a Chapter 11 case at least, unless the debtor proposes to transfer the license to a new party, the risks involved in the federal policy are not presented. The license enters the bankruptcy estate.). See also *Summit Inv. & Dev. Corp. v. Leroux*, 69 F.3d 608 (1st Cir. 1995).

¹³¹ UCC § 9-408(c) (Revised). It should be noted that, while this discussion emphasizes the effect of this rule on non-transferable licensee interests, the rule itself applies with equal force to any limit on transferability of the licensor's rights (other than the right to receive payment, which is fully allowed to be transferred).

Quite obviously, this rule cannot over-ride federal law, if applicable. Thus, the focus of the rule properly understood deals with two issues. The first is to create, under state law, the broadest possible reach for attaching a security interest. Contrary state laws and contractual agreements cannot prevent the creation or attachment of a security interest. Secondly, the provisions of this section create a basis for arguing that the federal rule only precludes an actual transfer to a third person, not merely the creation of an inert right. In effect, the argument is that the federal rule (or contract term) might be implicated in any eventual effort to foreclose on and sell the license interest, but that it does not come into play at the level of mere creation of the interest.

Under revised Article 9, if the contract term or the other rule of law preventing or conditioning transfer would be enforceable were it not for the new Article 9 invalidation rule, then the extent of the invalidation under Article 9 is quite limited. Section 408 sets out six express limits on its rule and what the creditor can do with the interest it can create despite contrary contract or legal terms. These include that the interest created in the licensee's interest:

- is not enforceable against the licensor
- does not impose duties or obligations on the licensor
- does not require that the licensor render any performance to the lender
- does not entitle the lender to use or assign the licensee's rights under the license
- does not entitle the secured party to use, assign, possess, or have access to any trade secrets or confidential material, and
- does not entitle the secured party to enforce the security interest¹³²

Overall, then, what is created under Revised Article 9 is a non-waivable, non-alterable right to create a security interest in a license, but only to create and perfect the interest, not to enforce it. This is a passive property right whose value may not be immediately apparent. That value emerges, however, when one considers that creating the security interest gives the lender a right to the proceeds of any sale of its collateral. Thus, if the license were sold (for example, as part of a liquidation of a bankruptcy estate), the lender's lien would attach to the proceeds of sale and, like any other security interest, would take priority over unsecured creditor and ownership interest. That, indeed, is the primary intended effect of the rule.

¹³² UCC § 9-408(d) (Revised).

XII. Priority Issues and Licenses

When two or more parties claim an interest in a single asset, in this case, a license or other contractual right, the resulting legal issue is treated in modern commercial finance law as a question of resolving priority of rights in that asset. We previously discussed priority issues focused on ownership claims and the role of federal law in that context. Here we focus on the relationship of priority questions associated with contractual rights. Yet, even so, we will have to deal with questions about the role of ownership.

The easiest contest to understand involves a fact setting in which two persons claim a direct interest in contractual rights of a debtor. Here, the issue does not seem to depend on whether the debtor is licensor or licensee in the particular contracts. Under either assumption, the core issue centers on whether the priority conflict is resolved under federal or state law. That, in turn, depends on what type of contracts are involved, what rights are claimed as collateral in reference to that contract, and as previously discussed what is the scope of the particular federal recording rule involved.

In general, the three primary federal statutes do not deal with security interests or other transfers of rights in a contract. Properly understood, the federal statutes primarily concern priority of rights in property which rights may be transferred by contract. For example, consider the following:

Illustration 14.7. Trademark Owner enters into a contract to assign its mark to Buyer-1. Subsequently, Trademark Owner enters into a second contract to assign the same mark to Buyer-2. In addition, Trademark Owner has security agreements with Lender 1 and Lender 2, both of which cover contracts with respect to the mark, but do not purport to create any security interest in the mark itself.

When the issue concerns a conflict over ownership of an intellectual property right, the federal priority rules may apply. As we have seen, those rules give precedence to the first transfer to be made, so long as it is recorded within a stated grace period. Federal law of that type would control in any conflict between Buyer-1 and Buyer-2, both of whom, in separate contracts, sought to purchase the mark. This is a question concerning property rights, not priority of claims to contract rights.

In contrast, in Illustration 14.8, Lender 1 and Lender 2 have an interest in the debtor's contract rights. A conflict over who has precedence with respect to, for example, rights to payment under the contract with Buyer-1 should be resolved under state law. That conflict does not concern ownership of the trademark, but a conflict of claims to rights under the particular contract.

As we previously discussed, however, two lower courts have held that copyright law recording rules cover not only the property rights dispute, but also this latter question about perfection and priority with reference to the contract rights. When placed into a context dealing with priority rules, this result if it stands has great significance. The Article 9 priority

rule with respect to the contract right dispute gives priority to the first lender to file or perfect its interest.¹³³ The property law rule deals with the issue differently. We believe that the Article 9 rule should apply to the disputer between lenders over rights to the rights contained in a contract, but given the presence of two lower court rulings in the field of copyright law, the potential of a contrary result cannot be dismissed.

Another type of priority conflict that affects licenses involves the mixed context in which ownership interests are involved and the conflict pertains to the rights of the licensee (or other transferee) against the other interest holder. If the transferee takes an ownership interest and the contract pertains to a transfer of ownership in a form covered by federal law recording rules, then the conflict will be resolved based on the federal priority rule. For now, however, we will assume that the transaction is a license of a type not directly covered by the federal priority rules we have already discussed.

The Copyright Act Section 205(e) provides that a non-exclusive license, whether recorded or not, prevails over a conflicting transfer of copyright ownership if the license is in a written instrument signed by the rights owner and either:

- the license was taken before the conflicting ownership transfer was executed; or
- the license was taken in good faith before the recordation of the transfer and without notice of it.¹³⁴

This rule, which has not been extensively litigated, has several important implications for financing that pertains to copyright interests and licenses. In understanding the significance of these, it is important to recall that the copyright law concept of a “transfer of ownership” includes a security interest. Thus, Section 205(e) arguably states priority law as between a secured party and a licensee, displacing any contrary state law.¹³⁵

First, copyright law rule confirms a limited, but important principle of first in time (or first to occur). In effect, a transferee of copyright ownership takes subject to existing, written non-exclusive licenses, even though not recorded. That rule, however, does not apply to licenses that are not in writing. The omission could mean several things. For example, one could simply argue that the issue was left to state law. While a possible argument, the more natural implication of the statutory language is that the unsigned or oral contract does not prevail over even a subsequent transfer of copyright ownership.

What about licenses taken after the transfer of ownership? The Copyright Act section gives only limited protection to such interests. The prevail over the ownership transfer only if taken in good faith and in writing before recordation of the transfer. These limited protection seems to confirm the converse assumption that, after a recorded transfer of ownership, licenses take subject to that recorded transfer. In effect, the nonexclusive license

¹³³ UCC § 9-322 (Revised); UCC § 9-312(5) (Original).

¹³⁴ 17 USC § 205(e).

¹³⁵ As discussed earlier, there is a disagreement in courts over whether the primary copyright law priority rule applies to unregistered copyrights, but the language of 205(e) seems less conditioned on the recording rules.

gives rights only if obtained from the record owner of the copyright or its authorized agent and, then, only under a concept of consent or authorization.

These rules do not, of course, apply patents or trademarks and licenses in them and do not apply to interests in intellectual property arising solely under state law. With reference to the federal intellectual property, however, it is likely that the rules of Section 205(e) would be inferred from the nature of a title-based system, except perhaps for the requirement of a writing to document the prior license.

What role remains for state law on this issue? Clearly, state law rules apply to purely state law interests. In addition, in the patent and trademark context, it is possible that state law, rather than an inference from the nature of the title records system should control in order to fit this area of practice more smoothly into general commercial law. That is an especially strong argument when, as in trademark and patent law, there is no clear treatment of transactions involving less than a full sale of the right.

The issue has special importance under Revised Article 9 since that statute adopts a rule regarding licenses that conflicts with the approach seemingly taken in the Copyright Act. Section 9-321 creates a new concept of “licensee in the ordinary course of business” and provides that such a licensee, under a non-exclusive license takes free of any security interest in the underlying property rights even if that security interest is perfected and the licensee knows that it exists.

This rule comes from a model created in original Article 9 for transactions in goods and reflects a concept of bona fide purchaser protection applicable to cases where an actual transfer of possession or potential thereof gives indicia of ownership that are protected in the general marketplace. As applied to licenses, one wonders about whether its underlying concept applies, even if copyright law were to allow states to create rules contrary to its rules. Transfers of intangibles and right therein often do not bear the same indicia of rights that accompany possession and delivery of a tangible item.

Revised Article 9 contains a lengthy description of a licensee in the ordinary course of business. This definitions makes clear that the concept refers to a transferee for value and in good faith who acquires the license in the ordinary course of the licensor’s business. Furthermore, the “person becomes a licensee in the ordinary course if the license ... comports with the usual or customary practices in the kind of business in which the licensor is engaged or with the licensor’s own usual or customary practices.”¹³⁶

As this indicates, an alternative justification for this priority rule focuses on a form of implied consent on the part of the secured party. Thus, in the goods world, a lender who takes as collateral the goods inventory of the debtor knows and implicitly consents to the fact that the debtor will try mightily to sell those goods and that the buyers should take from of the interest. The analogy here makes sense in a retail context where one deals with mass-market world, but it strains somewhat in a world where intangibles may or may not be

¹³⁶ UCC § 9-321(a) (Revised).

licensed to others. Of course, however, Article 9 applies its rule only if the debtor/ licensor is in the business of licensing intellectual property of the kind.

Part C. Bankruptcy Issues

XIV. Rights and Goodwill As Assets

The bankruptcy estate consists of all property owned by the debtor at the time of the bankruptcy petition and any property acquired by the estate after the filing. 11 USC § 541. Post-petition rights engendered from pre-petition property become property of the estate (e.,g., royalties earned from pre-petition copyrighted works). There is an exception for post-petition value obtained through *personal* services of the individual who is the debtor.

- ***Cusano v. Klein***, 60 U.S.P.Q.2d 1100 (9th Cir. 2001). Assets of songwriter's estate consisted of copyrights in songs he authored and rights to receive royalties based on pre-petition use of the songs. Plan that abandoned "songrights" at confirmation of bankruptcy plan place them back in debtor's control, giving him the right to sue for any post-petition royalties. Pre-petition royalties, however, were not properly listed in the bankruptcy filing, which referred only to "songrights of unknown value, and thus did not revert back to debtor. "Songrights" could reasonably be interpreted to mean copyrights and rights to royalty payments, and while it would have been more helpful for debtor to break down description by naming songs, albums, and royalty agreements, such details would not have revealed anything that was otherwise concealed.

Debtor's open book account claim under California law for royalties owed in connection with songs he had written accrued for bankruptcy purposes, and thus was required to be scheduled as a receivable or a cause of action after debtor filed Chapter 11 bankruptcy petition, to extent that sums were owed on account at time he filed his petition, as an action could have been brought for those sums at that time. Debtor's failure to schedule as asset open book account cause of action under California law for prepetition royalties owed in connection with songs he had written prior to filing of bankruptcy petition, or other claims for prepetition royalties, resulted in claims being vested in bankruptcy estate, and thus deprived debtor of standing to assert such a claim following confirmation of Chapter 11 plan.

- ***In re Prince***, 85 F.3d 314 (7th Cir. 1996) (Value of stock of Chapter 11 debtor's incorporated orthodontics practice included the goodwill of the practice and was not generally excluded from the estate by the statutory exclusion for personal earnings post petition. This was true even though the professional corporation did not have contractual guarantee that debtor would not leave practice and compete with it as debtor's assets were valued at time plan was confirmed when debtor owned stock himself and was not likely to compete with himself. The goodwill could be transferred by covenants not to compete and other devices. In this case, however, the value could not include the value of the doctor's future personal services because 11 USC 541(a)(6) excludes this. "In an important sense, however, Dr. Prince's goodwill

is unlike his skills, his schooling, or his dental license. These components of Dr. Prince's human capital can only manifest their value by increasing the worth of his future labors. Dr. Prince's innate physical ability, his personality, or his professional degree increase the market value of his services, but they cannot be sold to another orthodontist; they have value only as attributes of Dr. Prince. On the other hand, Dr. Prince's goodwill, like the practice's physical equipment, can be sold and transferred, and once sold and transferred can generate value for another orthodontist. Although the mechanism of using his best efforts to transfer his patients' loyalties to Dr. Clare and then securing the transfer with a covenant not to compete is not as simple as signing over title to a physical asset, the functional effect is the same. ... Thus, Dr. Prince's goodwill is not intrinsically part of his human capital, but rather is a separate intangible capital asset of the practice, like a trademark would be.”)

- ***Shanno v. Magee Indus. Enter., Inc.***, 856 F.2d 562, 566 (3d Cir.1988) (In most cases, liquidation value is only an appropriate estimation of stock worth where a company is dissolving. In dissolution, liquidation distributions are the only foreseeable future cash flows to the shareholder, and thus liquidation value is an accurate tool for measuring the stock's present value. On the other hand, where a business is expected to continue as a going concern, the company's expected future earnings from operations often far exceed the liquidation value of the company's physical assets.
- ***In re FitzSimmons***, 725 F.2d 1208, 1211 (9th Cir.1984) Involved an individual attorney operating his practice as a sole proprietorship, a situation quite analogous to Dr. Prince and his wholly owned professional corporation. The attorney, FitzSimmons, objected to being directed to pay any of his practice's future profits to his creditors as part of a Chapter 11 reorganization, arguing that the profits were excluded from the bankruptcy estate by § 541(a)(6). The Ninth Circuit held: FitzSimmons is thus entitled to monies generated by his law practice only to the extent that they are attributable to personal services that he himself performs. To the extent that the law practice's earnings are attributable not to FitzSimmons' personal services but to the business' invested capital, accounts receivable, *good will*, employment contracts with the firm's staff, *client relationships*, fee agreements, or the like, the earnings of the law practice accrue to the estate.
- ***In re Andrews***, 80 F.3d 906 (4th Cir. 1996). Chapter 7 debtor sought to exclude from debtor's estate all postpetition payments due debtor under noncompetition agreement. Held: postpetition payments to debtor pursuant to noncompetition agreement were not "earnings from services performed," and thus, payments could not be excluded from bankruptcy estate. According to the majority, this result would hold even if the no-compete contract were treated as executory because payments were plainly rooted in, and grew out of, debtor's prepetition sale of debtor's share in ready-mix concrete business. Forebearance (e.g., non-competition, was not treated as later personal services. "Pre-petition assets, like the NCA payments, are those assets rooted in the debtor's pre-petition activities, including any proceeds that may flow from those assets in the future. These assets belong to the estate and ultimately to the creditors.

Post-petition assets are those that result from the debtor's postpetition activities and are his to keep free and clear of the bankruptcy proceeding.”)

- **Non-Compete** in connection with sale of assets is treated as a means of conveying and preserving the goodwill. Payments on them will be treated as assets associated with the sale and thus, with pre-petition activity.
 - *Unsecured Creditor's Committee v. Prince (In re Prince)*, 127 B.R. 187, 192 (N.D.Ill.1991) (holding that agreement not to compete provided in conjunction with sale of business is agreement not to undermine value of goodwill that has been sold)
 - *In re Mid-West Motors, Inc.*, 82 B.R. 439 (Bankr.N.D.Tex.1988) ("Such [non-competition] provisions are necessary to secure the goodwill purchased by the buyer of the business.").
- **Casey v. Hochman**, 963 F.2d 1347 (10th Cir. 1992) (Patent on device invented by debtor after filing of his original Chapter 11 petition, as well as any income derived from patent, were assets of debtor individually and excluded from property the estate.)
- **In re Tudor Motor Assoc.**, 102 B.R. 936, 948 (D.N.J.1989) ("franchisee's contractual rights in a Franchise Agreement are generally considered property of the estate, except where said agreements have been effectively terminated prior to a debtor's filing.")
- **Krebs Chrysler-Plymouth, Inc. v. Valley Motors, Inc.**, 141 F.3d 490 (3d Cir. 1998) (Under Pennsylvania law, "[t]he ownership of a trade-mark has, in general, been considered as a right of property." "Trademarks are property, and franchises are licenses to use such property. Thus, under Pennsylvania law, these franchises are interests in property, and as such are property of the estate under section 541.")
- **Trademarks and Bankruptcy Generally**
 - Stuart M. Riback, *The Interface of Trademarks and Bankruptcy*, J. Proprietary Rts., June 1994, at 2
 - David M. Jenkins, *Licenses, Trademarks, and Bankruptcy, Oh My!: Trademark Licensing and the Perils of Licensor Bankruptcy*, 25 J. Marshall L.Rev. 143, 155-59 (1991)
 - Richard Lieb, *The Interrelationship of Trademark Law and Bankruptcy Law*, 64 Am. Bankr.L.J. 1, 35-38 (1990).

XV. Sales of Rights in Bankruptcy

Section 363 allows the sale of assets of the estate, either in the ordinary course of business or otherwise with the approval of the court. 11 USC § 363.

- ***In re Cult Awareness Network, Inc.***, 151 F.3d 605 (7th Cir. 1999) The court held that an anti-cult organization that objected to the sale of its trade-name, in its Chapter 7 case, to alleged affiliate of a church believed by organization to be cult, lacked standing to object to that sale. In the Chapter 7 case, the debtor had no pecuniary interest in the trade-name. There were, according to this court, no exceptions to pecuniary interest standing rule for debtor's Lanham Act and First Amendment claims.
- ***In re Gucci***, 126 F.3d 380 (2d Cir. 1997). Court held that a buyer at a bankruptcy sale of assets including trademarks was a good faith buyer even though evidence indicated that it intended to reject licenses and perhaps destroy the transferred trademark. "There is no question that some consequences of this sale are unsettling. As a result of it, several businesses that have made substantial investments to develop a market for Paolo Gucci goods will suffer. However, contrary to arguments made by appellants, Guccio Gucci's intent to terminate trademark licenses and destroy the trademarks themselves did not constitute bad faith within the meaning of § 363(m), nor does it violate public policy. Any apparent inequities in this case are as much an indictment of bankruptcy law generally as they are of the Gucci companies' intended use of the assets.... We conclude that Guccio Gucci's intended use of the assets purchased is not relevant to the good faith inquiry, and therefore we agree with the bankruptcy court's determination that Guccio Gucci is a good faith purchaser within the meaning of § 363(m)."
- ***Hoese Corp. v. Vetter Corp. (In re Vetter Corp.)***, 724 F.2d 52 (7th Cir. 1983) (objector who challenged debtor's sale of assets to newly formed corporation could not premise a lack of good-faith defense upon knowledge of patent infringement when the issue of patent infringement was not before the Bankruptcy Court, and therefore, the newly formed corporation was a good-faith purchaser)
- ***Kennedy v. Wright***, 867 F.2d 616 (Fed. Cir. 1989) (unpublished) (Kennedy, the inventor and patentee, sued Wright for infringement, but Wright set up as a defense, and the trial court held, that the suit could not be maintained because Wright had bought and paid for the patents and become their equitable owner. This occurred as a result of a bankruptcy sale. Kennedy, however, contends that the bankrupt, NPI, never was more than a licensee and he had validly revoked the license before the sale. The court held that, despite arguments that the debtor was a mere licensee, the defendant could assert as a defense that it took from an assignor (the debtor) with valid right to transfer ownership and that this was proper because the patent owner was the alter ego of the bankrupt company.)

- ***Denbicare USA, Inc. v. Toys R Us, Inc.***, 84 F.3d 1143 (9th Cir. 1996) (Bankruptcy trustee's sale of reusable diapers packaged in box that was subject to copyright protection, for original owner of copyright, in foreign trade zone subject to United States jurisdiction, was "first sale," barring subsequent copyright owner's right to claim that later sale of those particular boxes of diapers infringed owner's exclusive right of distribution. Owner of copyright in packaging for reusable diapers consented to sale of particular boxes of diapers by owner's bankruptcy trustee, for purpose of first sale doctrine. "When McCoy objected to the sale of the diapers, he could have exercised his right as the owner of the copyright in the diaper boxes to prevent the bankruptcy trustee's sale altogether. The proposed sale would have constituted a distribution of copies of the copyrighted work, and McCoy, as the copyright owner, had the exclusive right under § 106(3) to make or authorize such distributions. Without his authorization, the bankruptcy trustee's sale--a sale of copies located within the physical territory of the United States that required the approval of a federal court in California--would have been an infringement of his copyright. Instead of seeking to prevent this infringing sale, however, McCoy stipulated in court that the sale could proceed if the buyers were enjoined from reselling in the United States and Canada. Thus, McCoy consented to the sale of the copies; the fact that the buyers later violated the conditions imposed on the sale does not negate his consent.")
- ***Men's Sportswear, Inc. v. Sasson Jeans, Inc.***, 834 F.2d 1134 (2nd Cir. 1987) Licensor's failure to object to the bankruptcy court's assumption of "core jurisdiction" at any point in the extensive proceedings on Chapter 11 debtor's action for breach of license agreements and advertising plan and further failure to object to any part of the appeal process in the district court constituted "consent" to final adjudication of action before the bankruptcy court and permitted the bankruptcy court to enter final judgment as if action were "core proceeding".
- ***Krebs Chrysler-Plymouth, Inc. v. Valley Motors, Inc.***, 141 F.3d 490 (3d Cir. 1998) (Chapter 11 debtor-automobile dealership moved to reject buy-sell agreement for its interest in one of three franchises and to assume and sell all three franchise agreements. Held that manufacturer was not "person aggrieved" by bankruptcy court orders permitting debtor to reject buy-sell agreement and to assume and sell franchises and that appeal from bankruptcy court's orders was rendered moot by buyer's failure to obtain stay of sale pending appeal. Section 363(m) applies to the sale of the franchises.)
- ***Kuntz v. Cray Computer Corp. (In re Cray Computer Corp.)***, 97 F.3d 1464 (10th Cir. 1996) (Court rejects contest about the validity of a bankruptcy sale of patents where no stay pending appeal was granted)
- ***La Preferida, Inc. v. Cervecería Modelo, S.A.***, 914 F.2d 900 (7th Cir. 1990) Distributor, which had operated under distributorship agreement of malt beverage trademark holder, brought action against trademark holder's transferee. Held: consent judgment entered in trademark transferor's bankruptcy did not preclude relitigation of

whether transferor had breached distribution agreement with its exclusive distributor, but bankruptcy sale was binding on trademark transferor's exclusive distributor.

XVI. Contract Rights: General

The bankruptcy estate incorporates all contract rights existing at the time of the bankruptcy filing. 11 USC § 541. There is special treatment for so-called executory contracts, which are contracts where important performance remains outstanding on both sides of the transaction at the time of bankruptcy. 11 USC § 365.

- *In re Andrews*, 80 F.3d 906 (4th Cir. 1996). Postpetition payments to debtor pursuant to noncompetition agreement were not "earnings from services performed," and thus, payments could not be excluded from bankruptcy estate. "Pre-petition assets ... are those assets rooted in the debtor's pre-petition activities, including any proceeds that may flow from those assets in the future. These assets belong to the estate and ultimately to the creditors. Post-petition assets are those that result from the debtor's postpetition activities and are his to keep free and clear of the bankruptcy proceeding.")
- *Cusano v. Klein*, 60 U.S.P.Q.2d 1100 (9th Cir. 2001). Debtor's open book account claim under California law for royalties owed in connection with songs he had written accrued for bankruptcy purposes, and thus was required to be scheduled as a receivable or a cause of action after debtor filed Chapter 11 bankruptcy petition, to extent that sums were owed on account at time he filed his petition, as an action could have been brought for those sums at that time. Debtor's failure to schedule as asset open book account cause of action under California law for prepetition royalties owed in connection with songs he had written prior to filing of bankruptcy petition, or other claims for prepetition royalties, resulted in claims being vested in bankruptcy estate, and thus deprived debtor of standing to assert such a claim following confirmation of Chapter 11 plan.

XVII. Executory Contracts

Under Section 365, a debtor in possession or a trustee may assume or reject an executory contract. If a trustee of debtor-in-possession meets the Bankruptcy Code's requirements for assumption of an executory contract, it must assume the executory contract entirely. 11 USC 365. Once a trustee assumes an executory contract, the Bankruptcy Code also authorizes assignment. Bankruptcy law generally supports the right to assign, and allows a trustee to assume and assign executory contracts regardless of applicable laws or contractual provisions restricting assignment.

[1]. Licenses as Executory Contracts: Generally

- *Fenix Cattle Co. v. Silver (In Re Select-A-Seat Corp.)*, 625 F.2d 290, 292 (9th Cir.1980) ("an obligation of a debtor to refrain from selling software packages under an exclusive licensing agreement made a contract executory as to the debtor

notwithstanding the continuing obligation was only one of forbearance.")

- ***Lubrizol Enterprises, Inc. v. Richmond Metal Finishers, Inc.***, 756 F.2d 1043 (4th Cir.1985) (continuing duties of notice and forbearance render a technology license contract executory for the purposes of § 365; "although the license to Lubrizol was not exclusive RMF owed the same type of unperformed continuing duty of forbearance arising out of the most favored licensee clause running in favor of Lubrizol. Breach of that duty would clearly constitute a material breach of the agreement.").
- ***Everex Sys., Inc. v. Cadtrak Corp. (In re CFLC, Inc.)***, 89 F.3d 673, 679-80 (9th Cir.1996) (license is an executory contract: "Cadtrak owes significant continued performance to the licensee: it must continue to refrain from suing it for infringement, since a nonexclusive patent license is, in essence "a mere waiver of the right to sue" the licensee for infringement. ... The licensee also owes performance: it must mark all products made under the license with proper statutory patent notice. Since failure to mark deprives the patent holder of damages in an infringement action before the infringer has actual notice of the infringement, the licensee's performance of this duty is material. Therefore, the license is an executory contract under § 365.).
- ***In re Superior Toy & Mfg. Co., Inc.***, 78 F.3d 1169 (7th Cir. 1996) (Doctrine of estoppel barred Chapter 7 trustee from arguing that bankruptcy court erred in entering assumption order on grounds that debtor's licensing agreement was not executory contract; trustee's predecessor assumed licensing agreement with court approval, contracting party honored contract and allowed debtor to retain exclusive license, and bankruptcy estate benefited from contract for almost two years.)
- ***Otto Preminger Films, Inc. v. Quintex Entertainment Inc.***, 950 F.2d 1492 (9th Cir. 1991) Contract between debtor-film company and distributor which gave distributor exclusive right to subdistribute motion pictures and to colorize and distribute colorized versions of motion pictures was "executory contract," and thus, contract had to be assumed in order to be considered part of bankruptcy estate subject to sale, where agreement contained several significant unperformed obligations of both parties. Subdistribution agreement between debtor-film company and distributor and colorization agreement were not severable so as to make only one portion of contract executory and to allow sale of nonexecutory portion as asset of bankruptcy estate. However, television contracts between actor and debtor-film company were not executory and were properly sold as assets of debtor's estate, where contracts contained no substantial unperformed duties owed by actor or his agent to debtor.
- ***In re Three Star Telecast, Inc.***, 93 B.R. 310, 312 (D.P.R.1988) (television program licensing agreement)
- ***In re New York Shoes, Inc.***, 84 B.R. 947, 960 (Bankr.E.D.Pa.1988) (trademark contract).

- *In re Best Film & Video Corp.*, 46 B.R. 861, 869 (Bankr.E.D.N.Y.1985) (movie distribution contract).

[2]. Effect of Bankruptcy Termination Clauses

- *Computer Communications, Inc. v. Codex Corp.*, 824 F.2d 725 (9th Cir. 1987) (Unilateral termination of joint marketing and development agreement to purchase computer equipment from debtor after debtor filed petition for reorganization violated automatic stay. Contractual clause allowing for termination upon either party's declaration of bankruptcy was void.)

[3]. Employment Contracts

- *Cinicola v. Sharffenberger*, 248 F.3d 110 (3d Cir. 2001) Trustee of debtor-healthcare system sought approval of proposed settlement agreement involving sale of assets and assignment of executory contracts, including employment contracts of some physicians, who then objected to the sale arguing that it assignment of their contracts to a non-affiliate hospital without their consent violated their employment agreements, and that adequate assurance of assignee's future performance of their contracts had not been provided. Although the sale was approved, on appeal, the court held remanded for determination of the effect, if any, that vacating or modifying the assumption and assignment order would have on the overall sale. If assignment of their contracts were to be vacated, physicians might have claim for rejection damages, and covenants not to compete contained in the contracts might have survived physicians' resignations.

[4]. Non-Competition Agreements

- *In re Andrews*, 80 F.3d 906 (4th Cir. 1996) (Postpetition payments to debtor pursuant to noncompetition agreement were not "earnings from services performed," and thus, payments could not be excluded from bankruptcy estate. According to the majority, this result would hold even if the no-compete contract were treated as executory because payments were plainly rooted in, and grew out of, debtor's prepetition sale of debtor's share in ready-mix concrete business. Forebearance (e.g., non-competition) was not treated as later personal services. "Pre-petition assets, like the NCA payments, are those assets rooted in the debtor's pre-petition activities, including any proceeds that may flow from those assets in the future. These assets belong to the estate and ultimately to the creditors. Post-petition assets are those that result from the debtor's postpetition activities and are his to keep free and clear of the bankruptcy proceeding.")
- *In re McDaniel*, 141 B.R. 438, 440 (Bankr.N.D.Fla.1992) (payments to former employee in exchange for non-competition agreement not made for services performed and thus not excluded from estate under § 541(a)(6)); *In re Bluman*, 125 B.R. 359, 363 (Bankr.E.D.N.Y.1991) (same).

- *In re Hughes*, 166 B.R. 103, 105 (Bankr.S.D.Ohio 1994) (obligation to refrain from competition does not make no-compete contract an executory contract); *In re Pavaglio*, 1995 WL 465339 (Bankr.M.D.Pa.1993); *In re Drake*, 136 B.R. 325, 327-28 (Bankr.D.Mass.1992); *In re Oseen*, 133 B.R. 527, 529 (Bankr.D.Idaho 1991); *In re Bluman*, 125 B.R. at 362; *In re Cutters*, 104 B.R. 886, 890 (Bankr.M.D.Tenn.1989).
- *In re Hammond*, 35 B.R. 219 (Bankr.W.D.Okla.1983) (payments pursuant to a noncompetition agreement are not "property" within the meaning of § 541(a)(1); debtor had "not done all acts necessary to accrue his right to the future payments." The court went on to assert that, in order to receive the payments, "Hammond must abide by the agreement. We cannot force him to comply.")
- *In re Udell*, 18 F.3d 403 (7th Cir. 1994) (In a Chapter 13 case, employer's right to injunction to prevent former employee from violating his covenant not to compete did not qualify as a "claim" dischargeable in bankruptcy, but bankruptcy court could lift stay to allow creditor to seek permanent injunctive relief only after considering prejudice to debtor or bankruptcy estate, relative hardship to debtor and employer, and employer's probability of success on merits. For bankruptcy purposes, a "debt" is a liability on a "claim." 11 U.S.C. § 101(12). Under § 101(5) of the Code, a "'claim' means"-- (A) right to payment ... or (B) right to an equitable remedy for breach of performance if such breach gives rise to a right to payment, whether or not such right to an equitable remedy is reduced to judgment, fixed, contingent, matured, unmatured, disputed, undisputed, secured, or unsecured.")

[5]. Assumption of Licensee's Interest in License

- *Gardner v. Nike, Inc.*, 2002 WL 123296 (9th Cir. 2002) (Exclusive licensee did not have right to re-sell or sublicense copyright without consent of owner.)
- *In re Catapult Entertainment, Inc.*, 165 F.3d 747 (9th Cir. 1999) Debtor-in-possession (DIP) may not assume executory contract over nondebtor's objection if applicable law would bar assignment to hypothetical third party, even where DIP has no intention of assigning contract in question to any such third party. In this case, federal patent law made the nonexclusive patent licenses personal and nondelegable, thus barring debtor from assuming patent licenses without licensor's consent.
- *Everex Sys., Inc. v. Cadtrak Corp. (In re CFLC, Inc.)*, 89 F.3d 673, 679-80 (9th Cir.1996) (federal patent law of nonassignability preempts state law relating to patent license assignability; prevents assumption or assignment of the license in bankruptcy; "Allowing free assignability -- or, more accurately, allowing states to allow free assignability--of nonexclusive patent licenses would undermine the reward that encourages invention because a party seeking to use the patented invention could either seek a license from the patent holder *or* seek an assignment of an existing patent license from a licensee. In essence, every licensee would become a potential

competitor with the licensor-patent holder in the market for licenses under the patents. And while the patent holder could presumably control the absolute *number* of licenses in existence under a free-assignability regime, it would lose the very important ability to control the *identity* of its licensees. Thus, any license a patent holder granted--even to the smallest firm in the product market most remote from its own--would be fraught with the danger that the licensee would assign it to the patent holder's most serious competitor, a party whom the patent holder itself might be absolutely unwilling to license. As a practical matter, free assignability of patent licenses might spell the end to paid-up licenses such as the one involved in this case.").

- ***In re Alltech Plastics, Inc.***, 5 U.S.P.Q.2d 1806 (Bankr.W.D.Tenn.1987) (Section 365(c) precluded an entity, which had acquired the corporate debtor's stock pursuant to a chapter 11 reorganization plan, from exercising the debtor's rights under a prepetition patent license. Following the conversion of its original chapter 11 reorganization case to a chapter 7 liquidation, Alltech discontinued all operations and discharged its employees. Before the debtor once again converted to chapter 11, its trustee liquidated virtually all its assets, except for its patent license. Noting that plan confirmation is a fact-intensive, equity-based inquiry, the bankruptcy court characterized the sale of Alltech's stock as a *de facto* assignment of the patent license to a noncontracting party.)
- ***Harris v. Emus Records Corp.***, 734 F.2d 1329 (9th Cir. 1983) (copyright license is not transferable and does not become part of bankruptcy estate)
- ***Institut Pasteur v. Cambridge Biotech Corp.***, 104 F.3d 489 (1st Cir. 1997) (Chapter 11 reorganized debtor was not different entity from that with which patent holder entered into licensing agreement, so that federal common law and contractual restrictions against assignment of patent licenses did not preclude assumption of license by Chapter 11 debtor-in-possession.). See *Summit Inv. & Dev. Corp. v. Leroux (In re Leroux)*, 69 F.3d 608 (1st Cir.1995).
- ***In re Pioneer Ford Sales, Inc.***, 729 F.2d 27, 29 (1st Cir.1984) (Breyer, J.) ("[W]e see no conflict, for (c)(1)(A) refers to state laws that prohibit assignment 'whether or not' the contract is silent, while (f)(1) contains no such limitation. Apparently (f)(1) includes state laws that prohibit assignment only when the contract is *not* silent about assignment; that is to say, state laws that enforce contract provisions prohibiting assignment. These state laws are to be ignored. The section specifically excepts (c)(1)(A)'s state laws that forbid assignment even when the contract *is* silent; they are to be heeded.")
- ***Rieser v. Dayton Country Club Co. (In re Magness)***, 972 F.2d 689, 695 (6th Cir.1992) ("There is simply nothing in the language of § 365(f) which supports the limitation read into it by [the *Pioneer Ford*] court ... Neither *Pioneer Ford* nor any other decision to date provides a defensible explication of the parameters of the § 365(c) exception."). See also *Ford Motor Co. v. Claremont Acquisition Corp. (In re*

Claremont Acquisition Corp.), 186 B.R. 977, 980-984 (C.D.Cal.1995) (discussing the conflict and evaluating the two main positions).

- *PPG Industries, Inc. v. Guardian Industries Corp.*, 597 F.2d 1090, 1093 (6th Cir.), *cert. denied*, 444 U.S. 930, 100 S.Ct. 272, 62 L.Ed.2d 187 (1979) ("[q]uestions with respect to the assignability of a patent license are controlled by federal law".)
- *Unarco Industries, Inc. v. Kelley Co.*, 465 F.2d 1303, 1306 (7th Cir.1972) ("[T]he question of assignability of a patent license is a specific policy of federal patent law dealing with federal patent law. Therefore, we hold federal law applies to the question of the assignability of the patent license in question."), *cert. denied*, 410 U.S. 929, 93 S.Ct. 1365, 35 L.Ed.2d 590 (1973).

[6]. Effect of Rejecting a License in a Licensor Bankruptcy

- *Section 365(n)* gives the licensee of an "intellectual property right" the ability to either accept a licensor's rejection of the license, or to keep the licensed rights by continuing to pay any royalty payments required. The term "intellectual property" in Section 365(n) does not include trademarks.
- *In re Gucci*, 126 F.3d 380 (2d Cir. 1997) (court reserves judgment on the effect that a rejection of a trademark license would have on the "rights" created by that rejected license. "The effects of a rejection of a trademark licensing agreement are a matter that remains to be litigated. To date, this Court has not addressed whether a § 365 rejection operates as a kind of avoiding power to bring back into the estate a license of the debtor's trade name or trademark that was conferred by the debtor prior to its bankruptcy filing.")
- *In re Lavigne*, 114 F.3d 379, 387 (2d Cir.1997) ("rejection merely frees the estate from the obligation to perform; it does not make the contract disappear").
- Lieb, *The Interrelationship of Trademark Law and Bankruptcy Law*, 64 Am. Bankr.L.J. at 36-37 ("transfer of rights in a trademark should not be rescinded as a consequence of rejection, but, should be subject to continued enjoyment by the licensee").

[7]. Royalties to be Paid To Retain Rights

- *In re Prize Frize*, 150 B.R. 456 (9th Cir. BAP 1993), *aff'd*, 32 F.3d 426 (9th Cir.1994) (Prize Frize had granted a licensee an exclusive license to manufacture, use and sell its patented french fry vending machine. In exchange, the licensee agreed to pay certain license fees to Prize Frize. After Prize Frize filed for bankruptcy, it rejected the agreement. The court held that the license fees still owed by the licensee were "royalty payments" within the meaning of § 365(n), and that therefore § 365(n) required the licensee to pay those fees to the debtor in order to retain its rights under the agreement.)

XVI. Debtor's Use of Licensed IP After Filing Bankruptcy

- *In re DAK Industries, Inc.*, 66 F.3d 1091 (9th Cir. 1995) (Contract under which computer vendor (debtor) had entered prepetition allowing debtor to install software on computers that debtor sold, was in effect a sale of a right to make multiple copies of software in a particular format and, thus, payments due under the contract were not post-petition obligations, but a pre-petition debt; court had to look through form of transaction to the economic realities of the particular arrangement, to determine whether creditor was entitled to administrative expense for debtor's postpetition use of subject property. "The agreement here provided that upon signing, DAK was absolutely obligated to pay \$2,750,000, even if it sold only one copy of Word. The fact that some of the payments became due postpetition does not alter the fact that the entire debt was absolutely owed prepetition, and was therefore prepetition debt." "DAK did not employ Word over a period of time in order to run its operation. Rather, it sold the program to consumers. Accordingly, DAK's postpetition distribution of Word is more like the sale of inventory than the utilization of the claimant's trademark or device described in *B-K of Kansas* and *Neville Island*.")
- *In re B-K of Kansas, Inc.*, 82 B.R. 135 (Bankr.D.Kan.1988), *aff'd*, 99 B.R. 446 (D.Kan.1989) (court allowed an administrative expense claim for the debtor's postpetition display of the Burger King trademark in order to attract customers)
- *In re Neville Island Glass Co., Inc.*, 78 F.Supp. 508 (W.D.Penn.1948) (court allowed an administrative expense claim for the debtor's use in its glass manufacturing process of the claimant's patented equipment, which was installed in the debtor's plant pursuant to a lease-license agreement.)
- *Broadcast Corp. of Georgia v. Broadfoot*, 54 B.R. 606 (N.D.Ga.1985), *aff'd sub nom. In re Subscription Television of Greater Atlanta*, 789 F.2d 1530 (11th Cir.1986) (court allowed an administrative expense claim because the claimant had continued to provide video scrambling services to the debtor, a subscription television station, after it had filed for bankruptcy)
- *In re Prize Frize*, 150 B.R. 456 (9th Cir. BAP 1993), *aff'd*, 32 F.3d 426 (9th Cir.1994) (Prize Frize had granted a licensee an exclusive license to manufacture, use and sell its patented french fry vending machine. In exchange, the licensee agreed to pay certain license fees to Prize Frize. After Prize Frize filed for bankruptcy, it rejected the agreement. The court held that the license fees still owed by the licensee were "royalty payments" within the meaning of § 365(n), and that therefore § 365(n) required the licensee to pay those fees to the debtor in order to retain its rights under the agreement.)

XIX. Automatic Stay

As a general rule, a bankruptcy filing places an immediate, automatic stay against the

continuation or initiation of any action against the debtor, including actions alleging infringement of an intellectual property right. 11 USC § 362 (a).

- ***Seiko Epson Corp. v. Nu-Kote Int'l, Inc.***, 190 F.3d 1360 (Fed. Cir. 1999) (manufacturer's filing of bankruptcy petition resulted in automatic stay of patent infringement proceedings against the manufacturer but not against the manufacturer's affiliate, which had not filed bankruptcy)
- ***Checkers Drive-in Restaurants, Inc. v. Commissioner of Patents and Trademarks***, 51 F.3d 1078 (DC Cir. 1995) (Service mark holder seeking to cancel debtor's own similar mark was not barred, by automatic stay in place in debtor's Chapter 11 case, from filing affidavit required to maintain registration for its mark; filing of affidavit merely preserved status quo, and did not qualify as action or proceeding "against" the debtor barred by automatic stay. Competing service mark holder's filing of affidavit to maintain registration for its mark was not attempt to exercise control over Chapter 11 debtor's own similar mark, so as to be barred by automatic stay; both debtor and competitor had independent property right in their own service marks. 11 U.S.C. § 362(a)(3). "Moreover, while the application of the section 8 filing requirement may appear harsh in this case, Checkers failed to avail itself of a simple means of avoiding this result. Checkers neglected to take the prudential step of seeking clarification from the bankruptcy court, or even from the Commissioner, as to whether its section 8 filing obligation was stayed. Checkers had ample time to make such an inquiry; CRG filed its petition for bankruptcy approximately two months before the first day of the year-long "window" during which Checkers was required to file its section 8 affidavit. By failing to inquire, Checkers assumed the risk that the required filing was not stayed.")
- ***United States v. Inslaw, Inc.***, 932 F.2d 1467, 1473 (D.C.Cir.1991), *cert. denied*, 502 U.S. 1048, 112 S.Ct. 913, 116 L.Ed.2d 813 (1992) ("The object of the automatic stay provision is ... to make sure that creditors do not destroy the bankrupt estate in their scramble for relief." The automatic stay did not bar the Department of Justice from using computer software provided by, and claimed by, a debtor in bankruptcy. Court rejected debtor's argument that the Department's use of the software without the debtor's consent amounted to an "exercise of control" over property of the estate within the meaning of subsection 362(a)(3), commenting that such a construction of the statute "would take it well beyond Congress's purpose."). See also *In re Morton*, 866 F.2d 561, 564 (2d Cir.1989) (operation of state law requiring lien holder to renew lien in state court was not stayed by section 362 because "extension ... simply allows the holder of a valid lien to maintain the status quo--a policy not adverse to bankruptcy law, but rather in complete harmony with it").
- ***Time Warner Cable of New York city v. M.D. Electronics, Inc.***, 101 F.3d 278 (2d Cir. 1996) (Cable television corporation brought action against Chapter 11 debtor and its president for selling signal decoders in violation of Communications Act and New York law governing cable television rates. Held: corporation was required to seek discovery relief in bankruptcy court.)

XX. Infringement Actions

- *In re Cambridge Biotech Corp.*, 186 F.3d 1356 (Fed. Cir. 1999) Assignee of patents directed to structural components of and methods of detecting presence of two types of Human Immunodeficiency Virus (HIV) and its United States licensee brought infringement action in bankruptcy court against purported sublicensee, which claimed that it obtained sublicense from another licensee through a cross-license agreement. The court held that the claim could be brought in the bankruptcy court since it involved a so-called "core proceeding." It further held that the assignee, through its licensee, breached the "best efforts" clause of cross-license agreement.
- *In re Wilson*, 149 F.3d 249 (4th Cir. 1998) Bankruptcy court did not abuse its discretion when it ordered that sealed memorandum and judgment which it entered in prior action for misappropriation of trade secrets between debtor, debtor's company, and holder of trade secrets be disclosed to two employees of defendant in holder's state-court action, which alleged in part defendant's violation of injunctive relief granted in prior action; defendant was not party to prior action and therefore needed documents to understand core allegations leveled against it, and bankruptcy court's order reflected that it balanced harm from disclosure against defendant's need for employee access to documents.

THE STATE OF PRIVACY

*Cynthia L. Stewart
Frost Brown Todd LLC
Louisville, Kentucky*

Copyright 2002, Cynthia L. Stewart

SECTION F



THE STATE OF PRIVACY

*Cynthia L. Stewart
Frost Brown Todd LLC
Louisville, Kentucky*

Table of Contents

| | | |
|-------------|--|-------------|
| I. | Headlines..... | F-1 |
| II. | So What Parameters Exist for the Regulation of Privacy? Life After Geocities..... | F-2 |
| III. | FTC Enforcement | F-3 |
| | A. Geocities | F-3 |
| | B. Toysmart | F-3 |
| | C. Eli Lilly | F-4 |
| | D. Microsoft..... | F-4 |
| | E. Consistent Approach by FTC..... | F-5 |
| | F. Children's Online Privacy Protection Act | F-6 |
| IV. | Congressional and State Initiatives. | F-6 |
| V. | European Union Privacy Issues..... | F-8 |
| | A. Background | F-8 |
| | B. E.U. Data Transfer Options | F-8 |
| | C. Safe Harbor Requirements..... | F-8 |
| | D. How Are We Doing So Far? | F-9 |
| | E. Enforcement..... | F-10 |
| | F. The Beat Goes On..... | F-10 |
| VI. | Technology Solutions..... | F-10 |
| VII. | Conclusion.... | F-11 |

SECTION F

The State of Privacy Then & Now

While the steady collection of consumer data has been going on (practically unnoticed) in the United States since the beginning of commerce, the efficiency and automation of the Internet, together with the ease with which one can conduct business worldwide through the Internet, is pushing the privacy issue to the forefront.

I last spoke on privacy issues in March of 2000. In the last two and one-half years, there has been much gnashing of teeth and wringing of hands over the privacy issue on both sides of the Atlantic. Set forth below is an overview of significant events in the field of privacy that have occurred since March of 2000.

Headlines

As a good place to begin the "Then & Now" comparison of the state of privacy, I am going to pick up where I left off in March of 2000. At that time, the Washington based Electronic Privacy Information Center ("EPIC") had filed a request with the Federal Trade Commission to look into the data collection practices of DoubleClick, Inc.

In November of 1999, DoubleClick merged with Abacus Direct Corp., a marketing research company that allegedly maintains a data base of names, addresses and other marketing information for approximately 90% of American households, containing over ninety million personally identifiable individual purchaser profiles. *Stephen F. Ambrose, Jr. and Joseph W. Gelb, Consumer Privacy Regulation and Litigation, The Business Lawyer, Vol. 56, May 2001, citing Richard Raysman & Peter Brown, Protecting Consumer Privacy: Are you Prepared?, N.Y.L.J., Apr. 11, 2000, at 3.* EPIC claimed that, prior to the announcement of the merger, DoubleClick had represented that the information it collected, i.e., clickstream data from visitors to web sites that featured DoubleClick ads, would remain anonymous. Beginning in June of 1999, DoubleClick apparently revised its privacy policy to say that DoubleClick might combine personally identifiable data with clickstream data. *Privacy Group Seeks FTC Investigation of Net Marketer's Information Collection Practices, Electronic Commerce & Law, February 16, 2000, Vol. 5, No. 7, p. 157.*

In January of 2001, the FTC concluded its investigation of DoubleClick, dropping charges that DoubleClick had engaged in unfair and deceptive trade practices. This occurred **after** DoubleClick hastily retreated from its plans to combine the DoubleClick and Abacus databases. *FTC Ends DoubleClick Privacy Investigation, Jupitermedia Corporation, January 23, 2001, www.atnewyork.com/news/article.php/567441.* DoubleClick agreed to rewrite its privacy policy and modify certain of its privacy practices as a result of the FTC investigation, however, the public was not satisfied.

Since the initiation of the FTC investigation, DoubleClick has been the subject of federal and state class-action lawsuits alleging that DoubleClick violated the privacy of Internet users by using cookies and other data collection tools "to surreptitiously intercept,

monitor, and sell information about Web browsing habits and other personal data". *DoubleClick Settles Class Actions, Agrees to Change Privacy Practices, Electronic Commerce & Law, April 3, 2002, Vol 7, No. 14, p. 316.* The cases were settled this past summer with DoubleClick agreeing to pay legal fees and costs up to \$1.8 million and agreeing to take the following actions, among others: (1) DoubleClick will revise its privacy policy to include an easy to understand description of its services; (2) it can not combine personally identifiable information that it collects with previously collected click stream data without a clear and conspicuous notice to the internet user and receipt of the end user's opt-in documentation; (3) it will ensure that an internet user's information will only be used consistent with the privacy policy in effect when the information was collected; (4) the company must undertake a consumer education effort on the topic of online privacy; the company will establish internal policies to ensure the protection and routine purging of data collected on line; (5) the company will purge certain data it obtained during the course of testing the manner in which online and offline data could be merged; (6) the company has agreed to limit to five years the life of new ad servicing cookies; and (7) the company has agreed to have a nationally recognized accounting firm audit the company's compliance with certain terms of settlement. *DoubleClick Settles Class Action Suits, Agrees to Implement Privacy Protections, Electronic Commerce & Law Report, April 3, 2002, Vol. 7, No. 14., p. 316.*

On August 26, 2002, DoubleClick settled with the Attorneys General for ten states (Arizona, California, Connecticut, Mass., Michigan, New Mexico, New Jersey, New York, Vermont, and Washington) following 30 months of investigation by the Attorneys General into the data collection and use practices of DoubleClick. DoubleClick has agreed, among other agreements, to increase the visibility of its tracking activities, so consumers will have more notice that their activities are being monitored. Further, web sites that allow DoubleClick to profile their visitors must disclose DoubleClick's activities in the privacy policies of such web sites. In addition, DoubleClick will pay the states \$ 450,000 to cover investigation costs and for use in connection with consumer education. *DoubleClick Reaches Agreement with States on Visibility of Consumer Tracking Activities, Electronic Commerce & Law Report, Vol. 7, No. 35, September 11, 2002 (text of settlement available at www.oag.state.ny.us/press/2002/aug/aug26a_02_attach.pdf).*

"[T]o maintain its position as a leader in on-line privacy, DoubleClick has worked closely with the attorneys general to build upon the robust privacy practices it has already implemented, said Elizabeth Wang, DoubleClick general counsel." *Id.* Thus DoubleClick has apparently survived the onslaught and faithfully carries on.

So What Parameters Exist for The Regulation of Privacy? Life After Geocities

While there always seems to be one or more proposals for comprehensive privacy legislation pending in Congress, it does not appear that such legislation will be adopted in the current session. *ABA Panel Predicts Congress May Not Act Soon, But Privacy Legislation Inevitable, Electronic Commerce & Law Report, Vol. 7, No. 32, p. 809.* To date, Congress has taken a sectoral approach to privacy, adopting the Children's Online Privacy Protection

Act, the Gramm-Leach-Bliley Act (relating to financial institutions), and the Health Insurance Portability and Accountability Act (relating to medical information) and earlier adopting the Cable Communications Policy Act of 1984, the Fair Credit Reporting Act, the Federal Videotape Privacy Protection Act, among others. In 1998 and 1999, the FTC, with some disagreement among FTC commissioners, recommended to Congress that no comprehensive legislation relating to privacy be adopted and that given the opportunity, the private sector would appropriately self-regulate. *Speech of Commissioner Orson Swindle, Federal Trade Commission, Perspectives on Privacy Law and Enforcement Activity in the United States, June 2002* www.ftc.gov/speeches/swindle/perspectivesonprivacy.htm citing *Online privacy: A Report to Congress (June 1998)*, www.ftc.gov/reports/privacy3/index.htm; and *Federal Trade Commission, Self-Regulation and Privacy Online: A Federal Trade Commission Report to Congress (July 1999)*, www.ftc.gov/os/1999/9907/privacy99.pdf.

In 2000, the FTC changed its position and formally recommended that Congress adopt comprehensive legislation to address privacy issues, concluding that the private sector had made “insufficient progress toward developing genuine, pragmatic privacy protections for consumers”. *Id.* citing *Federal Trade Commission, Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress (May 2000)*, www.ftc.gov/reports/privacy2000/privacy2000.pdf. In the Fall of 2001, the FTC announced another shift in its focus indicating that it would in the future emphasize enforcement instead of the enactment of comprehensive privacy legislation. *Elaine M. Laflamme, Privacy is Becoming a Company Affair, New York Law Journal, June 10, 2002, Vol. 227, Pg. S6.*

FTC Enforcement

Even before the FTC’s shift in focus, it had taken the primary role in enforcement in the privacy arena in the United States. The FTC asserts jurisdiction over privacy through its enforcement power to regulate “deceptive acts and practices” under the Federal Trade Commission Act, 15 U.S.C. § 45.

Geocities. The first time the FTC flexed its muscles in the privacy area was with the well known Geocities case. www.ftc.gov/os/1999/9902/9823015d&o.htm. As of April of 1998, the Geocities web site was one of the 10 most frequently visited sites. It was a virtual neighborhood featuring web sites of interest to children, such as the “Enchanted Forest”. Geocities did not have a comprehensive privacy policy but did indicate that it would not share information collected with third parties. In fact, that information was being shared with third parties. The FTC took action and required Geocities to correctly inform users of how information was collected and used, and it further restricted Geocities’ collection and use of information gathered from children in a manner now essentially embodied in the Children’s On-line Privacy Protection Act of 1998. *Id.*

Toysmart.com. In 2000, the FTC took action against Toysmart.com as a result of an all too familiar dot.gone experience. While solvent, Toysmart.com collected information from customers with a privacy policy in effect that indicated that the company would not share the information with third parties. When the company went into decline,

Toysmart.com solicited bids for the sale of its assets, namely, customer lists that included information collected under the above referenced privacy policies. The creditors of the company forced it into bankruptcy and the customer information thus became an asset of the bankrupt estate. The FTC filed suit to prevent the sale of the customer information and to allege a violation by Toysmart.com of its privacy policy and of the Children's On-line Privacy Protection Act. The parties settled and as a result Toysmart.com's data could be sold only to a qualified buyer in the same market as Toysmart.com that would abide by the terms of Toysmart.com's privacy statement. A buyer who wanted to use the information differently had to get the consent of the customer. In addition, Toysmart.com was required to delete or destroy all information obtained in violation of COPPA. *Speech of Commissioner Orson Swindle, Federal Trade Commission, citing FTC v. Toysmart.com, LLC, and Toysmart.com, Inc., Civ. Action No. 00-11341-RGS (D. Mass 2000). Also see www.ftc.gov/opa/2000/07/toysmart2.htm.*

Eli Lilly. Eli Lilly, the large pharmaceutical company that manufactures and sell drugs including prozac, operated a web site at www.prozac.com that offered a reminder service to prozac users to help them remember to take or refill their prozac medication. In June of 2001, Eli Lilly decided to terminate the service, and one of its employees sent an email to all subscribers notifying them of the termination of service. Unfortunately, that notice included all 670 of the subscribers' email addresses within the "To" line of the message, thus disclosing to subscribers the email addresses of all other subscribers. The FTC claimed that Eli Lilly had failed to maintain or implement internal measures to protect the highly sensitive information of subscribers. In settlement, Eli Lilly agreed to strengthen internal standards relating to privacy protection, including employee training and monitoring of data. *Speech of Commissioner Orson Swindle, Federal Trade Commission, www.ftc.gov/speeches/swindle/perspectiveonprivacy.htm.*

In addition to its settlement with the FTC, on July 25, 2001, Eli Lilly settled with the Attorney Generals of eight states (Mass., NY, Cal., Conn., Idaho, Iowa, NJ, and Vermont) pursuant to which Eli Lilly has agreed to pay \$ 160,000 to the states and to strengthen internal standards relating to privacy protection, training and monitoring. The company must undergo an annual, independent compliance review for the next five years and report findings to the states. In response to the action taken by the states, Eli Lilly has put into place additional security measures to prevent such a disclosure from ever happening again, including implementing software that blocks emails with more one name on the email. Eli Lilly also appointed a director of Global Privacy, has in place a privacy policy team, and has in place security measures that "place personal information from customers in an environment as secure as Lilly's trade secrets". *Eli Lilly Reaches Agreements with States Over Accidental Release of Customer Data, Electronic Commerce & Law Report, Vol 7, No. 30, July 31, 2002.*

Microsoft. Most recently, the FTC has settled with Microsoft in regard to its Passport products, namely, Passport Single Sign-In (known as "Passport"); Passport Express Purchase (known as "Passport Wallet"); and Kids Passport. The "Passport" products collected and stored information from users that allowed them to sign in at any participating web site with a single name and password. Passport Wallet collected and stored user credit

card information and allowed users to apply the stored information when making purchases at participating web sites. Finally, Kids Passport allowed parents to create Passport accounts for their children that would block the collection of personal information by participating web sites. *Microsoft Settles FTC Charges Alleging False Security and Privacy Promises, The Computer & Internet Lawyer, Vol. 19, No. 10, October 2002.*

In July of 2001, the Electronic Privacy Information Center filed a complaint with the FTC regarding Microsoft's Passport products and as a result, the FTC launched an investigation. The FTC complaint alleged that Microsoft had misrepresented that purchase transactions made using Passport Wallet were generally safer than purchase transactions made without Passport Wallet, when in fact the same security measures were employed whether or not Passport Wallet was used in the transaction. The FTC further alleged that Microsoft misrepresented its practice in collecting personally identifiable information. Contrary to its privacy policy, Microsoft did collect and hold for a limited time certain personally identifiable information. Finally, with respect to Kids Passport, the FTC alleged that Microsoft misrepresented the control a parent would have over what information their children could provide to participating web sites when children were able to edit or change certain fields of information and change account settings previously established by a parent. *Commissioner Orson Swindle, United States Federal Trade Commission, Perspectives on Privacy Law and Enforcement Activity in the United States, www.ftc.gov/speeches/swindle/perspectivesonprivacy.htm.*

The settlement requires that Microsoft refrain from making any misrepresentations about its information practices and the qualities of its products and services. In addition, Microsoft must implement and maintain a comprehensive security program in relation to personal information collected by Microsoft, and the program must be certified by an independent professional every two years. *Id.*

Consistent Approach by FTC. There appears to be a common thread to the recent FTC settlements, to the FTC's final rule under Gramm-Leach-Bliley and to the Organization for Economic Cooperation and Development's new guidelines for security of information systems and networks. The U.S. delegation to the OECD was headed by U.S. FTC Commissioner Swindle. *Barbara Yuill, Attorneys Create Compliance Roadmap From Terms of Eli Lilly, Microsoft Settlements, Electronic Commerce & Law Report, Vol 7, No. 33, p. 838, August 21, 2002.*

Legal commentators conclude that the FTC takes the position that companies that collect consumer data **must** (1) have a written, comprehensive information security program, (2) designate qualified personnel to coordinate and oversee data protection and information security, (3) identify reasonably foreseeable risks and take action to protect against them, (4) conduct periodic audits (that may be done by independent third parties), and (5) make adjustments to the program if appropriate in light of the results of the audit. *Id. at 839.*

This may answer some questions for companies looking for guidance on privacy and data collection, but it leaves many questions unanswered, one of the most significant of which is what rules govern information collection outside of the online environment and

what governs information that has been collected by long standing US entities for decades past.

Children's Online Privacy Protection Act. The Children's Online Privacy Protection Act, effective as of April 21, 2000, regulates online services that collect information from children under 13. *15 U.S.C. § 6501-6505*. As noted earlier, this statute came into effect in part due to the alleged transfer to third parties of information collected from children by Geocities. This is a fairly rigorous statute that uses a parental opt in approach to regulate the use of information provided by children to online services. As of April 22, 2002, there had been only six enforcement cases under COPPA, the most recent one involving the Etch-A-Sketch Web site, which resulted in Etch-A-Sketch agreeing to pay a fine of \$ 35,000. The FTC alleged that Etch-A-Sketch collected personal information from children registering with "Etchy's Birthday Club" for a chance to win an Etch-A-Sketch on the child's birthday. This information was collected without prior parental consent and with Etch-A-Sketch merely directing the child to "get your parent or guardian's permission first". *Etch-A-Sketch Draws \$ 35,000 Penalty for Violating the Children's Online Privacy Protection Act, KeyTLaw, www.keytlaw.com, April 22, 2002.* Also, see www.ftc.gov/os/04/ohioartcomplaint.htm.

In February of 2002, the American PopCorn Company, maker of "Jolly Time" popcorn agreed to settle with the FTC by paying \$ 10,000. The FTC alleged that the company maintained the web site www.jollytime.com, through which it collected information from children without parental consent. *Popcorn Company Settles FTC Privacy Violation Charges, KeyTLaw Business, Internet, e-Commerce & Domain Name Law, February 14, 2002, www.keytlaw.com.*

In an action against the web site girlslife.com, the respondent claimed on its web site privacy statement that it did not structure its site to attract anyone under the age of 13. In addition to being required to comply with COPPA, the respondent agreed to pay penalties of approximately \$ 30,000. *John F. Noble, Children's Online Privacy Protection Act Marks Its First Anniversary, Internet Law & Business, Vol., 2, No. 10, p. 865.* The only regulatory changes relating to the statute is the FTC extended to April 21, 2005 the time in which online services can rely on an email from a parent coupled with other verification methods for the collection and internal use of personal information about children. *FTC Extends Time for E-Mailed Consent From Parents for Information Collection, Electronic Commerce & Law Report, Vol. 7, No. 17, p. 381, April 24, 2002.*

Congressional and State Initiatives

Although two bills have been advanced in Congress that address privacy comprehensively, it does not seem likely either of those bills will become law prior to the end of 2002. *Anandashankar Mazumdar, ABA Panel Predicts Congress May Not Act Soon, But Privacy Legislation Inevitable, Electronic Commerce & Law Report, Vol. 7, No. 32, pg. 809, August 14, 2002.* One of the competing bills is The Online Personal Privacy Act (S. 2201) sponsored by Senator Ernest F. Hollings (D.-S.C.). This bill provides for an opt out approach, mandatory notice online of privacy practices, a private right of action for

violations, a limited right of access to information, and opt-in protection for sensitive information. It also provides for the federal preemption of all state and local privacy laws. *Michael E. Aruda, Ross A. Dreyer, and Margaret R. Prinzing, Can Congress Opt Out of Privacy Legislation in an Election Year?, Electronic Commerce & Law Report, Vol. 7, No. 28, p. 728, July 17, 2002.*

The other bill that gained support throughout the year but that probably will not make it past the finish line is the one sponsored by Rep. Clifford B. Stearns (R-Fla.) and known as the Consumer Privacy Protection Act of 2002 (H.R. 4678). The Stearns legislation would also preempt state law but would take a less stringent approach from the business perspective. Businesses must provide notice only the first time they collect personally identifiable information if such information may be used for purposes unrelated to the transaction in question. The notice must be prominently displayed and the consumer must be able to easily access the privacy policy of the company, which must be "plainly written". A significant difference in the Stearns proposal is that it applies to all personally identifiable information whether collected online or offline. *Id.*

Although as a general rule businesses are adverse to general legislation governing privacy, many in the business world are beginning to advocate a consistent nationwide policy. Many states are enacting legislation that is more restrictive than current or proposed federal legislation. In 2001, Vermont adopted legislation requiring that consumers "opt-in" with respect to the use of personal financial and medical information. New Mexico requires that financial institutions obtain customer permission before they share information with third party marketers. *Richard Cowden, Privacy Issues May Advance to Top of Policy Agendas in 2003, Experts Say, Electronic Commerce & Law Report, Vol. 7, No. 25, p. 612, June 19, 2002.*

In June of this year, North Dakota residents voted overwhelmingly in favor (72.2%) of reinstating legislation that required that financial institutions obtain written approval prior to the disclosure of customer information. *Mark Wolski, North Dakota Voters Tounce Bid to Let Banks Use Opt-Out on Financial Privacy, Electronic Commerce & Law Report, Vol. 7, No. 25, p. 612, June 19, 2002.* California's legislators are also considering financial privacy legislation that is much more stringent than the Gramm-Leach-Bliley Act. If legislation of this type passes, "California could set a de facto national standard". *Treasury Receives Some 50 Comments on Early Effect of Consumer Privacy Notices, Electronic Commerce & Law Report, Vol. 7, No. 21, p. 486, May 22, 2002.*

As a part of a study of information sharing practices among financial institutions, the FTC, the Treasury Department and other federal agencies requested public comment on the adequacy of existing law to protect consumer privacy. Thirty-five state Attorneys General responded indicating that they "believe that the current practices allowed under GLB are insufficient to protect consumers and pose considerable risk to them." *Id. at 487.* In 2001, 5 % or fewer consumers elected to opt-out of having information shared by their bank. *Id.* The Attorneys General indicated that the notices sent by financial institutions "have been dense and require a high reading level to comprehend, resulting in consumer confusion and inability to exercise informed choice." *Id.*

European Union Privacy Issues

Background. In October of 1998, the European Union Privacy Directive became effective. The Directive prevented E.U. businesses from transferring any personal information to businesses in other countries if such countries did not provide adequate privacy protection. The United States is one country that has been deemed to not provide adequate privacy protection. Since the adoption of the Directive, representatives of the European Commission and the U.S. Department of Commerce have been negotiating to establish a safe harbor to facilitate a process by which U.S. companies can comply with the Directive. In May of 2000, after the submission of seven proposals by the U.S. delegation, the parties finally achieved an agreement known as the Safe Harbor Principles. Participation in the safe harbor creates a presumption that the business provides an adequate level of privacy protection, which enables the business to receive data from E.U. entities. *Anna E. Shimanek, Do you want Milk with Those Cookies?: Complying with the Safe Harbor Privacy Principles, 26 Iowa J. Corp. L. 455, Winter 2001.*

E.U. Data Transfer Options. In addition to complying with the safe harbor, there are two other ways that U.S. companies can comply with the Directive. The first is to obtain express consent from the individuals with respect to whom the data relates. Consent is defined as “any freely given specific and informed indication” of the individual’s agreement to the use of the information for the described purpose. *Parliament and Council Directive 95/46/EC of October 24, 1995 on the Protection of Individuals with Regard to the Processing of Personal Data on the Free Movement of Such Data, 1995 O.J. (L 281), article 2(h).* This approach may be appropriate in many circumstances but will likely not work in an employer/employees situation since many European countries would not honor an employee’s consent in this context. *Christopher Terry, Clock Running on Time to Comply with the EU Privacy Directive, Chicago Lawyer, February 2002.*

A third approach is for businesses to enter into a version of the EU model contract with the transferring party. Most U.S. companies have rejected this approach because it imposes joint and several liability on all parties, is highly regulated by EU data protection agencies and allows third parties, such as the individuals about whom the data relates, a private right of action. *Id.*

Safe Harbor Requirements. To receive the benefits of the safe harbor, businesses must comply with the Safe Harbor Principles set forth in the Directive and “publicly declare that they do so.” *Do you want Milk With Those Cookies at 473 citing Issuance of Safe Harbor Privacy Principles and Transmission to European Commission, 65 Fed. Reg. 45,666 (July 24, 2000).*

For a business to satisfy the public declaration requirement, the business must certify on an annual basis to the Department of Commerce that the business adheres to the Safe Harbor Principles. To comply with the Safe Harbor Principles, the privacy program of a business must (1) provide clear notice with respect to the purpose for the data collection and use of the data, (2) provide an option to opt out of allowing use of the information; provided,

that with respect to certain sensitive data, the individual must opt in; (3) provide access by an individual to his or her data, (4) implement reasonable security measures; (5) take steps to ensure and protect the integrity of the data, making sure it is reliable, accurate, complete and current and that the data is being used for its stated purpose; and (6) implement effective enforcement mechanisms. *Barbara Crutchfield George, Patricia Lynch, Susan J. Marsnik, U.S. Multinational Employers: Navigating Through The Safe Harbor Principles To Comply with the EU Data Privacy Directive, American Business Law Journal, Summer 2001, Vol. 38, Issue 4, p. 735 citing the Safe Harbor Privacy Principles and Transmission to European Commission at 45,666 – 45, 677.*

In addition, the business must certify that it has joined a private sector privacy program such as TRUSTe or BBB Online, that it has developed and pronounced its own privacy policies in conformity with the Safe Harbor Principles or that the business is already subject to a sector-specific statute, regulation or legal requirement. To effect the self-certification, the business must send a letter signed by a corporate officer to the Department of Commerce stating that it is joining the safe harbor. The letter must include a description of the privacy policy, information about how the business uses the EU data, information about who handles complaints and requests for access to information, among other information. *Id.*

How are We Doing So Far? As of October 17, 2002, the Department of Commerce web site reflected 254 self-certified companies. www.export.gov/safeharbor. On February 13, the EU Commission issued a report on the operation of the U.S. safe harbor program and indicated that fewer than one-half of the businesses in the Safe Harbor at the time of evaluation posted a privacy policy that complied with all of the Safe Harbor Principles. In particular, the ability of an individual to access his or her data was not addressed in most policies. Many of the policies failed to clearly explain how a party could make use of the dispute resolution mechanism. The Commission further reported that 27 complaints had been received against Safe Harbor participants and that all had been resolved without any formal enforcement action. *Marc Roth, EU Takes New Look at Safe Harbor Program, e-Commerce Law & Strategy, Vol. 18, No. 11, p. 1, March 2002, citing the European Commission Feb. 13, 2002 report at http://europa.eu.int/comm/internal_market/en/dataprot/news/02-196_en.pdf.*

In Nov. of 2001, Arthur Anderson conducted a study that indicated that none of the 75 Fortune 500 companies that were participating in the safe harbor at the time complied with all safe harbor requirements. Two of 75 had five of the eight requirements of the safe harbor and several of the companies only had one safe harbor requirement. *U.S. Firms Slow to Adopt Global Privacy Practices, Direct Marketing, Nov. 2001, Vol. 64, Issue 7, p. 12.*

While the studies above may or may not be accurate, it is obvious that American organizations struggle in creating privacy policies, monitoring their compliance and implementing effective security. In July of 2001, the Department of Commerce discovered that its safe harbor site inadvertently exposed information about U.S. companies that was confidential. The site revealed sales figures, employee head counts and other details about the company's European operations. In addition, visitors to the site could modify a

company's information without any authorization from the company. *Ted Kemp, Privacy Rules Cross the Pond, InternetWeek, July 16, 2001, Issue 869, p.1.*

Enforcement. The EU agreed not to take enforcement action against US companies until after January of this year and as of the date of its report in February, the FTC had taken no enforcement action in regard to U.S. Safe Harbor companies. The EU took action in the European Court of Justice in January of 2001 against Luxembourg, France and Ireland for not adopting the Directive as law. Those matters were still pending as of January of 2002. Also, the country of Spain fined MicroSoft approximately \$ 57,000 in early 2001 for an alleged violation of the Directive. *Christopher Terry, Clock Running on Time to Comply with EU Privacy Directive, Chicago Lawyer, February 2002.*

The Beat Goes On. Financial institutions were not included under the Safe Harbor agreement between the U.S. and E.U. because the Gramm-Leach-Bliley Act was in the process of being adopted by Congress. The U.S. banking industry's position is that the Gramm-Leach-Bliley Act provides adequate protections to information, however, many who are watching the progress of this negotiation believe the European Commission will not agree. In the meanwhile, the Commission has begun approving contract provisions, which if inserted in a contract between the U.S. and E.U. party would satisfy the Directive. Another approach by financial institutions is to adopt a sector-by-sector model contract being proposed by industry associations in the United Kingdom and Germany. One of the U.S. banking industries most significant concerns regarding the Directive is the ability to use data without consent to prevent fraud. *Anandashankar Mazumdar, As U.S., EU Reengage on Financial Privacy, Industry Argues Current Law is Good Enough, Electronic Commerce & Law Report, Vol. 7, No. 15, p. 324, April 10, 2002.* Other concerns by the financial industry center on whether U.S. bank regulators would regulate financial institutions with respect to privacy issues or some other regulator and the relationship between American and European banking regulators with regard to privacy enforcement. *Id.*

Technology Solutions

While it seems that a significant portion of the population is focusing on legislative approaches to privacy issues which have yet to come to fruition, the more technology oriented population has been working on possible technological solutions. The World Wide Web Consortium was formed in 1994 to develop and promote common protocols to ensure the ongoing evolution and interoperability of the Internet. www.w3.org. The World Wide Web Consortium has developed an industry standard called the Platform for Privacy Preferences Project ("P3P"), which is an automated way for a user to access and obtain information about a web site's privacy policy. www.w3.org/p3p/. P3P also enables a user to take certain actions with respect to a web site, such as the ability to block the installation of cookies. For the system to work, a web site must make its privacy policy P3P enabled. Close to 500 web sites are using the protocol, including IBM's and Microsoft's web sites. www.w3.org/P3P/compliance_sites.

Conclusion

Much has occurred in the privacy arena over the last two and one-half years. Slowly but surely privacy issues are getting more attention and legislators are responding accordingly. While for the last few years businesses have successfully fended off broad privacy legislation, the regulation of privacy will undoubtedly come. Going forward, businesses must accept the reality that the gathering and protection of private information must be seriously addressed and tended to, and that such a task will now and in the foreseeable future be a regular part of doing business.

LOUIMDMS/195061.1



**LAW, ETHICS AND PUBLIC OPINION REGARDING
COMMERCIALIZATION OF BIOTECHNOLOGY:**

Pharmacogenomics as an Example

*Mark A. Rothstein
Herbert H. Boehl Professor of Law and Medicine
Director, Institute for Bioethics, Health Policy & Law
University of Louisville School of Medicine
Louisville, Kentucky*

Copyright 2002, Mark A. Rothstein

SECTION G



LAW, ETHICS AND PUBLIC OPINION REGARDING COMMERCIALIZATION OF BIOTECHNOLOGY:

Pharmacogenomics as an Example

*Mark A. Rothstein
Herbert H. Boehl Professor of Law and Medicine
Director, Institute for Bioethics, Health Policy & Law
University of Louisville School of Medicine
Louisville, Kentucky*

Table of Contents

| | | |
|------|--|------|
| I. | Introduction..... | G-1 |
| II. | Support of Research Provided By..... | G-2 |
| III. | Background..... | G-3 |
| IV. | Summary of Methodology..... | G-6 |
| V. | Areas of Inquiry..... | G-10 |
| | A. Willingness to Participate in Genetic Research..... | G-11 |
| | B. Perceptions of the Affordability of Pharmacogenomic-based Medications..... | G-19 |
| | C. Concerns About the Confidentiality of Genetic Information..... | G-24 |
| VI. | Conclusions..... | G-32 |
| VII. | Ethical and Legal Implications of Pharmacogenomics..... | G-33 |

SECTION G

Pharmacogenomics: Ethics, Policy and Public Views

Mark A. Rothstein, J.D.

1

Herbert F. Boehl Chair of Law and Medicine

Director

Institute for Bioethics, Health Policy and Law

University of Louisville School of Medicine

Pharmacogenomics: Ethics, Policy and Public Views

This research was supported by a grant from the National Institutes of Health (NIGMS, NHGRI, and NIEHS).

Mark A. Rothstein, J.D., Principal Investigator

Gabriela Alcalde, M.P.H., Program Director

Phyllis Griffin Epps, J.D., Program Director

Carlton A. Hornung, Ph.D., M.P.H., Consultant

Rosie Zamora, M.S., Principal Survey Contractor

Sharon P. Cooper, Ph.D., Survey Consultant

Dick Jaffee, Ph.D., Survey Consultant

Eun-Sul Lee, Ph.D., Survey Consultant

Barry Petree, Ph.D., Survey Consultant

Background

1. Each year in the U.S., about 100,000 people die from adverse drug events, making it between the 4th and 6th leading cause of death.
2. The most commonly prescribed medications have a median efficacy of 50 to 60%, ranging from 25% for oncology drugs to 80% for analgesics.

Background

3. Pharmacogenomics, by matching medications to genotypes, promises to improve safety and efficacy, as well as lowering research costs (through genotype-matched clinical trials) and development time.

Background

4. Does the public support research and prescribing of pharmacogenomic-based drugs?

Is the public concerned about access to medication, confidentiality, or discrimination?

What do public views on pharmacogenomics indicate about more general views about genetics and biomedical research?

Summary of Methodology

- Overall sample size of 1,796
- Over-sampling was used to achieve minimum subgroup sample size of 300 for whites, African Americans, Hispanics, and Asians
- Hispanics and Asians are heterogeneous groups, but sample size limited further refinements
- Maximum margin of error of +/-2.3%

Summary of Methodology

- Telephone interviews were conducted in English, Spanish, Chinese, Vietnamese, and Korean, and the survey instrument was translated and back- translated by separate translators
- Up to 5 contact attempts were made for each number at differential times
- Response rate for residential calls with answers was 84.6%

Summary of Methodology

- There were 12 substantive questions (some in several parts) that asked about genetic testing, genetic research, access to genetic information, and prescription medications

Summary of Methodology

- The demographic variables are as follows:
health status, prescription or over-the-counter medicine usage, health of family members, size of household, age, education, regular use of computer, marital status, employment status, work in health care, city or rural, race/ethnicity, language spoken at home, country of birth, health insurance coverage, religion, income, and gender
- All interviews were conducted in the spring and summer of 2001 (before 9/11/01)

Three Areas of Inquiry

1. Willingness to participate in genetic research.
2. Perceptions of the affordability of pharmacogenomic-based medications.
3. Concerns about the confidentiality of genetic information.

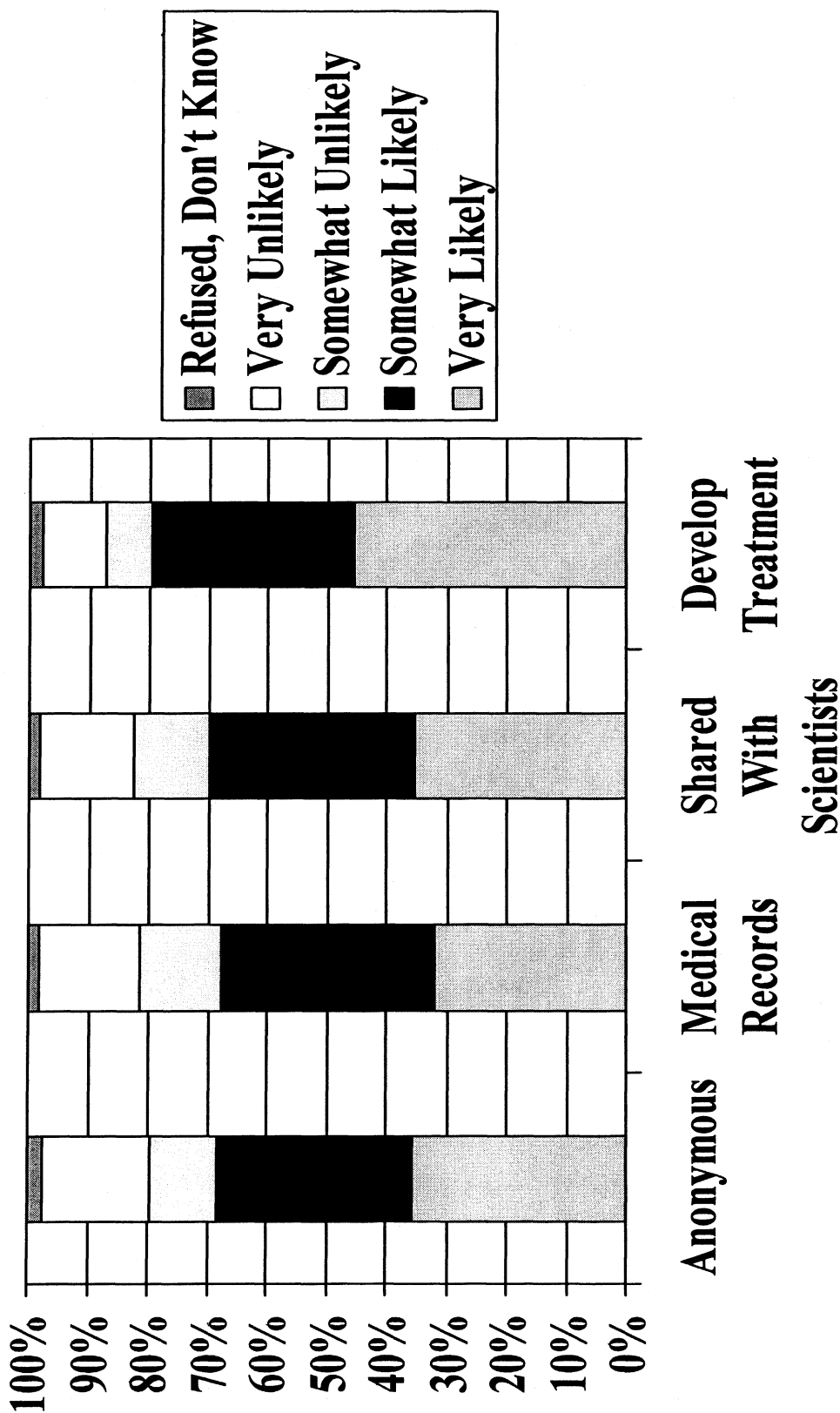
1. Willingness to participate in genetic research.

Question 4

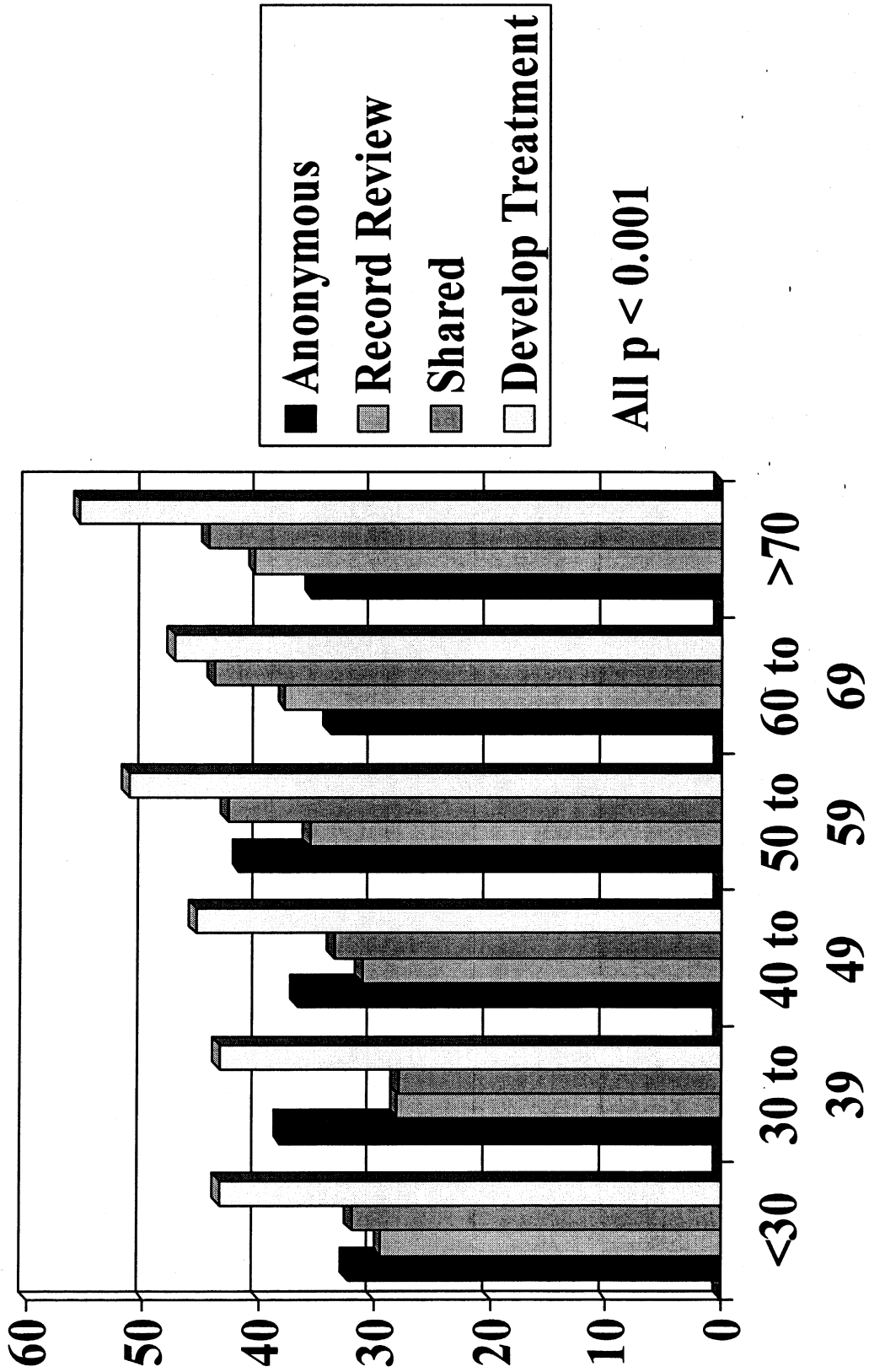
How likely would you be to participate in genetic research under each of the following conditions?

- A. Anonymous
- B. Linked with medical records
- C. Shared with other scientists nationwide
- D. Possibility existed to develop a treatment

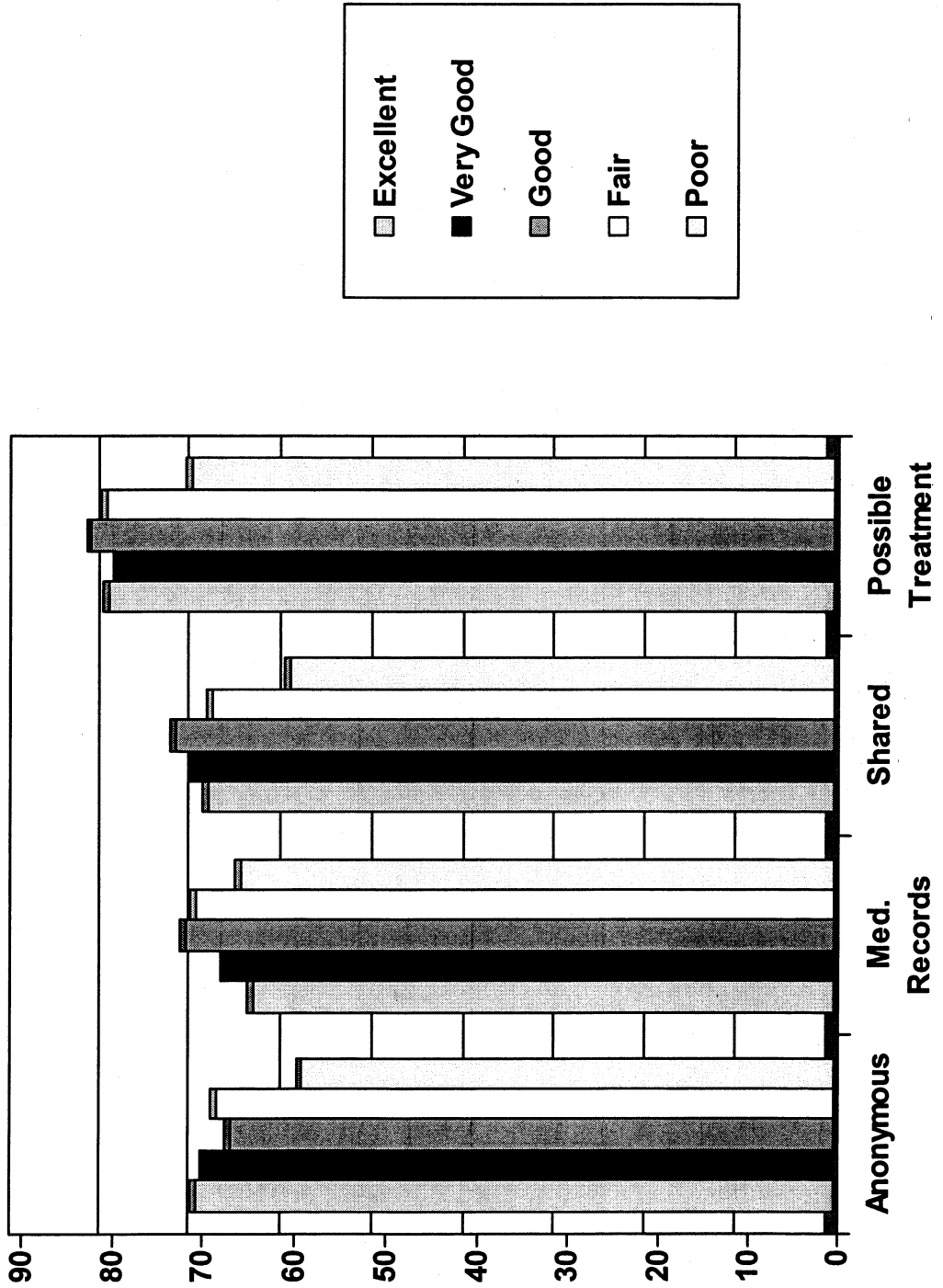
Likelihood of Participating in Research and Confidentiality



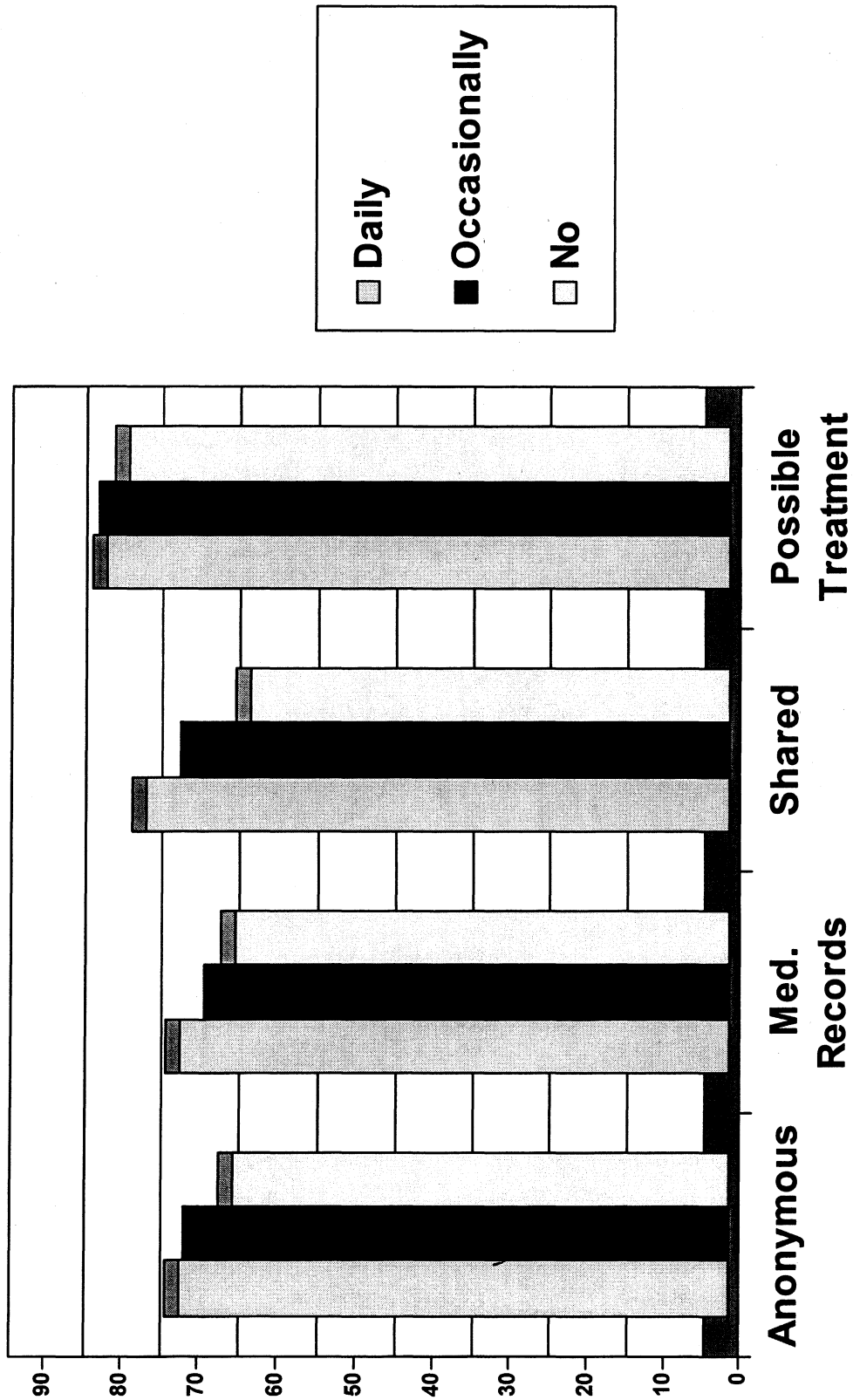
Age, % Very Likely to Participate in Genetics Research and Confidentiality



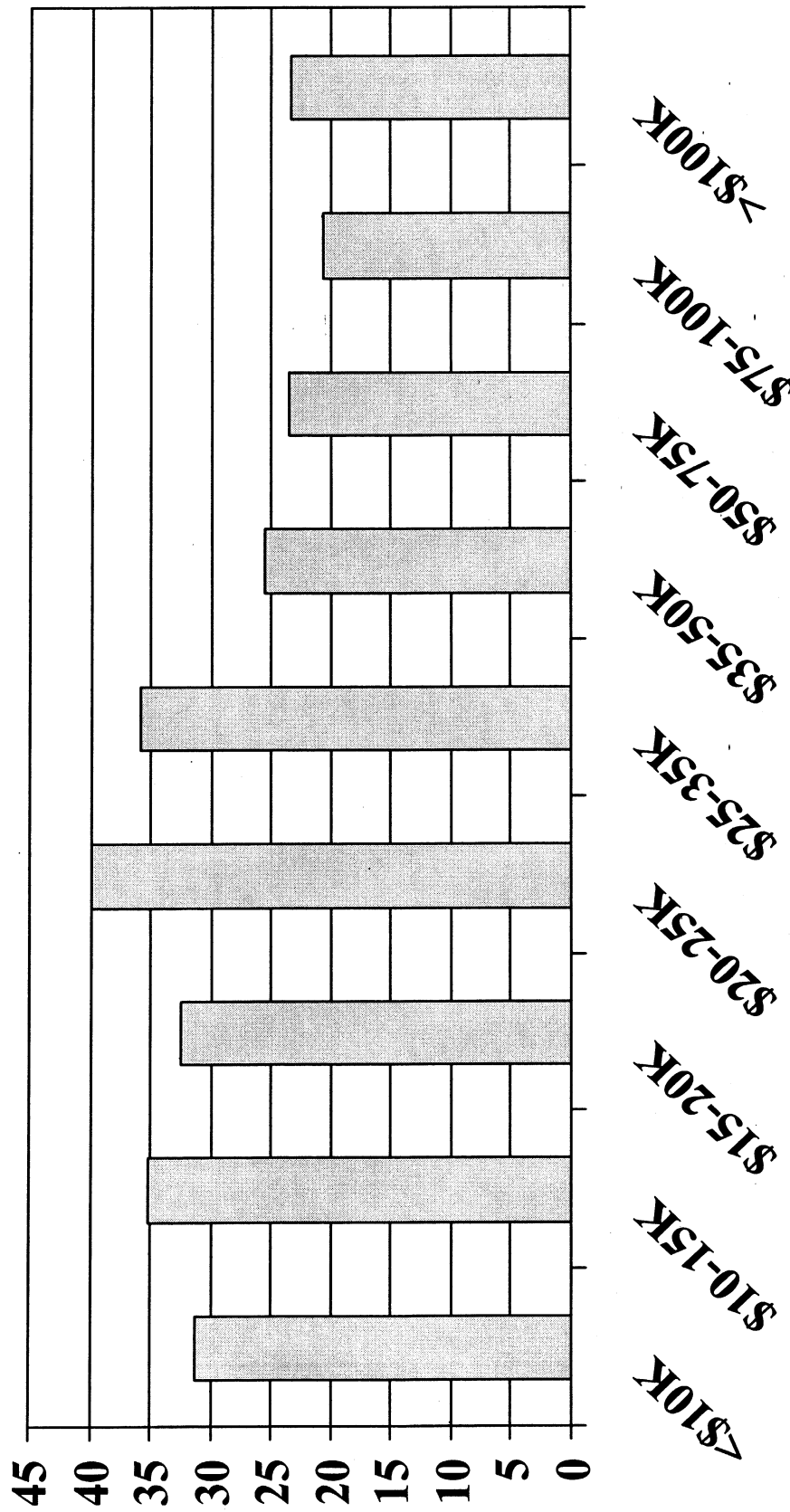
Willingness to Participate by Self Reported Health Status



Willingness to Participate According to Use of Prescription and/or OTC Drugs



Percent More Likely to Participate in Genetic Research if Paid \$50



Other findings related to willingness to participate in genetic research.

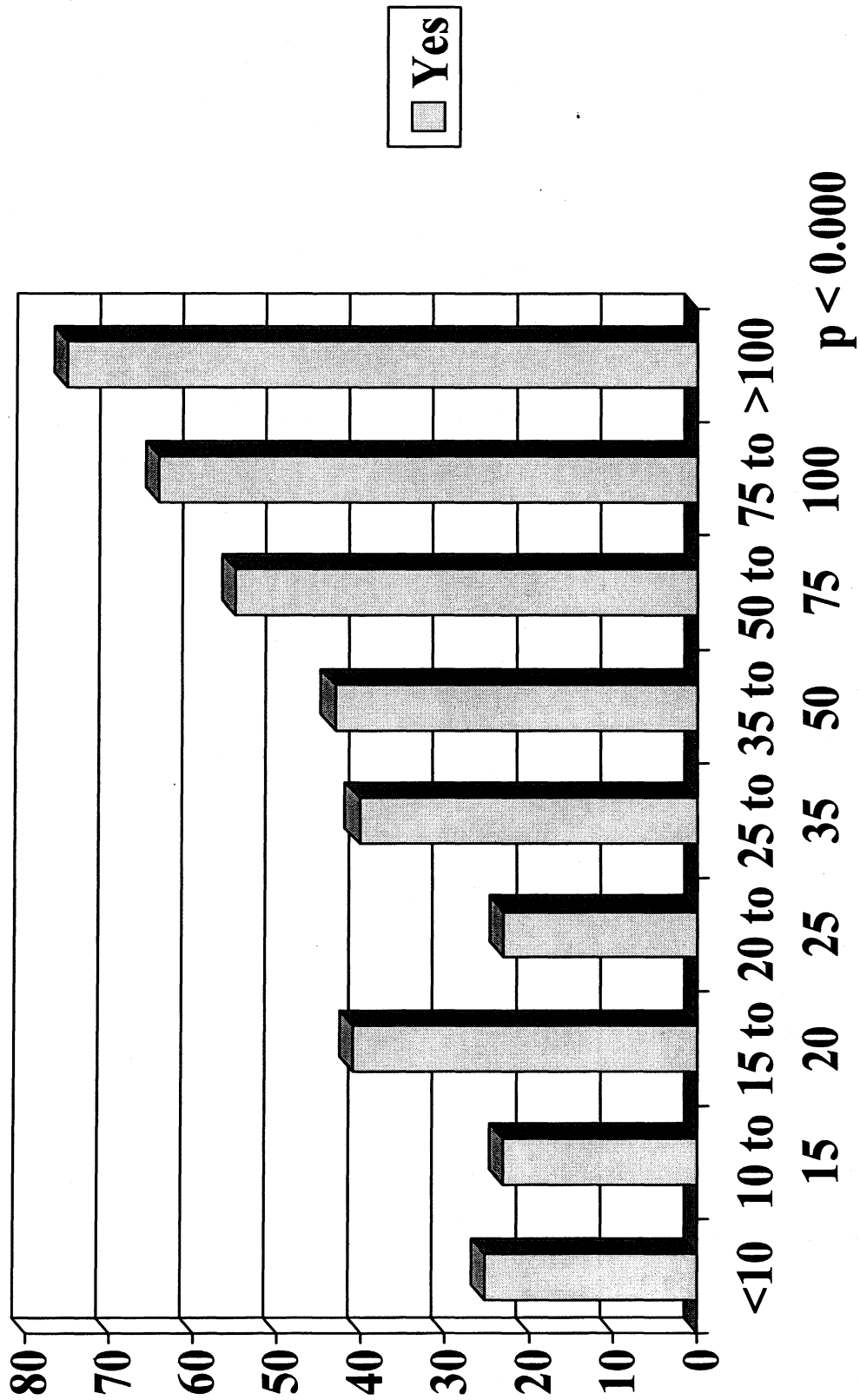
- Whites and Asians are about 8-10 percentage points higher than African Americans and Hispanics in willingness to participate.
- Higher education is associated with a greater willingness to participate.

2. Perceptions of the Affordability of Pharmacogenomic- based Medications.

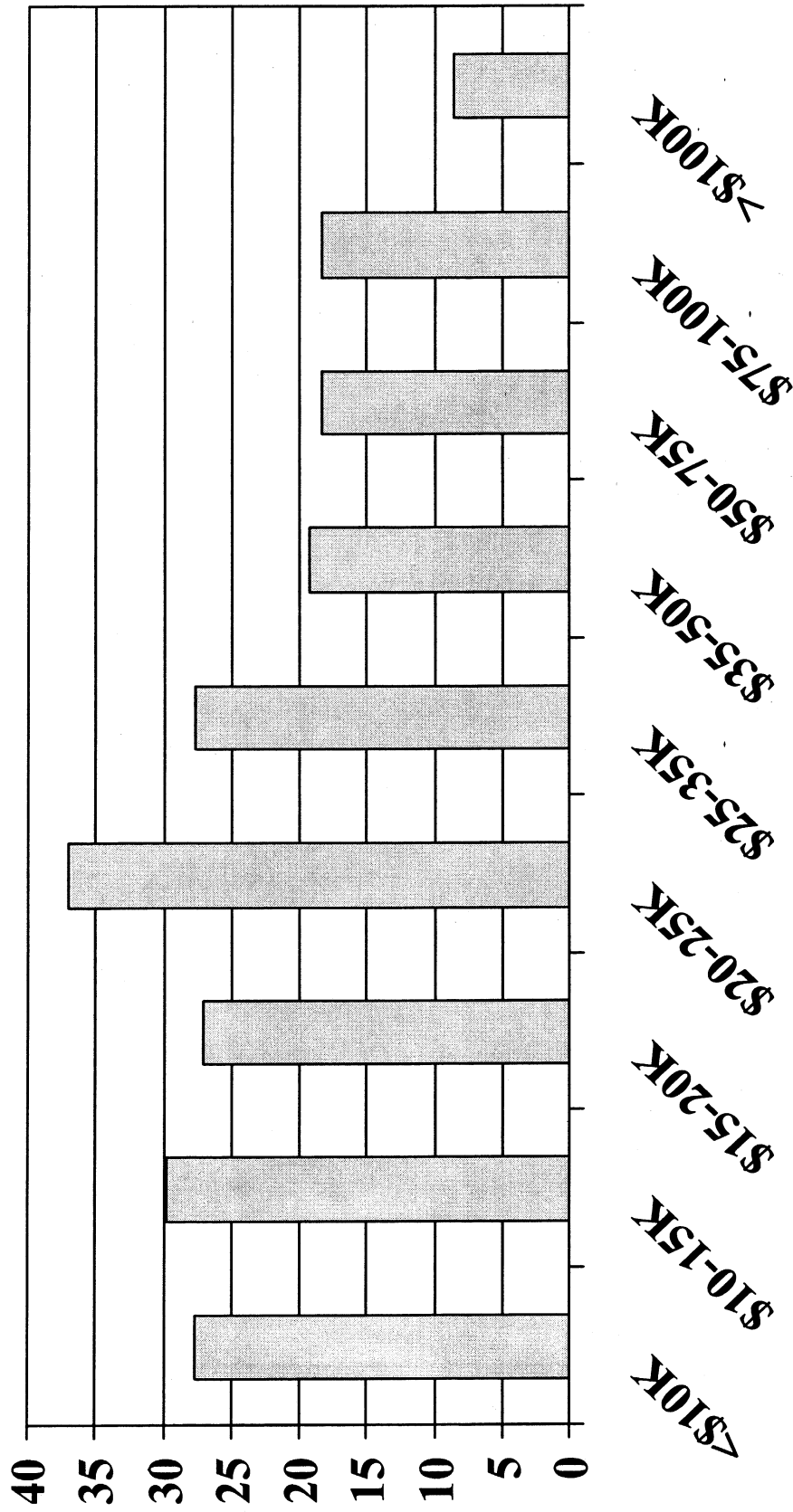
Question 9

If medicines were developed that were matched to the genetic makeup of individuals, do you think that people of your income level could afford them?

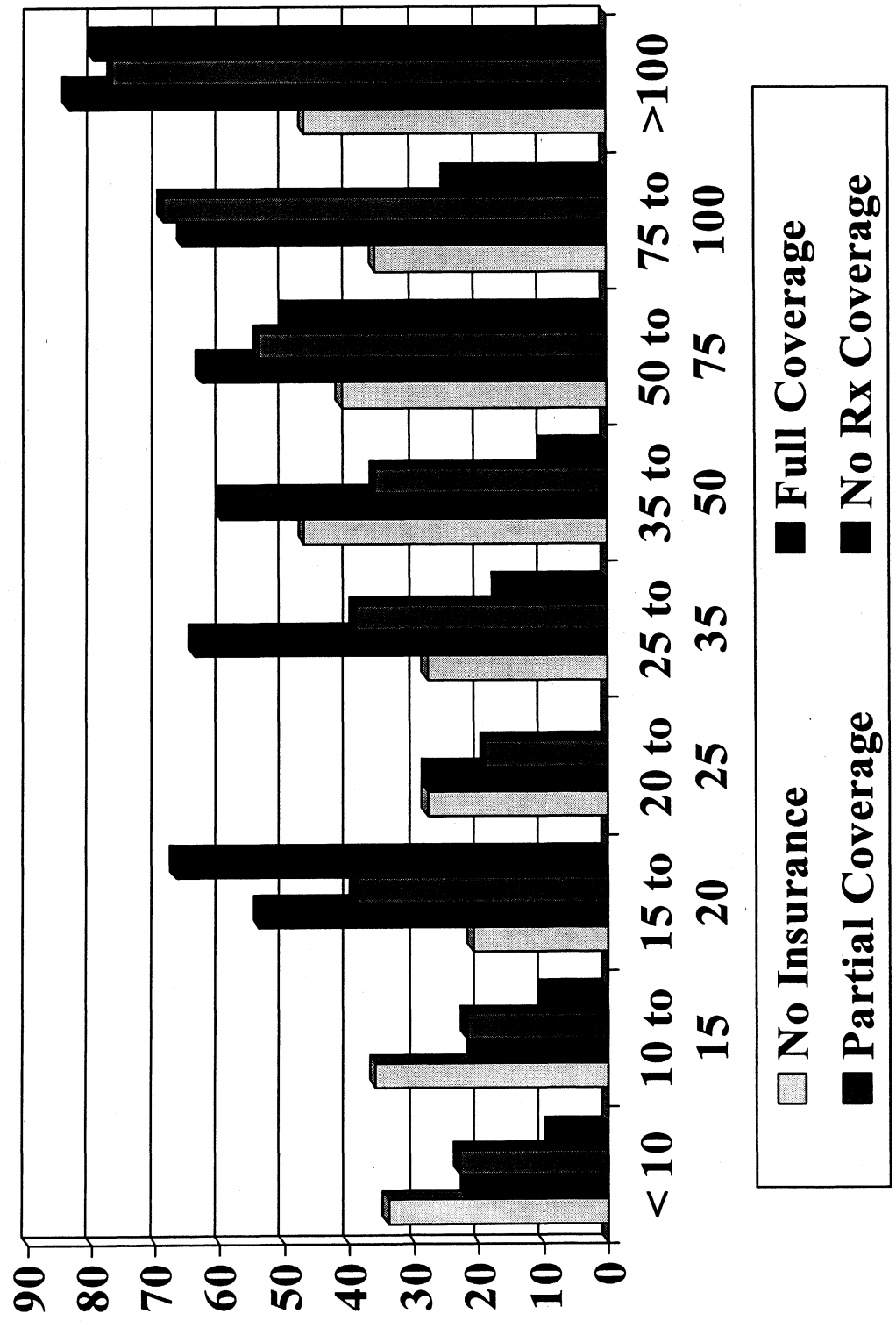
Income and % Believing They Could Afford Genetically Matched Drugs



Percent Not Filling a Prescription Because of Cost



Insurance and % Believing They Could Afford Genetically Matched Rx Drugs



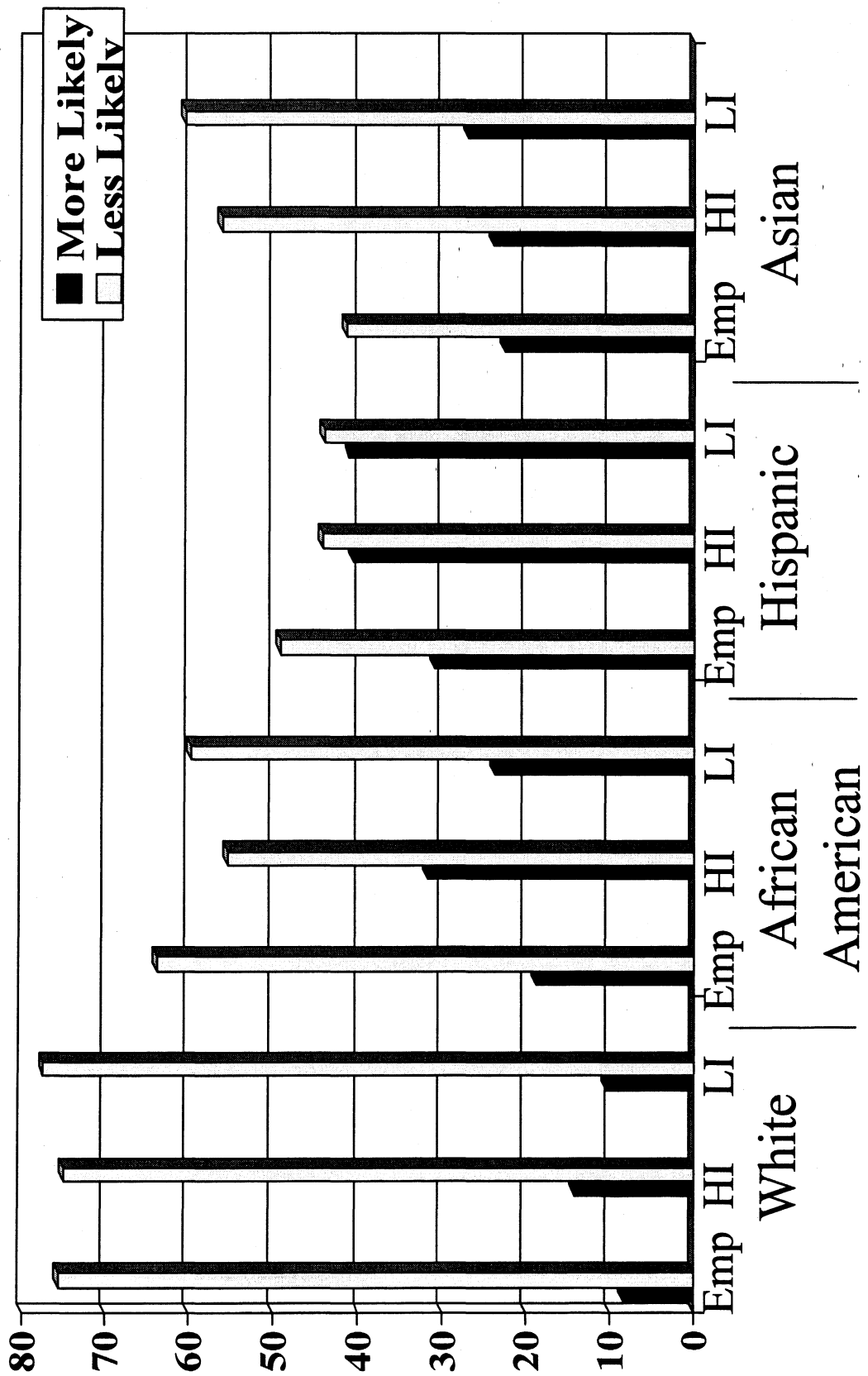
3. Concerns About the Confidentiality of Genetic Information.

Question 10

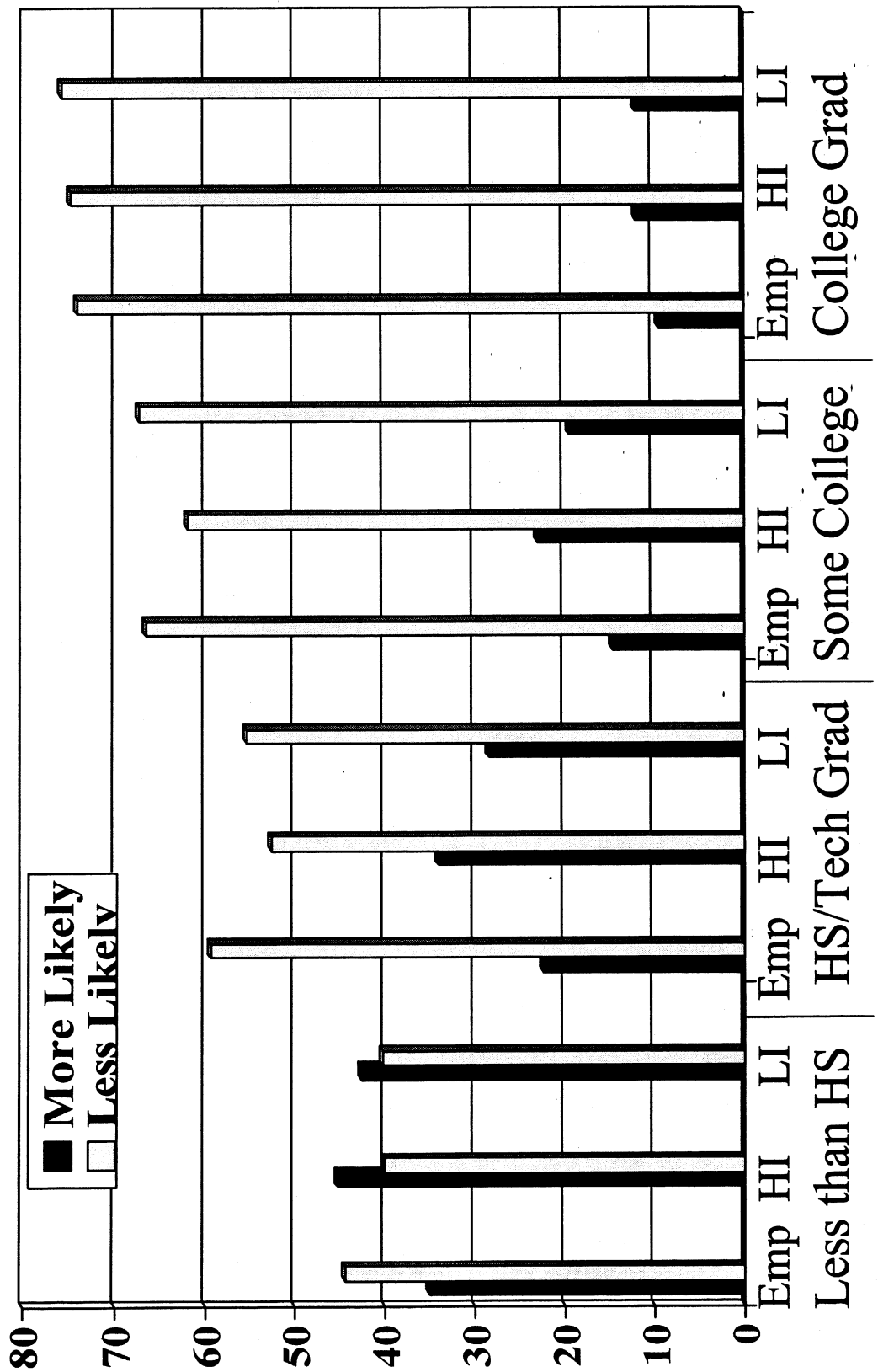
What impact, if any, would it have on your willingness to take a genetic test that showed whether you were more likely to get sick in the future if one of the following could get the results?

- A. Your employer
- B. Your health insurance company
- C. Your life insurance company

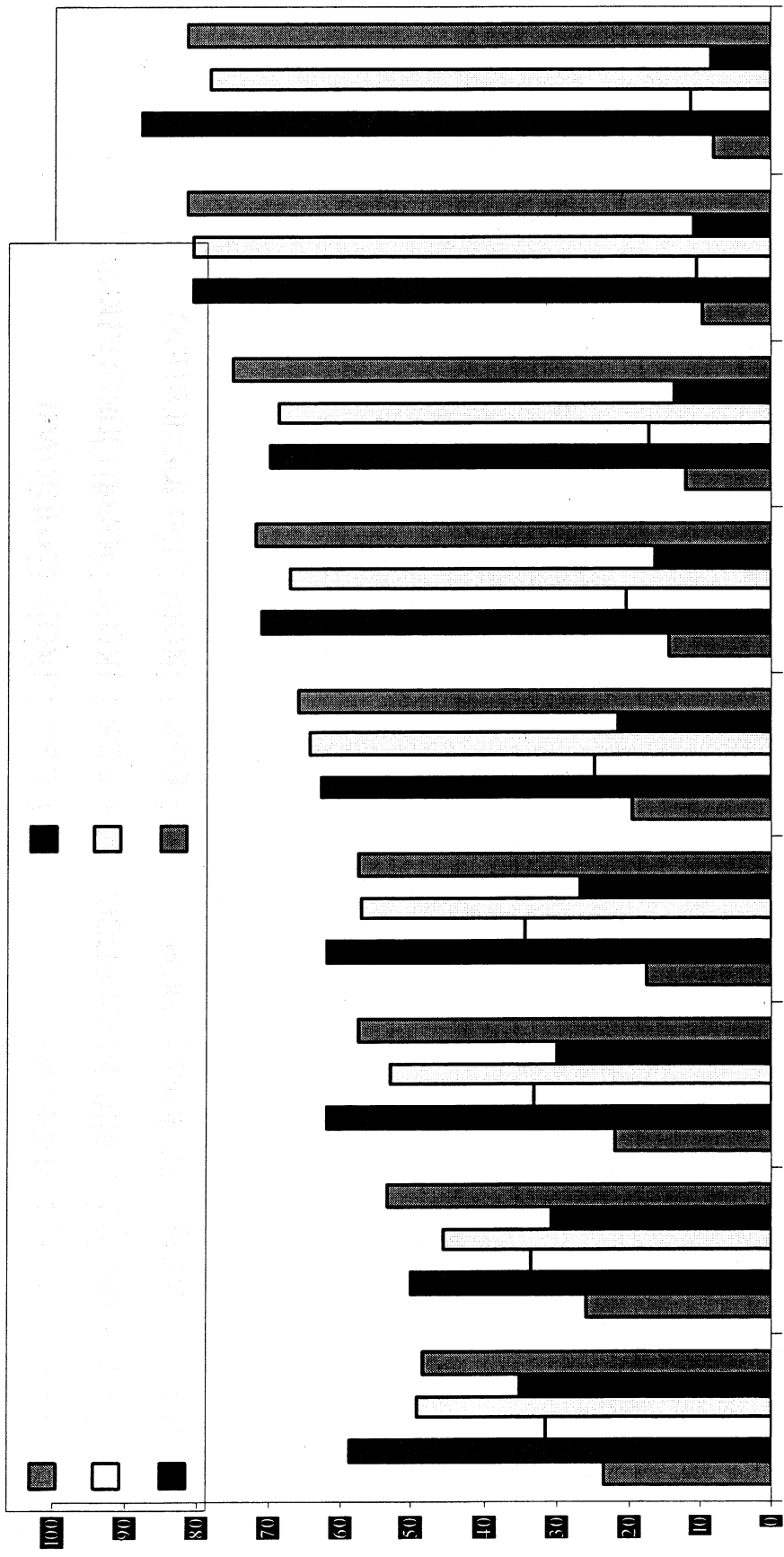
Availability of Test Results and Willingness to Participate in Genetic Testing



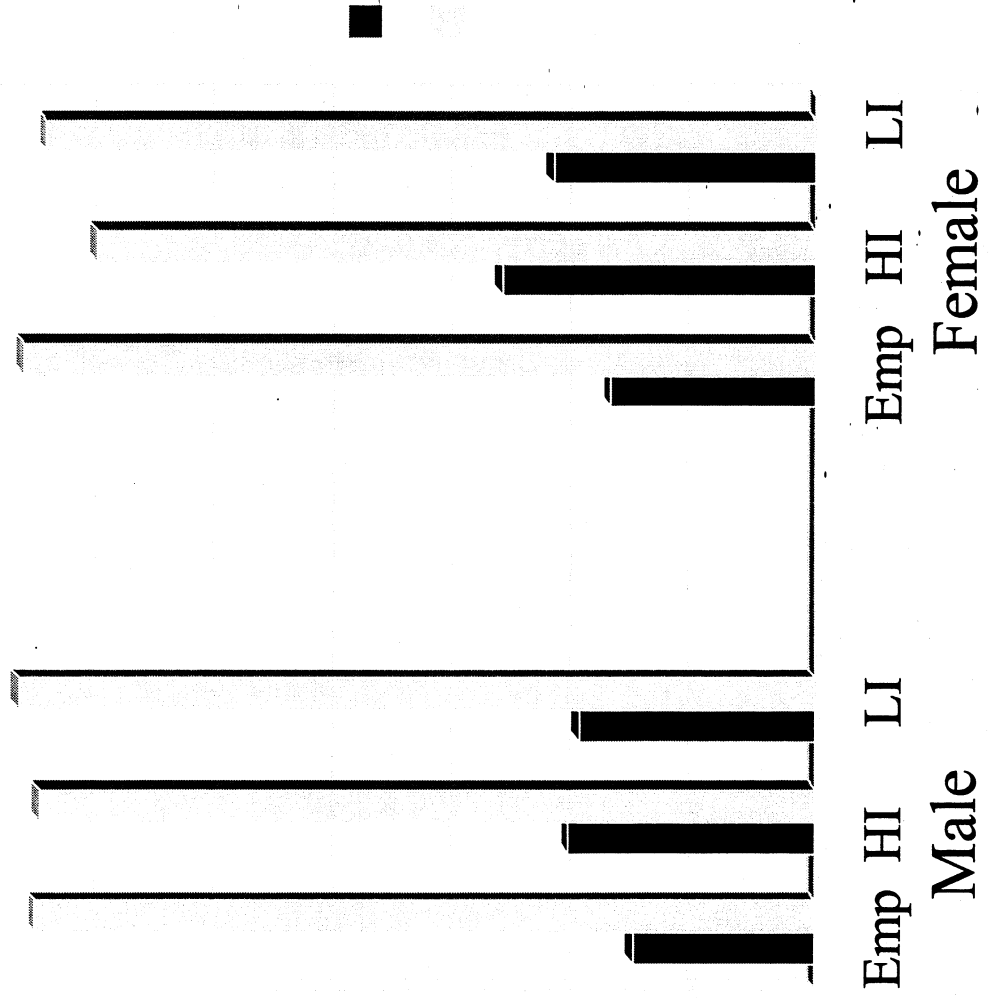
Availability of Test Results and Willingness to Participate in Genetic Testing



Availability of Test Results and Willingness to Participate in Genetic Testing



Availability of Test Results and Willingness to Participate in Genetic Testing



**Other findings related to
concerns about the
confidentiality of genetic
information**

**Controlling for education and
income. . .**

- African Americans were 1.9 times, Asians were 2.6 times, and Hispanics 3.1 times more likely to be tested if an employer could get the results.
- Willingness to have a genetic test if a health insurer could get the results declines with being white, having a higher income, and being male.
- Willingness to have a genetic test if a life insurer could get access to the results declines with having an income over \$50,000, having more years of education, and being white.

Conclusions

1. The need for increased public education about science and genetics.
2. The need for greater cultural sensitivity in research and genetic services.
3. The need to reassess some assumptions about public attitudes regarding research, confidentiality, discrimination, and related matters.
4. The need for continued research about public attitudes about genetics, including surveys in more ethnically homogeneous populations.

Ethical and legal implications of pharmacogenomics

Mark A. Rothstein and Phyllis Griffin Epps

Pharmacogenomics is the application of genomics technology to the discovery and development of drugs. A greater understanding of the way in which individuals with a particular genotype respond to a drug allows manufacturers to identify population subgroups that will benefit most from a particular drug. The increasing emphasis on pharmacogenomics is likely to raise ethical and legal questions regarding, among other things, the design of research studies, the construction of clinical trials and the pricing of drugs.

Pharmacogenomics is changing the way that drugs are developed, approved, marketed and prescribed. The objective of pharmacogenomics is to define the pharmacological significance of genetic variation among individuals and to use this information in drug discovery, thereby decreasing the number of adverse drug responses that injure and kill thousands each year¹. By determining which genetic variations are likely to affect a person's ability to metabolize a drug, drug manufacturers intend to develop more predictable and effective therapeutic agents. Towards this end, pharmaceutical companies are investing huge amounts of capital in the technologies that will revolutionize both how researchers identify drug targets and the amount of time needed to move a drug through development and approval^{2,3}. Pharmacogenomics promises to streamline the clinical trial phase of drug development. Researchers hope to use knowledge gained from high-throughput screening

and other technologies to construct clinical trial groups that are composed of people most likely to benefit from a particular drug. The ability to streamline clinical trials by genotyping will enable researchers to 'rescue' drugs that could not be approved under conventional models of research trials. In other words, drugs that were previously rejected after giving unacceptable rates of adverse responses in traditionally constructed trials will yield lower adverse-response rates after testing under the new model, thereby becoming acceptable candidates for approval. Pharmacogenomics will not only produce better drugs but also yield greater efficiency in the allocation of resources in drug development.

Other changes attributable to pharmacogenomics will be less welcome. Notwithstanding the increasingly efficient research and development process, pharmacogenomic-based drugs will be expensive, because of, for example, the need to recoup the cost of investment in new technologies. The ability to develop specialized drugs that are ultimately approved for smaller populations rather than for general use will fragment the market for pharmaceuticals. Will a pharmaceutical manufacturer react to this economic reality in a way that better suits profit margins than health, and is that socially acceptable? The use of groups in clinical trials that are increasingly similar genotypically raises several important ethical issues regarding social inclusion and the adequacy of current regulatory frameworks. Because polymorphisms of pharmacological interest

might vary in frequency among different population subgroups, important social issues arise in multi-ethnic countries, such as the United States. Finally, pharmacogenomics will change the standard of care for pharmaceutical companies and health professionals, including physicians and pharmacists.

This article provides an overview of some ethical and social concerns that arise with the integration of pharmacogenomics into the discovery of drugs and the practice of preventive and therapeutic medicine. Specifically, the article addresses issues associated with the design of clinical trials, the relatively higher cost of pharmaceuticals developed using pharmacogenomics, and the allocation of ethical and legal responsibility. The objective is to highlight a few of the questions and challenges that will require further attention in the near future.

A new model of clinical trials

Pharmacogenomics promises to reduce the time and money required to develop a drug. The ability to predict drug efficacy by genotyping participants during the early stages of clinical trials for a drug would enable researchers to recruit for later trials only those patients who, according to their genotype, are likely to benefit from the drug⁴. As a result, clinical trials could become smaller, cheaper and faster to run.

The prospect of clinical trials that are composed of smaller groups with the same polymorphisms at one or more loci of interest poses some risks, however. A group that reflects the diversity of the population yields information on how a drug will behave in a greater number of people. If the clinical trial group is smaller, or is less genotypically diverse, there is a greater risk that some side effects will go undetected. So, the trials will yield a greater quantity and quality of information, but on a smaller segment of the population. Whereas the conventional model yielded information about harmful side effects in a greater proportion of the population, the concentration of individuals pre-selected for a favourable response under the newer model might not produce the same information. Compared with traditionally designed human clinical trials, genotype-specific human clinical studies might be subject to equal or greater limitations in that the relatively short duration of the study, combined with the narrower subject population and smaller size, would hinder the ability of the studies to identify rare or delayed adverse reactions or drug interactions⁵. A drug could reach the market with less information about the side effects or risk of harm from its non-prescribed uses. An

Box 1 | Ethical principles of human subject research

In the United States, federal regulations that govern human subject research stem from three ethical principles that were identified in the Belmont Report: respect for persons, beneficence and justice²⁶. As a principle, respect for persons includes two moral requirements: acknowledgement of personal autonomy and protection of individuals with diminished autonomy. In research that involves human subjects, the proper exercise of autonomy demands that research participants agree to enter into research voluntarily and with adequate information. The participant's informed consent is essential. Beneficence also entails two requirements: do no harm and maximize the possible benefits, while minimizing the possible harms. Justice looks at how to fairly distribute the benefits and burdens of research. In the context of research on human subjects, questions regarding how and why research participants are selected are important in satisfying the principle of justice²⁷.

Box 2 | Post-approval monitoring of pharmaceuticals

Despite continuing efforts to harmonize pharmaceutical regulations worldwide, the protection afforded to populations from the risks attendant to drugs that have been approved, after testing in smaller, less genotypically diverse clinical trial groups, depends on the market, member state or country at issue.

United States: In addition to clinical trials, the Food and Drug Administration requires manufacturers to maintain records of clinical experience that would be relevant to determining whether approval of a drug should be withdrawn, and to submit adverse drug reports.

European Union (EU): For pharmaceuticals that have been approved according to the centralized approval process administered by the EU, the European Agency for the Evaluation of Medicinal Products and the Commission on Proposed Medicinal Products require that reports on adverse reactions be submitted every six months for the first two years after approval. Individual member states may have different guidelines in effect that override the guidelines of the European Agency.

Japan: Through the Pharmaceuticals Affairs Bureau, the Ministry of Health and Welfare requires the manufacturer to collect data on adverse drug reactions and to submit products for re-examination and re-evaluation.

unresolved issue is whether the ethical principles of beneficence (BOX 1) and non-maleficence (that is, not causing harm to others) would preclude the deliberate inclusion of anyone who is not likely to respond favourably to treatment. With the advent of genotype-specific clinical trials, manufacturers and regulators must be ready to carefully evaluate post-market data by strengthening the existing guidelines for phase IV, or post-approval, clinical trials^{2,3,5,6-8} (BOX 2).

As in other areas of genetic research that involve human subjects, the likely effect of pharmacogenomics on clinical trials raises important questions regarding informed consent, which might include considerations of privacy and confidentiality⁹. Current ideas regarding patient autonomy and informed consent require that patients agree to enter into research on the basis of adequate information regarding the risks and consequences of participation. Genotyping that is appropriate to pharmacogenomic research might not produce information regarding susceptibility to disease or early death, but it might reveal evidence of genetic variation that could lead to individuals being classified as 'difficult to treat', 'less profitable to treat', or 'more expensive to treat'. The fear of being so classified could act as a barrier to the recruitment of research participants.

Fear of stigmatization might prove to be a significant barrier to participation in clinical trials among members of population subgroups. Genetic variations of pharmacological significance are known to occur in varying frequency in groups categorized by their ethnicity^{10,11}. For example, different variants of glucose-6-phosphate dehydrogenase (G6PD — an enzyme critical for NADPH (nicotinamide-adenine dinucleotide phosphate reduced) generation in mature red blood cells) are found at a high frequency in African,

Mediterranean and Asiatic populations¹², some of which disrupt the function of the enzyme. A deficiency of G6PD can predispose individuals from these populations to haemolytic anaemia, both in individuals with loss-of-function *G6PD* mutations and in

The ability to develop specialized drugs ... for smaller populations rather than for general use will fragment the market for pharmaceuticals. Will a pharmaceutical manufacturer react to this economic reality in a way that better suits profit margins than health ...?

response to some drugs, such as the malarial drug primaquine¹³. Isoniazid is an anti-tuberculosis drug that is inactivated by acetylation; its impaired metabolism by slow acetylation causes it to accumulate to toxic levels. Variation in the *N*-acetyl transferase 2 (*NAT2*) gene accounts for whether individuals are rapid or slow acetylators of isoniazid, as well as of other therapeutic and carcinogenic compounds¹⁴. About 50% of individuals in many Caucasian populations are genotypically slow acetylators of isoniazid, but more than 80% of individuals in certain Middle Eastern populations and fewer than 20% in the Japanese population have the slow acetylator phenotype¹⁵.

The significance of data that imply a role for ethnicity in research has been a source of considerable debate among the research ethics community¹⁵. One issue is how to advise potential research participants about the possibility of social harms from group-based findings even where the research is conducted without using the names of participants. Another matter of considerable debate in the literature is whether it is necessary or feasible to engage in community consultation when genetic research focuses on socially or politically distinct population subgroups^{15,16}.

Cost as a barrier to access

Pharmacogenomic drugs will be expensive, cheaper clinical trials notwithstanding¹⁷. Collectively, the pharmaceutical industry is investing huge amounts of time and money in the development of new technologies that will yield drugs that are more effective than those already available². Without the opportunity to recoup their investment, drug companies will not continue their efforts. At the same time, insurance systems and consumers are struggling to absorb the rising costs of pharmaceutical products^{18,19}.

Pharmacogenomics is based on the idea that pharmaceutical consumers will be better served by drug therapy once they have been subdivided by genotype and matched with the most suitable drug. From the industry perspective, the subdivision of a market into smaller markets is hardly ideal¹⁷. Incentives for pharmaceutical companies to invest time, effort and resources into the development of drugs to treat limited populations are few compared with the development of drugs to treat more prevalent genotypes in the context of pharmacogenomics. Most drug companies might be expected to direct their resources towards the development of drugs to treat the more prevalent genotypes.

Those groups characterized by less-profitable genotypes are at risk of becoming therapeutic 'orphans'. At present, pharmaceuticals for rare diseases are termed 'orphan drugs'²⁰. The United States and Japan have enacted legislation to stimulate research and the development of orphan drugs through market mechanisms, such as tax-based cost incentives and time-limited monopolies²⁰, with varying degrees of governmental intervention. Canada, Sweden, France, the United Kingdom and other countries rely on broader national drug policies based on more substantial governmental intervention. The European Union has entertained initiatives to stimulate legislative action on orphan drugs, and the European Agency for the Evaluation of Medicinal Products has a provision that exempts drug

companies from having to pay application fees to develop a drug if it is an orphan drug (see link to The European Commission's report on orphan medicinal products). Despite allegations of overpricing of orphan drugs under the American model¹⁹, nearly all efforts have been followed by a measurable increase in the number of drugs that have been developed and approved for the treatment of rare diseases²¹. As clinical trials increasingly consist of genetically non-diverse groups, policy makers will need to consider whether to expand the concepts underlying orphan drug policies to stimulate research into and the development of drugs for populations who, by virtue of their genetic make-up, face inequities in drug development efforts.

Cost might act as a barrier to access to pharmacogenomics in that the cost of participating in clinical trials or of the resulting drug therapy might be excluded from insurance coverage. Particularly in the United States, where managed care systems attempt to contain costs by rationing medical services, public and private third-party payers have refused or been reluctant to pay for treatments that they deem 'experimental' or not 'medically necessary'^{22,23}. Increasingly, these terms have more political than legal or medical significance. There is some evidence that the insurers' disinclination to cover expenses that are associated with new drug therapies can be countered by high physician or consumer demand for the new drug²¹. If consumers must absorb rising pharmaceutical costs, pharmacogenomics will not introduce new questions so much as it will intensify existing ones about equitable access to medical care.

Professional standards of care

As pharmacogenomic-based drugs enter into the marketplace, physicians will encounter alternatives to conventional drug therapy and prescription practices. Although the evaluation of genetic variation among patients to determine proper medication and dosage during the course of treatment is not the standard of care at present, ethical concerns, economic considerations and the threat of malpractice liability are likely to encourage physicians to begin testing for and prescribing medications designed for use by specific, smaller groups of individuals. Moral and ethical proscriptions against causing harm might require a physician to integrate pharmacogenetics into clinical practice where necessary to minimize risk to a patient. By contrast, budgetary constraints imposed by insurers could slow the acceptance of drugs developed through pharmacogenomics by limiting their use by physicians and their

availability to patients. The issues raised are not unique to pharmacogenomics but do require new applications of ethical principles and legal doctrine.

In countries where the legal systems are based on common law (that is, the English tradition of law-making based on the court decisions of judges), physicians and pharmacists are subject to liability under theories of negligence, which involve the violation of a duty based on a 'reasonableness' standard or a standard of reasonable care. The standard of care is defined by how a similarly qualified practitioner would act in treating a patient under the same or similar circumstances. The literature, which includes professional scholarship and guidelines published by professional societies, and clinical experience establish the standard of care. In cases based on negligence in the form of medical malpractice, the standard of care is defined through the testimony of witnesses regarding what constitutes conventional practice within the medical community.

Genotyping appropriate to pharmacogenomic research may not produce information regarding susceptibility to disease or early death, but it may reveal evidence of genetic variation that could lead to individuals being classified as ... less profitable ... or 'more expensive to treat'.

As pharmacogenomic-based drugs increase in prevalence over the next several years, the use of genotyping or genetic testing as a diagnostic tool and the prescription of medications based on genotypic information will become the standard of care for physicians. Physicians and pharmacists might be subject to liability if they lack sufficient knowledge of genetics to adequately interpret diagnostic tests, prescribe appropriate pharmacogenomic-based drug therapy in proper dosages, consider pharmacogenomic-based drug interactions, or properly dispense pharmacogenomic-based prescriptions. With greater knowledge comes greater responsibility. Pharmacogenomics might provide greater information about the likelihood

of a drug being effective or causing adverse reactions in persons possessing a particular genetic characteristic, and will certainly yield drugs that are more likely to be suitable for smaller, specific groups of individuals. By increasing the information available for consideration in drug therapy and the importance of matching the right drug to the right person, pharmacogenomics will raise the standard of care applicable to all involved in the safe prescription and distribution of pharmaceuticals.

Pharmacists are primarily charged with the dispensation of prescriptions as administered by physicians, but the scope of their responsibilities has expanded over time to include ensuring that prescriptions and patient directions are correct and appropriate. Pharmacists also have a duty to warn their customers of the potential adverse effects or other problems associated with a prescribed drug therapy. Even if a pharmacist has dispensed a prescription according to a physician's instructions, some jurisdictions have imposed liability on pharmacists for the harm that resulted from a drug that was properly dispensed in accordance with an improper or harmful prescription²⁴. As information regarding the genotype of an individual becomes increasingly important to safe prescription and dosage, pharmacists might be charged with greater knowledge of their customers' genetic information than they now require. The increased amount of genetic information in pharmacies raises privacy and confidentiality concerns, especially where pharmacists belong to large pharmacy chains or corporations with widely accessible, centralized records. For physicians and pharmacists, the issue of continuing professional education and record maintenance will become more important, not only for improving competence but also for preventing liability.

Pharmacogenomics is likely to increase the burden shared by the pharmaceutical industry to provide adequate warnings of the limitations and dangers of their products. In the United States, for example, pharmaceutical manufacturers have a duty to warn physicians about any known or knowable risks, or dangers, of the use of a manufactured drug. Many states in the US will impose strict liability on a drug company for harm caused by the failure to adequately warn against the dangerous propensities of a drug that it has manufactured. Unlike negligence theory, the rules of strict liability are not concerned with the standard of care nor the reasonableness of the manufacturer's conduct; and an aggrieved party need only prove that the manufacturer did not adequately warn of a particular risk

Physicians and pharmacists might be subject to liability if they lack sufficient knowledge of genetics to adequately interpret diagnostic tests, . . . , or properly dispense pharmacogenomic-based prescriptions. With greater knowledge comes greater responsibility.

that was knowable in the light of generally recognized and prevailing best scientific and medical knowledge available at the time of manufacture and distribution. Pharmaceutical companies must consider the potential for liability if patients are harmed because they were excluded from the subgroup for which a pharmacogenomic-based drug is deemed safe and efficacious, particularly if the exclusion leads to a failure to yield information on possible side effects or alternative therapies. Not all adverse side effects are predictable, owing to the number of genes relevant to drug responsiveness, as well as environmental factors⁴. The question is how to allocate responsibility for taking the greatest advantage of drugs specialized to suit relatively smaller segments of the population.

In June 2000, four individuals filed a class action lawsuit against SmithKline Beecham, alleging that the manufacturer of a vaccine for Lyme disease knew that some individuals would be susceptible to arthritis on exposure to the vaccine because of their genotype, but failed to warn about this by labelling²⁵. The case is still pending. Similar cases involve malpractice actions by the patient against the prescribing physician, who in turn seeks to recover against the manufacturer for failure to provide adequate information. Put simply, pharmacogenomics will raise the legal stakes for all involved whenever a patient suffers adverse reactions from the use of a drug that might have been contraindicated based on his or her genotype.

Conclusion

By lessening the uncertainty associated with the selection of drug targets and the design of human clinical studies in the development of new drugs, pharmacogenomics will result in the production of safer, more effective drugs

for use in therapeutic medicine. The integration of pharmacogenomic technology into the drug development process and the practice of medicine will require consideration of ethical, social and legal questions. Answers to these questions might well determine the level of social acceptance and realization of the benefits of pharmacogenomic technology.

Mark A. Rothstein is at the Institute for Bioethics, Health Policy and Law, University of Louisville School of Medicine, 101 West Chestnut, Louisville, Kentucky 40202, USA. Phyllis Griffin Epps is at the Health Law and Policy Institute, University of Houston Law Centre, Houston, Texas 77204-6391, USA. Correspondence to: maroth01@gwise.louisville.edu

Links

DATABASE LINKS G6PD | haemolytic anaemia | NAT2 | Lyme disease

FURTHER INFORMATION European Agency for the Evaluation of Medicinal Products | The European Commission's report on orphan medicinal products | Belmont Report | Food and Drug Administration | European Agency for the Evaluation of Medicinal Products | Pharmaceuticals Affairs Bureau | Journal of Health Politics, Policy and Law | Journal of International Law and Practice | Santa Clara Computer & High Technology Law Journal | Genetic Engineering News

1. Lazarou, J., Pomeranz, B. H. & Corey, P. N. Incidence of adverse drug reactions in hospitalized patients: a meta-analysis of prospective studies. *J. Am. Med. Assoc.* **278**, 1200-1205 (1998).
2. Fanagan, A. Screening technologies evolve: innovations spurred by race to profit from genetic data. *Genet. Eng. News* **20**, 1, 19-20, 71 (September 1, 2000).
3. Barrett, A. The pharma frenzy: in the race for gene-based therapies, big drugmakers join forces with upstarts. *Business Week* 160-161 (June 2000).
4. Roses, A. D. Pharmacogenetics and the practice of medicine. *Nature* **406**, 857-865 (2000).
5. Noah, B. A. Adverse drug reactions: harnessing experiential data to promote patient welfare. *Catholic U. Law Rev.* **48**, 449-504 (2000).
6. Roses, A. D. Pharmacogenetics and future drug development and delivery. *Lancet* **355**, 1358-1361 (2000).

7. Richmond, M. H. et al. *Human Genomics: Prospects for Health Care and Public Policy* (Pharmaceutical Partners for Better Healthcare, England, 1999).
8. Wood, A. J. J. & Woosley, R. Making medicines safer — the need for an independent drug safety board. *N. Engl. J. Med.* **339**, 1851-1853 (1998).
9. Rothstein, M. A. Genetic privacy and confidentiality: why they are so hard to protect. *J. Law Med. Ethics* **28**, 196-204 (1998).
10. Meyer, U. A. Pharmacogenetics and adverse drug reactions. *Lancet* **356**, 1667-1671 (2000).
11. Evans, W. E. & Relling, M. V. Pharmacogenomics: translating functional genomics into rational therapeutics. *Science* **286**, 487-491 (1999).
12. Beutler, E. G6PD: population genetics and clinical manifestations. *Blood Rev.* **10**, 45-52 (1996).
13. Weber, W. W. *Pharmacogenetics* Vol. 15 (Oxford Univ. Press, New York, 1997).
14. Grant, D. M. et al. Human acetyltransferase polymorphisms. *Mutat. Res.* **376**, 61-70 (1997).
15. Sharp, R. S. & Foster, M. W. Involving study populations in the review of genetic research. *J. Law Med. Ethics* **28**, 41-50 (2000).
16. Juengst, E. T. Commentary: what 'community review' can and cannot do. *J. Law Med. Ethics* **28**, 52-54 (2000).
17. Holmer, A. F. Correspondence: the pharmaceutical industry — to whom is it accountable? *N. Engl. J. Med.* **343**, 1415 (2000).
18. Mirzakhani, M. F. & Mossialos, E. Increasing demand while decreasing costs of generic medicines. *Lancet* **355**, 1784-1785 (2000).
19. Angell, M. The pharmaceutical industry — to whom is it accountable? *N. Engl. J. Med.* **342**, 1902-1904 (2000).
20. Thamer, M. et al. A cross-national comparison of orphan drug policies: implications for the U. S. Orphan Drug Act. *J. Hlth Politics Policy Law* **23**, 265-290 (1998).
21. Pulinelli, G. A. The orphan drug act: what's right with it. *Santa Clara Computer & High Technology Law J.* **16**, 299-345 (1999).
22. Kusler, P. C. Financing clinical research and experimental therapies: payment due, but from whom? *DePaul J. Hlth Care Law* **3**, 441-494 (2000).
23. Schoonmaker, M. M. et al. Factors influencing health insurers' decisions to cover new genetic technologies. *Int. J. Technol. Assess. Hlth Care* **16**, 178-189 (2000).
24. *Homer v. Spillito*, 1 S. W. 3d 519 (Mo. Ct. App. 1999) (reversing grant of summary judgement in favor of customer who died from overdose following accurate filling of incorrectly prescribed drug by pharmacist). Available at <http://www.mobar.org/bulletin/nov99/bul-bod.htm>
25. *Cassidy v. SmithKline Beecham*, No. 99-10423 (Pa. Chester County Dec. 14, 1999).
26. National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. *The Belmont Report* (April 18, 1979).
27. Emanuel, E. J., Wendler, D. & Grady, C. What makes clinical research ethical? *J. Am. Med. Assoc.* **283**, 2701-2711 (2000).

Acknowledgements

This work was supported by the National Institutes of Health. The authors are grateful to Joseph Wang for his research assistance.

We welcome correspondence

Has something in the journal caught your attention?

If so, please write to us about it by sending an email to: naturereviews@nature.com and flag it for the attention of the *Nature Reviews Genetics* editors.

Correspondence to the journal will be selected by the editors for publication on the *Nature Reviews Genetics* website at <http://www.nature.com/reviews/genetics/> where it will be linked to the relevant article.

ETHICS:

**Taking an Equity Interest in Your Start-Up Client &
What Can Attorneys Do When the Client Fails**

*Grace M. Giesel
Distinguished Teaching Professor
and James R. Merritt Fellow
Louis D. Brandeis School of Law
University of Louisville
Louisville, Kentucky*



ETHICS: Taking an Equity Interest in Your Start-Up Client

Grace M. Giesel
Distinguished Teaching Professor
and James M. Merritt Fellow
Louis D. Brandeis School of Law
University of Louisville

Table of Contents

| | | |
|-------------|---|------------|
| I. | Background.... | H-1 |
| II. | Forms of Arrangements With Clients..... | H-2 |
| | A. Equity as Compensation | H-2 |
| | 1. Equity as Fees | H-2 |
| | 2. Equity Plus an Hourly Fee at a Discounted Rate..... | H-2 |
| | 3. Equity Plus a Standard Hourly Fee | H-3 |
| | B. Equity Not as Compensation | H-3 |
| | 1. Opportunity to Invest in Start-Ups as a Condition to Representation | H-3 |
| | 2. Lawyers Buy Stock in On-Going Client Enterprises..... | H-3 |
| III. | Motivations... .. | H-3 |
| | A. Client Access to Legal Services | H-3 |
| | B. Access to Legal Advice Plus | H-3 |
| | C. Vote of Confidence | H-3 |
| | D. Potential for a Healthy Paycheck for the Lawyer | H-3 |
| IV. | Investment Vehicles | H-4 |
| | A. Individual Lawyer | H-4 |
| | B. Investment Pool | H-4 |
| | C. Outside Investment Vehicle | H-4 |
| V. | Ethical Concerns | H-4 |
| VI. | Ethical Concerns: Any Compensation for Legal Services Must be a Reasonable Fee | H-5 |
| | A. Rule 1.5(a) of the Rules of Professional Conduct | H-5 |
| | B. Factors in Stock Payment Scenario | H-6 |
| | C. Time of Judging Fairness | H-6 |
| | D. How Can a Stock Fee be Reasonable? | H-6 |
| | E. The Condition of an Opportunity to Invest | H-7 |
| | F. Rule 1.5(b) Requires Communication of the Details | H-7 |

| | | |
|--------------|---|-------------|
| VII. | Ethical Concerns: A Stock Transaction with a Client or Prospective Client Must Abide by Rule 1.8(a), Which Deals with Business Transactions with Clients | H-7 |
| A. | The Rule | H-7 |
| B. | The Rule Applies to Stock Transactions | H-8 |
| C. | There Must Be Full Disclosure in Writing So that the Transaction is Understandable to the Client | H-8 |
| D. | Advice About Independent Counsel | H-9 |
| E. | Burden of Proving Validity | H-9 |
| VIII. | Enforcement of the Contract as a Matter of Common Law | H-9 |
| IX. | Rule 1.8(j)..... | H-9 |
| X. | Conflicts of Interest | H-10 |
| A. | Possible Scenarios | H-10 |
| 1. | Scenario 1: The IPO | H-10 |
| 2. | Scenario 2: The Merger | H-12 |
| 3. | Other Possibilities | H-13 |
| B. | The Lawyer as Advisor | H-13 |
| C. | The Basic Conflict Rule..... | H-14 |
| D. | Application..... | H-15 |
| E. | In-House Counsel Conflict | H-16 |
| F. | Proof of the Conflict's Effect? | H-16 |
| G. | NASD Provisions..... | H-18 |
| H. | Disclosure | H-18 |
| I. | Methods of Limiting the Potential for Problematic Conflict..... | H-18 |
| XI. | Sources Relating Directly to the "Investing in Clients" Movement..... | H-19 |

Ethics:

Taking an Equity Interest in Your Start-Up Client

Grace M. Giesel
Distinguished Teaching Professor
and James R. Merritt Fellow
Louis D. Brandeis School of Law
University of Louisville

Years ago, attorneys did not publicly discuss compensation for legal work. Yet, by the mid-eighties, Gilson and Mnookin noted a change in the profession regarding discussion of compensation with the comment that "yesterday's taboo has become today's fixation." See Ronald J. Gilson & Robert H. Mnookin, *Symposium on the Law Firm as a Social Institution: Sharing Among the Human Capitalists: An Economic Inquiry into the Corporate Law Firm and How Partners Split Profits*, 37 *Stan. L. Rev.* 313 (1985).

This statement may apply exponentially regarding the practice of investing in clients.

I. Background

In recent years, for a variety of reasons, some lawyers have turned to the option of taking an ownership interest in the client business. See Jason M. Klein, *No Fool for a Client: The Finance and Incentives Behind Stock-Based Compensation for Corporate Lawyers*, 1999 *Colum. Bus. L. Rev.* 329. See also Debra Baker, *Who Wants to be a Millionaire*, 86 *A.B.A. J.*, Feb. 2000, at 36. Generally, lawyers did not use such schemes before the 1990s. See John C. Coffee, *The New Compensation*, *N.Y.L.J.*, Mar. 16, 2000, at 5. In some areas of the country, the practice may have been more common earlier. See Shawn Neidorf, *Silicon Valley Lawyers Embrace VC-Like Role*, *Venture Capital Journal*, Oct. 1999, at 35.

One in three lawyers representing the more than 500 companies in Initial Public Offerings (IPOs) in 1999 held stock in that company at the time of the IPO. Sixty-three law firms handled the 500 IPOs. Those lawyers held stock in 174 of the companies. As of the time of an ABA study, the lawyers' investments in forty percent of the companies were worth over one million dollars each. Nine investments exceeded ten million each. See Debra Baker, *Who Wants to be a Millionaire*, 86 *A.B.A. J.*, Feb. 2000, at 36.

At the end of 1999, Wilson Sonsini Goodrich & Rosati, the California firm most often associated with the concept of investing in clients, held stock worth \$230 million in newly-public clients. That amount divided into \$1.9 million per partner. Renee Deger, *Taking Stock: Hitting the Jackpot*, **Recorder**, Jan. 6, 2000, at 1, cited by Royce De R. Barondes, Professionalism Consequences of Law Firm Investments in Clients: An Empirical Assessment, 39 **Am. Bus. L. J.** 379 (2002).

Yet, many nascent businesses fail. Less than ten percent of start up companies ever reach the initial public offering stage. See Mark Suchman & Mia L. Cahill, *The Hired Gun as Facilitator: Lawyers and the Suppression of Business Disputes in Silicon Valley*, 21 **Law & Soc. Inquiry** 679 (1996). Even if the company gets past the IPO stage, chances are that the investment will not yield a return. Nelson D. Schwartz, *The Ugly Truth About IPOs*, **Fortune**, Nov. 23, 1998, at 190.

Even after the sharp downturn of the market, lawyers have continued to be interested in investing in clients. See Francy Blackwood, *Lawyers Take Long View and Put Stock in Clients*, **S.F. Bus. Times**, June 16, 2000. See also Krischer Goodman, *Some Entrepreneurs are Replacing Cash with Equity when Seeking Legal Help: Start Ups and the Law*, **San Diego Union-Trib.**, June 11, 2000. ("The volatility will change our thinking process, but it won't scare us off. We won't get out of the service-for-stock business. We'll just be much more selective about what kind of companies we take equity positions [in] in the future.") (quoting Eliot Abbott of Kluger, Peretz, Kaplan & Berlin).

II. Forms of Arrangements With Clients

A. Equity as Compensation

1. Equity for Fees

The lawyer agrees to do the work but instead of receiving money, the lawyer receives stock. If the company is ultimately successful, the lawyer will be well-compensated for the lawyer's efforts. If the company is not successful, the lawyer has agreed to no payment. This arrangement is much like a traditional contingency fee.

2. Equity Plus an Hourly Fee at a Discounted Rate

Perhaps the lawyer agrees to do the work for a much lower than usual hourly fee with the added compensation of equity. The lawyer shoulders some risk of nonpayment but is certain of partial payment.

3. Equity Plus a Standard Hourly Fee

The equity premium may be consideration for the delay in obtaining payment. The equity may be consideration for the entree the lawyer or firm gives the company in the venture capital market or the reputational benefit in general that comes from being represented by that lawyer or firm.

B. Equity not as Compensation

1. Opportunity to Invest in Start-Ups as a Condition to Representation

The lawyer in demand might request an opportunity to invest as a condition of representation but the equity is not linked to compensation for the legal work performed.

2. Lawyers Buy Stock in On-Going Client Enterprises

III. Motivations

A. Client Access to Legal Services

Taking an ownership interest in the client in exchange for services provides for payment of the lawyer but at the same time does not call for the client to expend sums it does not yet have. Like contingency fees, the stock approach to payment for legal services allows clients to obtain legal services when the client might not otherwise be able to do so.

B. Access to Legal Advice Plus

In addition to legal advice, lawyers invested in the company tend to be more involved in the business decisions. See Poonam Puri, *Taking Stock of Taking Stock*, 87 **Cornell L. Rev.** 99 (2001).

C. Vote of Confidence

Clients like the notion that the lawyer doing the client's work believes in the client. The lawyer who agrees to be paid in stock in the client is showing confidence in the client.

D. Potential for a Healthy Paycheck for the Lawyer

Lawyers like the potential for financial rewards but not necessarily the potential for financial penalty. Apparently, some firms see the opportunity to

share in clients' equity as a way to keep good lawyers from jumping ship and going in-house with clients.

IV. Investment Vehicles

A. Individual Lawyer

The lawyer, whether s/he is in a firm or not, does the legal work and also does the investing. The lawyer decides how much and when.

B. Investment Pool

The lawyer's firm might have an investment pool. Investments would be subject to a committee approval and subject to guidelines as to lawyer involvement and appropriate size of the equity holding. The pool, not the lawyer, would hold the investment.

C. Outside Investment Vehicle

Usually, firms that have an outside-the-firm investment vehicle use a limited liability company form. Unfortunately, some firms have so many partners that the limited liability company may be subject to the Investment Company Act of 1940. See 15 U.S.C. § 80a-1. Compliance with the Act can be very burdensome.

V. Ethical Concerns: Introduction

Some lawyers, uncomfortable with any payment scheme that is not tied to the billable hour, have not ventured into taking stock in clients. Other attorneys have worried that such an arrangement creates insurmountable ethical problems, regardless of whether the equity is compensation for legal services or not.

The ethics issues involve several different ethical principles represented in Kentucky by Rules 1.8(a), 1.5, 1.7(b), and 2.1. (Note that Kentucky's ethics rules are contained in the Kentucky Supreme Court Rules at Rule 3.130.)

In 2000, the American Bar Association Committee on Ethics and Professional Responsibility issued Formal Opinion 00-418 in which the Committee concluded that taking stock in a client as a form of payment can be ethical if the lawyer takes proper precautions with regard to these ethical rules.

Other ethics committees have addressed the issue and have issued the following opinions:

Ass'n of the Bar of the City of New York Comm. on Prof. & Judicial Ethics, Formal Op. 2000-3 (2000);
D. C. Bar Legal Ethics Comm. Op. 300 (2000);
Miss. Bar Op. 230 (1995);
Utah Op. 98-10 (1998); and
Va. Op. 1593 (1994).

VI. Ethical Concerns: Any Compensation for Legal Services Must be a Reasonable Fee

A. Rule 1.5(a) of the Rule of Professional Conduct

Rule 1.5(a) states:

"(a) A lawyer's fee shall be reasonable. Some factors to be considered in determining the reasonableness of a fee include the following:

- (1) The time and labor required, the novelty and difficulty of the questions involved, and the skill requisite to perform the legal service properly;
- (2) The likelihood that the acceptance of the particular employment will preclude other employment by the lawyer;
- (3) The fee customarily charged in the locality for similar legal services;
- (4) The amount involved and the results obtained;
- (5) The time limitations imposed by the client or by the circumstances;
- (6) The nature and length of the professional relationship with the client;
- (7) The experience, reputation, and ability of the lawyer or lawyers performing the services; and
- (8) Whether the fee is fixed or contingent."

Comment 2 to Rule 1.5(a): A fee paid in property "may be subject to special scrutiny because it involves questions concerning both the value of the services and the lawyer's special knowledge of the value of the property."

B. Factors in the Stock Payment Scenario

Obviously, if the lawyer has agreed to equity in exchange for legal services, a big factor is the risk that the stock ultimately will be worth nothing. The lawyer who agrees to do the legal work in exchange for a share of the stock of the company is taking a huge risk that s/he will never realize the value of the legal services. The lawyer who agrees to do the work at a discounted rate plus equity also takes a risk, but does have the possibility, though not certainty, of some payment for the legal work. The lawyer who receives equity on top of standard fee takes the risk of reputational injury if s/he is perceived to have backed a losing enterprise.

Other factors that must be considered in determining reasonableness of a stock for fee arrangement:

1. whether the stock can be publicly traded,
2. when the stock can be traded,
3. other restrictions on transfer, and
4. presently anticipated value.

See Utah Op. 98-13 (1998).

C. Time of Judging Fairness

The determination of reasonableness must be judged by facts known at the time of the agreement. See also **Restatement (Third) of the Law Governing Lawyers** § 126, cmt. e, which states, "Fairness is determined based on facts that reasonably could be known at the time of the transaction, not as facts later develop." This stance is consistent with how contingent fees are judged. See Lester Brickman, *Contingent Fees Without Contingencies*, 37 **U.C.L.A. L. Rev.** 29 (1989).

D. How Can a Stock Fee Be Reasonable?

Determine what would be a reasonable fee under 1.5(a) and then make the agreement give the attorney stock worth that amount at the time of the agreement. The stock should "be valued at the amount per share that cash investors, knowledgeable about its value, have agreed to pay for their stock about the same time." ABA Op. 00-418.

If the stock does not have an ascertainable value, the agreement can award the attorney a percentage of the stock that represents the value that the legal services will "contribute to the potential success of the enterprise." ABA Op. 00-418.

E. The Condition of an Opportunity to Invest

If the lawyer demands an opportunity to invest as a condition of taking the client, one must ask what the client is buying by "paying" the opportunity. If Rule 1.5(a) applies to this setting, note that the "fee" is the opportunity, not simply the investment.

F. Rule 1.5(b) Requires Communication of the Details

The Rule states:

"(b) When the lawyer has not regularly represented the client, the basis or rate of the fee should be communicated to the client, preferably in writing, before or within a reasonable time after commencing the representation."

VII. Ethical Concerns: A Stock Transaction with a Client or Prospective Client Must Abide by Rule 1.8(a), Which Deals with Business Transactions with Clients

A. The Rule

Rule 1.8(a) states:

(a) A lawyer shall not enter into a business transaction with a client or knowingly acquire an ownership, possessory, security or other pecuniary interest adverse to a client unless:

- (1) The transaction and terms on which the lawyer acquires the interest are fair and reasonable to the client and are fully disclosed and transmitted in writing to the client in a manner which can be reasonably understood by the client;
- (2) The client is given a reasonable opportunity to seek the advice of independent counsel in the transaction; and
- (3) The client consents in writing thereto.

B. The Rule Applies to Stock Transactions

ABA Formal Opinion 00-418 states that an agreement with a client to be paid by stock in the client is clearly a business transaction with the client governed by 1.8(a). See also **Restatement (Third) of the Law Governing Lawyers** § 126, cmt. a and G. C. Hazard & W. W. Hodes, **The Law of Lawyering** (3d Ed. 2001) § 12.4.

This rule does not apply when the lawyer gets the stock on the open market or any other way that does not directly involve the client.

Note that the ABA recently issued an opinion clarifying that a contractual security interest obtained by a lawyer to secure a fee must abide by Rule 1.8(a) as well. See ABA Op. 02-427.

C. There Must Be Full Disclosure in Writing So that the Transaction is Understandable to the Client

Match the disclosure to the sophistication of the client.

General disclosure requires discussion of

- "1. the nature of the transaction and each of its terms;
2. the nature and extent of the lawyer's interest in the transaction;
3. the ways in which the lawyer's participation in the transaction might affect the lawyer's exercise of professional judgment in concurrent legal work for the client, if any;
4. the desirability of the client's seeking independent legal advice if the client is not already independently represented; and
5. the nature of the respective risks and advantages to each of the parties to the transaction."

C. Wolfram, **Modern Legal Ethics** (1986) § 8.11.4, at 484-85 (footnotes omitted).

The required disclosure includes a discussion of potential effects. If the lawyer's interest will limit the client's control of the corporation, the lawyer must explain this to the client. If the lawyer is acquiring rights not shared by stockholders generally, the lawyer should explain this.

The lawyer must explain that the lawyer's ownership can create conflict of interest problems for the lawyer in the future. The lawyer must explain that it is possible that the attorney will be torn between acting in the best interest of the corporation and maximizing his own share value. Note that this is especially an issue when the client does poorly. The lawyer should explain that if the conflict manifests, the attorney may feel the need to withdraw completely or with regard to the issue in which the conflict has arisen. See Rule 1.16(b) on the right of permissive withdrawal.

Full disclosure requires a clear statement of the services to be provided in exchange for the stock and a clear statement of the terms of the stock payment. For example, if the stock is to be nonrefundable regardless of the amount of work done, the agreement needs to clearly so state. (Note that some courts, but not in Kentucky (KBA E-380), have found nonrefundable fees contrary to public policy unless the fee is a true retainer--payment to take the matter and to be available. See *In re Cooperman*, 83 N.Y.2d 465, 611 N.Y.S.2d 465, 633 N.E.2d 1069 (N.Y. 1994)).

A recent amendment to the Model Rules (not yet adopted in Kentucky) requires that the client give informed consent "in a writing signed by the client, to the essential terms of the transaction and the lawyer's role in the transaction, including whether the lawyer is representing the client in the transaction."

D. Advice About Independent Counsel

The client must be told of the right to consult other independent counsel. Actual consultation with independent counsel is not required. The lawyer might protect against future claims by having the client state in writing that the client declined from obtaining advice from independent counsel.

See *Passante v. McWilliam*, 53 Cal. App. 4th 1240, 62 Cal. Rptr. 2d 298 (Cal. Ct. App. 1997). A lawyer for a corporation could not recover \$33 million in stock in connection with legal services because the lawyer failed to advise the board of directors prior to the authorization of the stock deal that the board should consult independent counsel.

A recent amendment to the Model Rules (not yet adopted in Kentucky) requires that the client be advised "in writing of the desirability of seeking" independent legal advice.

E. Burden of Proving Validity

If the agreement is ever questioned in the future, the burden will be on the attorney to prove that the transaction was fair and reasonable and in accordance with 1.8(a). Attorneys should take special care to document the circumstances of the transaction at the time of the agreement. See *In re Robins Co.*, 86 F.3d 364 (4th Cir. 1996). See also **Restatement (Third) of the Law Governing Lawyers** § 126 and cmt. e.

***Give the client a choice.

VIII. Enforcement of the Contract as a Matter of Common Law

The relationship of attorney and client is fiduciary in nature. Thus, the lawyer is presumed to have used undue influence in any contractual arrangement with a client. As the Kentucky Court stated in *Hunt v. Picklesimer*, 162 S.W.2d 27 (Ky. 1942), "Even where a conveyance by a client to his attorney is fair upon its face, it is presumptively invalid, and the burden of establishing its fairness is upon the attorney." See also *Gold v. Greenwald*, 55 Cal. Rptr. 660 (Cal. Ct. App. 1966); **Restatement (Third) of the Law Governing Lawyers** § 126 and cmt. b. If the lawyer cannot rebut the presumption, the contract is voidable. See generally Joseph M. Perillo, *The Law of Lawyers' Contracts Is Different*, 67 **Fordham L. Rev.** 443 (1998).

IX. Rule 1.8(j)

Rule 1.8(j) states:

"A lawyer shall not acquire a proprietary interest in the cause of action of subject matter of litigation the lawyer is conducting for a client, except that the lawyer may:

- (1) acquire a lien granted by law to secure the lawyer's fee or expenses; and
- (2) contract with a client for a reasonable contingent fee in a civil case."

This rule may be relevant in rare cases. For example, if the corporation has one asset, and that asset is a claim or property right that is the subject of a pending or expected law suit, Rule 1.8(j) may be applicable. If the stock represents a reasonable contingent fee, 1.8(j) would not be relevant.

X. Conflicts of Interest

A. Possible Scenarios

1. Scenario 1: The IPO

"Flipping through the morning's correspondence deposited in his in-box, Tom Esquire shuffles past envelopes containing plane tickets to a client meeting in New York, an invitation to speak at a conference in Washington, and a chipper notice announcing his twenty-five year high school reunion. Arriving at a gusset-sized envelope from a nearby venture capital firm, Tom stops his shuffling. He slices through the creased flap with his Waterford crystal letter opener and pulls forth the draft offering statement for his new client, Cashout-Dot-Com. Thumbing through the first few pages of the statement, Tom smiles at how the success of this new client will provide him with a proportional windfall. Tom's compensation package for his work on the deal includes eight percent of the stock that he arranged to issue to the incorporators of the company. Cashout-Dot-Com received its Angel financing and substantial venture financing in its first venture capital round. The venture capitalists are eager to take the company public. The market for IPO issues seems strong, and the public offering is set at 100 million dollars with the closing to occur in two weeks. Tom is overwhelmed with pride in helping to facilitate this potential success, and even more overwhelmed at the prospect of finally breaking free of the shackles of his personal line of credit, so frequently strained since the spring that his daughter was accepted at Stanford.

"Just then, Tom receives a telephone call from Washington. Cashout-Dot-Com's principal patent application has just been made the subject of an interference proceeding with a patent application filed by a competitor dot com company. Furthermore, the Patent Office has named Cashout-Dot-Com's inventor as the junior party. As a junior party, Tom's client will have the burden of proof to show that his company invented first. Tom looks more intently at the draft offering statement on his desk. The draft statement includes a section on patent filings, but nothing about the interference. "Investors will want to know about this," Tom thinks to himself. Then the phone rings again. It's Victor Ventura, senior partner in the venture capital firm. Tom tells him about the pending interference.

"Victor exclaims, 'We don't have to put that in there because you're going to win that one for us, aren't you Tom?'

"Tom explains, 'As junior party, this is a tough hill to climb.'

"Victor's response is immediate and authoritative: 'If we put THAT in the statement, this deal may not go. We've got to have an opinion letter from a top-drawer firm like yours that we will win the interference.'

"The phone call ends. Tom slumps in his chair. If he writes a strong opinion letter, the client will think that his firm will win the interference. If he hedges too much, the deal might not go. He doesn't even have enough time before the closing to interview all the principal individuals, analyze the competitor's legal and factual position, and determine the strength of the evidence and the law supporting Cashout-Dot-Com's date of invention. Tom now realizes that his opinion letter is going to be a second-class piece of work. He wishes that he could just pick up the phone, call Victor and say, 'No, we're not going to give an opinion like that.'

"The phone rings again. It's Cashout-Dot-Com's founder. He says, 'Tom, I just talked with Mr. Ventura. He said that this market may have only a short window for doing this IPO, and that you are working on getting the disclosure issues resolved in time. I'm glad we have you to solve these problems.'

"Tom's throat suddenly feels very dry. He can hardly choke out a soft 'thank you,' before hanging up. Tom now realizes his problem. If he had this work on an hourly basis, he would have told Victor 'no way!' without much hesitation ten minutes ago. After all, he has walked away from other client schemes in the past even though the lost fees could have amounted to twenty-five, fifty, or even a hundred thousand dollars. But this one was much harder. In two weeks he would go from a barely positive net worth to never having to work again. He would COUNT. He would be one of the PLAYERS, not just a spectator in the game. He could be worth five to eight million at the moment of issuance, and maybe worth twenty million at the end of the first day's run-up.

Tom knows what is wrong. He has lost his independence. He can no longer provide effective legal advice. He's not practicing a profession now. He's just trying to make money."

Robert C. Kahrl & Anthony T. Jacono, *"Rushes to Riches" The Rules of Ethics and Greed Control in the Dot.Com World*, 2 **Minn. Intell. Prop. Rev.** 51 (2001).

2. Scenario 2: The Merger

Genius and Greedy start Zoom Company. "Times are hard and Greedy thinks that Zoom should merge with Big Pharma Corporation.

Greedy offers Stock, Fore, Feis LLP one percent of all the stock options in the company to handle the legal aspects of the merger. The attorney at Stock, Fore, Feis LLP recognizes that if Big Pharma acquires Zoom, their stock options will probably immediately vest at three to five times any potential Zoom IPO price. Stock, Fore, Feis LLP agrees to handle the merger on these terms and soon Big Pharma arrives at Zoom for a visit. Genius is shocked and exclaims, "What are those suits doing here!" The attorney tries to calm Genius and to explain the merger negotiations, but Genius adamantly refuses. "I worked for that company to help mankind and I'll not involve people like them!" The attorney at Stock, Fore, Feis LLP now faces losing the entire deal, not to mention their only chance at finally getting a good price for all the stock options the firm has accepted. However, if it came down to a vote, Stock, Fore, Feis LLP now has the deciding vote in Zoom and can override Genius. The law firm owns one percent and Genius and Greedy own equal parts of the remainder of Zoom."

Susan A. McQuiston, *Ethical Issues in the Acceptance of Stock Options as Fee Payments for Legal Work*, 6 **Intell. Prop. L. Bull.** 21 (Spring 2001).

3. Other Possibilities

- Conflicts with creditors of the client
- Conflicts with other classes of shareholders
- Conflicts with other constituencies
- Conflicts with venture capitalists
- Conflicts with serial entrepreneurs
- Conflicts in representation of competitors

B. The Lawyer as Advisor

Rule 2.1 states:

"In representing a client, a lawyer shall exercise independent professional judgment and render candid advice. In rendering advice, a lawyer may refer not only to law but to other considerations such as moral, economic, social and political factors, that may be relevant to the client's situation."

C. The Basic Conflict Rule

Rule 1.7(b) states:

"(b) A lawyer shall not represent a client if the representation of that client may be materially limited by the lawyer's responsibilities to another client or to a third person, or by the lawyer's own interests, unless:

(1) The lawyer reasonably believes the representation will not be adversely affected; and

(2) The client consents after consultation. When representation of multiple clients in a single matter is undertaken, the consultation shall include explanation of the implications of the common representation and the advantages and risks involved."

Rule 1.7, comment 3 states, in part:

"Loyalty to a client is also impaired when a lawyer cannot consider, recommend or carry out an appropriate course of action for the client because of the lawyer's other responsibilities or interests."

Rule 1.7, comment 4 states:

"A client may consent to representation notwithstanding a conflict. However, as indicated ... in paragraph (b)(1) with respect to material limitations on representation of a client, when a disinterested lawyer would conclude that the client should not agree to the representation under the circumstances, the lawyer involved cannot properly ask for such agreement, or provide representation on the basis of the client's consent. When more than one client is involved, the question of conflict must be resolved as to each client. Moreover, there may be circumstances where it is impossible to make the disclosure necessary to obtain consent. For example, when the lawyer represents different clients in related matters and one of the clients refuses to consent to the disclosure necessary to permit the other client to make an informed decision, the lawyer cannot properly ask the latter to consent."

A revised Rule 1.7 has been adopted by the ABA but not yet by Kentucky. The revised rule states:

"(a) Except as provided in paragraph (b), a lawyer shall not represent a client if the representation involves a concurrent conflict of interest. A concurrent conflict of interest exists if:

(1) the representation of one client will be directly adverse to another client; or

(2) there is significant risk that the representation of one or more clients will be materially limited by the lawyer's responsibilities to another client, a former client or a third person or by a personal interest of the lawyer.

(b) Notwithstanding the existence of a concurrent conflict of interest under paragraph (a), a lawyer may represent a client if:

(1) the lawyer reasonably believes that the lawyer will be able to provide competent and diligent representation to each affected client;

(2) the representation is not prohibited by law;

(3) the representation does not involve the assertion of a claim by one client against another client represented by the lawyer in the same litigation or other proceeding before a tribunal; and

(4) each affected client gives informed consent, confirmed in writing."

New Comment 14 states, in part:

"Ordinarily, clients may consent to representation notwithstanding a conflict. However, as indicated in paragraph (b), some conflicts are nonconsentable, meaning that the lawyer cannot properly ask for such agreement or provide representation on the basis of the client's consent."

New Comment 15 states:

"Consentability is typically determined by considering whether the interests of the clients will be adequately protected if the clients are permitted to give their informed consent to representation burdened by a conflict of interest. Thus, under paragraph (b)(1), representation is prohibited if in the circumstances the lawyer cannot reasonably conclude that the lawyer will be able to provide competent and diligent representation. See Rule 1.1(competence) and Rule 1.3 (diligence)."

D. Application

Owning stock in a client does not create an inherent conflict of interest. Usually, the lawyer's interest in stock value and the corporation's interest are consistent.

Conflicts can occur, however. In such a situation, the lawyer must consider:

1. the lawyer's ability to render judgment uninhibited by personal concerns and
2. the value of the lawyer's advice given the fact that others may know of the lawyer's interest.

"A partner at one of these firms recently told friends that in 1999 his firm's stock portfolio grew by over \$2 million per partner—more by a significant margin than the firm's per partner earnings from the practice of law. At this point, such a firm truly does become 'multidisciplinary,' with portfolio management being its principal business and legal practice becoming a secondary activity." John C. Coffee Jr., *The New Compensation*, 223 *N.Y.L.J.*, Mar. 16, 2000, at 5.

E. In-House Counsel Conflict

The issue for in-house attorneys may be even more difficult. Think about the conflicts created by Mark Belnick's situation at TYCO International Ltd. Mr. Belnick was general counsel. (He has been indicted for falsifying business records to conceal more than \$14 million in loans he obtained from TYCO. Belnick received a salary of \$700,000, a signing bonus of \$300,000, a \$1.5 million bonus in 1999, a \$4 million bonus in 2000, and \$34 million from the sale of restricted shares. See Laurie P. Cohen, *Tyco's Top Lawyer Joins CEO on Hot Seat*, **Wall Street Journal**, Sept. 13, 2002.

F. Proof of the Conflict's Effect?

A recent article empirically examines the effect investment in clients has on the legal service rendered. The author reported that law firm investment in clients issuing stock may reduce the amount of negative disclosure in IPO prospectuses. The result is that the public interest is injured. See Royce De R. Barondes, *Professionalism Consequences of Law Firm Investments in Clients: An Empirical Assessment*, 39 **Am. Bus. L.J.** 379 (2002).

SEC rules require disclosure in the prospectus of all material information. One of the roles of lawyers in this process is the rendering of an opinion that states that the IPO prospectus is not misleading. Barondes considered whether lawyer ownership of stock in the client affected the disclosure by causing less disclosure, burying the disclosure, or limiting the due diligence investigation. Barondes compared the estimated IPO price that existed prior to due diligence by lawyers and the actual IPO price. Barondes performed a regression analysis regarding his hypotheses.

Barondes based his analysis in part on the idea that a lawyer who is improperly swayed by equity ownership has little risk of punishment. While it is theoretically possible for a lawyer to be held responsible for inadequate securities disclosure, that penalty is not likely. Thus, other than professional morality, there are no significant restraints on fudging behavior.

1. Lawyers are subject to Section 11 of the Securities Act of 1933 only with regard to portions of the prospectus included on the authority of the lawyer as an expert. Usually, this applies to the description of the validity of the securities issued, the description of tax consequences, or unusual descriptions of legal matters.
2. Lawyers are not liable under Section 12 of the 1933 Act because they, generally, are not offering the securities nor are they selling them.
3. Lawyers could be liable under 10b-5 as a primary violator. Some courts may have viewed a lawyer's acts in drafting documents as the basis of a primary violation. See *Breard v. Sachnoff & Weaver, Ltd.*, 941 F.2d 142 (2d Cir. 1991); *Molecular Technology Corp. v. Valentine*, 925 F.2d 910 (6th Cir. 1991).

The Supreme Court has held that there is no private cause of action against one who "aids and abets" a violation of 10b-5. *Central Bank v. First Interstate Bank*, 511 U.S. 164 (1994).

Other courts have held that lawyers cannot be guilty of conspiracy regarding 10b-5. *Dinsmore v. Squadron, Ellenoff, Plesent, Sheinfeld & Sorkin*, 135 F.3d 837 (2d Cir. 1998). See also Mary M. Wynne, Comment, *Primary Liability Amongst Secondary Actors: Why the Second Circuit's "Bright Line" Standard Should Prevail*, 44 *St. Louis L. J.* 1607 (2000).

4. The SEC could bring a civil action against the lawyer as one who "knowingly provides substantial assistance" to a violator. 15 U.S.C. § 78t(e).
5. The receiver appointed to run the law firm's former client could sue for malpractice.
6. The SEC under Rule 102(e) could suspend a lawyer who has engaged in unethical practice before the agency.

For a discussion of the increased liability the practice of investing in clients creates, see Tanya Patterson, Note, *Heightened Securities Liability for*

Lawyers Who Invest in Their Clients: Worth the Risk?, 80 *Tex. L. Rev.* 639 (2002).

G. NASD Provisions

The National Association of Securities Dealers (NASD) forbids underwriters of IPOs to "pay or allocate stock to any of its agents in the transaction, specifically ... attorneys, if the transaction will qualify as a 'hot issue.'" Yet, the attorney does not know in advance what will become a hot issue. John C. Coffee, *The New Compensation*, *N.Y.L.J.*, Mar. 16, 2000, at 5. See also NASD Manual, Standards of Commercial Honor and Principals of Trade, IM-2110-1, Free Riding and Withholding, Part (b), Violations of Rule 2110, Nov. 1998.

H. Disclosure

Regulation S-K imposes an obligation on an issuer's law firm to disclose stock ownership in an issuer. Item 403 of S-K requires disclosure of more than 5% ownership of any class of a company's voting stock. 17 C.F.R. § 229.403.

Item 509 of Regulation S-K requires any expert or counsel who is to receive a "substantial" interest in a company in connection with the offering provide a brief statement of the interest in the related prospectus. "Substantial" is greater than \$50,000. 17 C.F.R. § 229.509.

I. Methods of Limiting the Potential for Problematic Conflict

1. limit investment to an insubstantial percentage of stock,
2. limit the amount invested to a nonmaterial sum,
3. have the supervisory responsible or billing partner not have a financial interest in the client,
4. require executive committee approval of any investment in a client,
5. allot investments in nonpublic clients to partners or put the stock in a pooled fund,
6. take care with regard to securities laws and regulations,
7. use limited liability companies for investments.

XII. Sources Relating Directly to the "Investing in Clients" Movement

Debra Baker, *Who Wants to be a Millionaire*, 86 **A.B.A. J.**, Feb. 2000, at 36.

Royce De R. Barondes, *Professionalism Consequences of Law Firm Investments in Clients: An Empirical Assessment*, 39 **Am. Bus. L.J.** 379 (2002).

Jodi Brandenburg & David Cohen, *Going for the Gold: Equity Stakes in Corporate Clients*, 14 **Geo. J. Legal Ethics** 1179 (2001).

Lester Brickman, *Contingent Fees Without Contingencies*, 37 **U.C.L.A. L. Rev.** 29 (1989).

John C. Coffee, *The New Compensation*, **N.Y.L.J.**, Mar. 16, 2000, at 5.

Laurie P. Cohen, *Tyco's Top Lawyer Joins CEO on Hot Seat*, **Wall Street Journal**, Sept. 13, 2002.

Renee Deger, *Taking Stock: Hitting the Jackpot*, **Recorder**, Jan. 6, 2000, at 1, cited by Royce De R. Barondes, *Professionalism Consequences of Law Firm Investments in Clients: An Empirical Assessment*, 39 **Am. Bus. L. J.** 379 (2002).

G. C. Hazard & W. W. Hodes, **The Law of Lawyering** (3d Ed. 2001) § 12.4

Robert C. Kahrl & Anthony T. Jacono, *"Rushes to Riches" The Rules of Ethics and Greed Control in the Dot.Com World*, 2 **Minn. Intell. Prop. Rev.** 51 (2001).

Jason M. Klein, *No Fool for a Client: The Finance and Incentives Behind Stock-Based Compensation for Corporate Lawyers*, 1999 **Colum. Bus. L. Rev.** 329.

Gwyneth E. McAlpine, Comment, *Getting a Piece of the Action: Should Lawyers Be Allowed to Invest in Their Clients' Stock?*, 47 **UCLA L. Rev.** 549 (1999).

Susan A. McQuiston, *Ethical Issues in the Acceptance of Stock Options as Fee Payments for Legal Work*, 6 **Intell. Prop. L. Bull.** 21 (Spring 2001).

Shawn Neidorf, *Silicon Valley Lawyers Embrace VC-Like Role*, **Venture Capital Journal**, Oct. 1999, at 35.

Tanya Patterson, Note, *Heightened Securities Liability for Lawyers Who Invest in Their Clients: Worth the Risk?*, 80 **Tex. L. Rev.** 639 (2002).

Poonam Puri, *Taking Stock of Taking Stock*, 87 **Cornell L. Rev.** 99 (2001).

Anne E. Thar, *Taking An Equity Interest in a Client--Is It Worth the Risk?*, 89 **Ill. B. J.** 101 (2001).

C. Wolfram, **Modern Legal Ethics** (1986) § 8.11.4 (footnotes omitted).

Mary M. Wynne, Comment, *Primary Liability Amongst Secondary Actors: Why the Second Circuit's "Bright Line" Standard Should Prevail*, 44 **St. Louis L. J.** 1607 (2000).

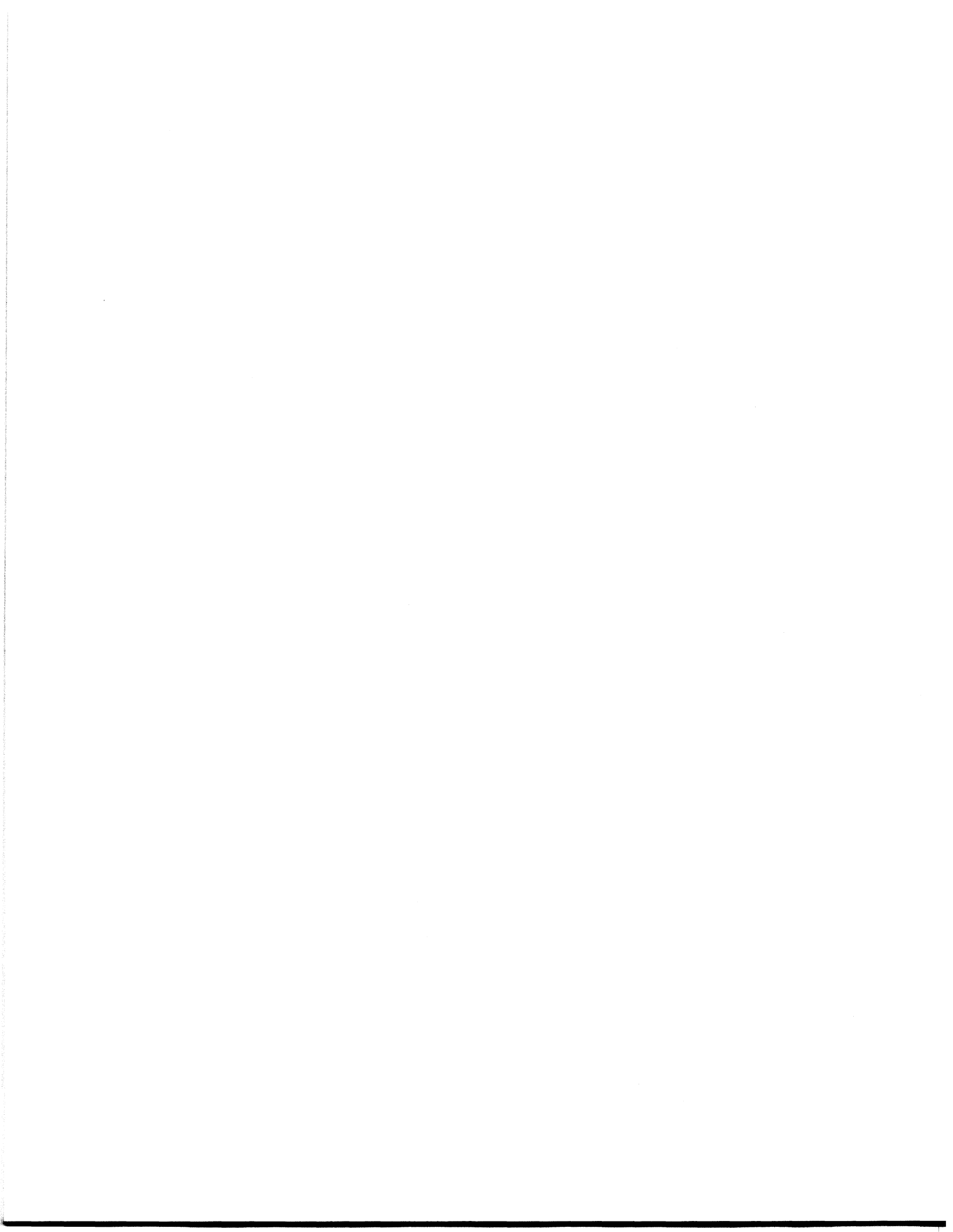
DOTGONE – THE DEATH OF DOTCOMS:

Why did it Happen? Who has Survived? The Next Wave? Bankruptcy Considerations

*Charles R. Keeton
Frost Brown Todd LLC
Louisville, Kentucky*

Copyright 2002, Charles R. Keeton

SECTION I



DOTGONE – THE DEATH OF DOTCOMS:

Why did it Happen? Who has Survived? The Next Wave? Bankruptcy Considerations

*Charles R. Keeton
Frost Brown Todd LLC
Louisville, Kentucky*

Table of Contents

| | | |
|--------------|---|-------------|
| I. | Introduction..... | I-1 |
| II. | Bankruptcy Law vs. Intellectual Property Law and Commercial Law..... | I-3 |
| III. | The Bankruptcy Code..... | I-5 |
| IV. | Licenses..... | I-6 |
| V. | Patents..... | I-8 |
| | A. The Creditor's Perspective..... | I-9 |
| | B. Patent Holder's Perspective..... | I-12 |
| VI. | Copyrights..... | I-19 |
| VII. | Mergers and Acquisitions | I-21 |
| VIII. | The Intersection of Bankruptcy, Online Businesses and Privacy..... | I-22 |

SECTION I

DotGone—The Death of DotComs

Bankruptcy Issues in a Technology Based Economy

By Charles R. Keeton¹

I. Introduction

Throughout history (indeed, even before recorded history²), technological advances have generated growth in specific sectors of the society or economy. In recent years, however, technological advances in industry led the way in terms of over all economic growth.³ The last decade's acceleration in the United States economy was largely technology based. The winners in the stock market for nearly a decade were not the brick and mortar companies, but software companies, computer companies and dot.com startups.⁴ Electronic media such as broadcasting, cable, satellites, telephony and computers were responsible for much of the growth and rapid expansion in communications; computer and Internet industries made a major impact on the way business was conducted.⁵

But technology's impact on business is not new. For example, businesses have used computers since the 1940's.⁶ The Internet as we now know it emerged in 1993. With great

¹ A.B., *summa cum laude*, Marshall University, 1971; J.D., With High Distinction, University of Kentucky College of Law, 1975. Mr. Keeton practices with Frost Brown Todd LLC and is resident in its Louisville, Kentucky, office. Mr. Keeton expresses his gratitude to Jessica C. White, B.A./B.S., University of Arizona, 1995; J.D., Cornell Law School, 1998, for her assistance in preparing this paper.

² See Diamond, J., Guns, Germs and Steel, The Fates of Human Societies (Norton Paperback 1999).

³ Slater, Eric S., *Intellectual Property and Failed Dot-Coms: A New Type of Law Practice*, Chemical Innovation, December 2001, Vol. 31, No. 12, at 56.

⁴ Agin, Warren E., *Reconciling Commercial Law and Information Technology: An Essay on Bankruptcy Practice During the Next Business Cycle*, ABA Business Section Spring Meeting, March 25, 2000, <http://www.swiggartagin.com/articles/reconcile.html>, p 1.

⁵ Slater at 56.

⁶ Agin at 2.

speed the Internet and other computer based technology was integrated into U.S. business. It took radio 38 years to capture 50 million listeners, 13 years for television to reach that mark but only four years for the Internet to hit 50 million users.⁷ Today, the Internet consists of millions of websites and hundreds of millions of people now use it. Ten years ago, some attorneys even in major law firms did not use personal computers, e-mail or the Internet. Today, all major firms and many other industries must use this technology to stay competitive.⁸

Despite technology's impact on today's economy, many technology companies have gone out of business and many investors have lost money. The list of failed dot.coms is enormous and, consequently, an article written today listing the closings would become outdated virtually by the time it is printed. Technology companies extending beyond the dot.coms continue to announce massive layoffs, reorganizations and bankruptcies and the Nasdaq continues to be in bear market territory.⁹ Though this downturn has been aggravated by many other factors, such as the terrorist attacks of September 11, 2001, a weakened job market, and the decline in consumer confidence resulting from accounting errors at WorldCom and the collapse of Enron, issues facing technology companies will continue to play a major role in the economy as companies that are now on the cutting edge are most likely to fail as the business cycle continues to turn downward.¹⁰

⁷ Conrad, Francis G., *Development: Dot.Coms in Bankruptcy Valuations Under Title 11 or [www.Snipehunt in the Dark.noreorg/noassets.com](http://www.Snipehunt.in)*, 9 *Am. Bankr. Inst. L. Rev.* 417 (2001).

⁸ Agin at 2.

⁹ Slater at 56-57.

¹⁰ Agin at 2.

In the midst of these chaotic times for the technology sector, a new specialty is emerging in the practice of law, which includes a mix of bankruptcy, corporate, and intellectual property law.¹¹ Technology issues now play a major role in many bankruptcy cases as new forms of technology become more pervasive in industry. When technology companies, or simply companies using technology, go bankrupt, old fact patterns will give rise to new issues as bankruptcy attorneys gain greater knowledge of and appreciation for technology related issues.

II. Bankruptcy Law vs. Intellectual Property Law and Commercial Law

In general, Bankruptcy law is designed around commercial law concepts. It works well when applied to traditional brick and mortar businesses defined by contract law and the Uniform Commercial Code; however, its application to technology issues is often more difficult or uncertain.¹²

Any analysis in bankruptcy begins with identification and valuation of a company's assets. Unlike the typical brick and mortar company, technology company assets are often described as "virtual," consisting of largely intangible property.¹³ Individual intangible assets include computer software, proprietary technology, copyrights, patents, trademarks, contracts, licenses, employee relationships, supplier relationships, data and customer lists.¹⁴ These assets are generally intellectual property assets and any disposition of such assets will employ intellectual property law principles.

¹¹ Slater at 56-57.

¹² Agin at 3.

¹³ Slater at 56-57.

¹⁴ Reilly, Robert F., *Valuation of Dot-com and Intellectual Property-Intensive Companies*, 2000 ABI JNL, Lexis 101, October 2000. (Note: Many of the citations in this paper are to versions of periodicals on Lexis.)

Unfortunately, the fundamental goals of intellectual property law often directly conflict with bankruptcy law and credit law creating uncertainty for creditors, lenders, investors and the company itself. Bankruptcy law can undermine the protections granted by intellectual property law and has the potential to undo legal protections and interfere with incentives for the creation, cultivation, marketing and distribution of artistic works, brand names, marks and inventions. In addition, the special protections afforded by copyright, trademark, and patent laws impair the predictability that is necessary to the operation of the credit system that finances creative works.¹⁵

Federal bankruptcy law provides a procedure through which a debtor can obtain a “fresh start,” through the liquidation of property and payment of claims or through reorganization. Within bankruptcy, secured creditors who have perfected their interests obtain priority, in the liquidation of claims, over other secured creditors who have failed to perfect, and over all *unsecured* creditors with respect to the secured creditor’s collateral. Perfected secured creditors also receive priority with respect to their secured claims (to the extent of the value of their collateral¹⁶) in bankruptcy reorganizations.¹⁷

Intellectual property law includes three broad areas under federal law: copyrights, trademarks, and patents¹⁸; and covers several incidental areas under state law, such as trade secret law and unfair competition law. The law of secured credit encompasses both state and

¹⁵ Ghosh, Shubha, *The Morphing of Property Rules and Liability Rules: An Intellectual Property Optimist Examines Article 9 and Bankruptcy*, 8 *Fordham Intell. Prop. Media & Ent. L. J.* 99, 102-110 (1997).

¹⁶ See 11 U.S.C. § 506.

¹⁷ Ghosh at 122.

¹⁸ See the U.S. Patent Act (35 U.S.C. § 101 *et seq.*), the Copyright Act (17 U.S.C. § 101 *et seq.*) and the Lanham Act (15 U.S.C. § 1051 *et seq.*). Intellectual property in technology businesses also include domain names, customer lists, customer information databases, trade secrets, online content and back-end systems, among other things.

federal law, but is largely state law. The primary body of state law being Article 9 of the Uniform Commercial Code, which governs the rights of secured creditors against the debtor and other creditors. It follows that the biggest implications of Article 9 are for the federal law of bankruptcy, in which many legal disputes between creditors and the debtor are settled.¹⁹

Intellectual property law and the law of secured credit present two different property rights regimes with different goals and mechanisms. Intellectual property law protects creative efforts and allows creators to exclude others from using the product of such efforts. On the other hand, state credit law and federal bankruptcy law protect the interests that creditors may have in a particular property against claims of the debtor and claims by other creditors. In doing so, the law gives the creditor a *property* interest in the debtor's property.²⁰

Registration of intellectual property rights creates the right of the owner to sue for infringement under federal law; however, filing a security interest secures the rights of a creditor in a legal battle against an owner under state law. This paper will discuss certain rights that exist under the two property systems and will highlight certain conflicts that occur when these two systems interact.

III. The Bankruptcy Code

Section 541 of the Bankruptcy Code defines the property of a bankruptcy estate as including "all legal or equitable interests of the debtor in property." This definition includes intellectual property, of course. The Bankruptcy Code defines intellectual property as

¹⁹ Ghosh at 110.

²⁰ Ghosh at 111-112.

including any trade secret, any invention, process design or plant protected by title 35 of the United States Code (patents), patent application, plant variety, work of authorship protected by title 17 of the United States Code (copyrights), or mask work protected under chapter 9 of title 17 of the United States Code.²¹ If intellectual property is included in the bankruptcy estate, it is subject to being sold in ordinary course, or outside of ordinary course, transactions or included in a reorganization plan.²² Applicable non-bankruptcy law, however, governs the extent of the bankruptcy estate's interest in intellectual property.²³

IV. Licenses

Technology transfers typically take the form of licenses. In many cases, the licensee requires use of the licensed technology for its business operations.²⁴ Bankruptcy courts generally treat licenses as executory contracts because performance is due from both parties to the agreement.

Prior to 1988 licenses for the use of intellectual property received no special treatment or protection under the Bankruptcy Code.²⁵ In bankruptcy, in general the debtor has a choice between keeping a license in effect by "assuming" it, or terminating the license by "rejecting" it. If a debtor who is the licensor rejects the license, the debtor would then

²¹ 11 U.S.C. § 101(35A).

²² As will be discussed later in this paper, a bankruptcy debtor-in-possession authorized under 11 U.S.C. § 1108 to operate the debtor's business may use, sell, or lease property of the estate in the ordinary course of business; and under 11 U.S.C. § 363, may even use, sell or lease property *outside* the ordinary course so long as the requirements of 11 U.S.C. § 363 (including, for example, the requirement that the use occur only "after notice and a hearing," which, as defined in the Bankruptcy Code, really means notice and an opportunity for a hearing.)

²³ Mills, Aleta A., Note & Comment: *The Impact of Bankruptcy on Patent and Copyright Licenses*, 17 Bank. Dev. J. 575, 576, Spring 2001.

²⁴ Agin at 3-4.

²⁵ Weil, Gotshal & Manges LLP, Reorganizing Failing Businesses, Volume I, p. 26-1 (2002).

have lost the license's benefit, and the licensee would have been left with a pre-petition unsecured claim against the debtor.²⁶ Allowing a debtor to legally breach the terms of its license and leave the licensee with only a claim for damages as a remedy was potentially very destructive; the license might have been so crucial that its termination would put the licensee out of business, while the debtor and the other creditors gain only a comparatively minor benefit.²⁷ This course of action also had the effect of denying a licensee of use of intellectual property that it specifically bargained to obtain.²⁸

Lubrizol Enterprises, Inc. v. Richmond Metal Finishers, Inc. (In re Richmond Metal Finishers, Inc.),²⁹ exemplified this issue as the Fourth Circuit took the position that the harm caused to a licensee by rejection of a license was not relevant to the court's decision whether or not to authorize rejection of the contract. The decision created significant business risks for companies relying on licensed technology that were feared would chill technology development and innovation.³⁰ In response, Congress enacted the Intellectual Property Licenses in Bankruptcy Act (codified as 11 U.S.C. § 365(n)) which allows certain licensees to retain certain rights under a license despite a debtor's rejection of the license agreement in bankruptcy.³¹ Most importantly, a licensee can retain the right to retain use of the licensed intellectual property for the remaining term of the license if the licensee continues to pay

²⁶ Id.

²⁷ Again at 4.

²⁸ Weil, Gotshal & Manges LLP at 26-1.

²⁹ 756 F.2d 1043 (4th Cir. 1985); *cert. denied*, Lubrizol Enterprises, Inc. v. Canfield, Bankruptcy Trustee for Richmond Metal Finishers, Inc., 475 U.S. 1057, 106 S. Ct. 1285, 89 L.Ed.2d 592 (1986).

³⁰ Agin at 4.

³¹ See 11 U.S.C. § 365(n).

royalties due under the license contract.³² Under Section 365(n), when a debtor-licensor rejects a contract for a license of intellectual property, the licensee may either elect to treat the license agreement as terminated and assert a claim in the bankruptcy case for damages arising from the breach or elect to retain its rights under the license agreement for the duration of the agreement, as those rights existed immediately prior to the bankruptcy filing by the licensor.³³

V. Patents

Under the Patent Act, 35 U.S.C. § 134, an owner of a patent controls the use of a unique process, business method or machine for twenty years. The patent system seeks to bring advances in technology and design into the public domain. The patent laws encourage public disclosure of new and useful ideas by giving an inventor the exclusive right to practice an invention for a period of years.

In bankruptcy, issues arise for both patent holders and creditors. For example, patent holders face uncertainty in anticipating whether a bankruptcy court will protect patented technology in a sale pursuant to a confirmed plan of reorganization.³⁴ On the other hand, creditors are challenged by uncertainty in the bankruptcy court's interpretation of the law on perfecting security interests in such property.³⁵

³² Agin at 4.

³³ Weil, Gotshal & Manges LLP at 26-5.

³⁴ Henschel, Virginia P., *On the Edge: "Back Door" Access to Patented Technology*, 1998 ABI JNL. Lexis 49, February 1998.

³⁵ Singer, George H., *Security Interests in Patents Ninth Circuit Holds that Article 9 (Not the Patent Act) Governs Perfection*, 2002 ABI JNL. Lexis 33, April 2002.

A. *The Creditor's Perspective*

Patents, copyrights, trademarks and other forms of intellectual property usually constitute "general intangibles" under Article 9 of the Uniform Commercial Code.³⁶ Nevertheless, the law on perfecting security interests in such forms of property is not entirely clear. The primary source of uncertainty comes from the interplay between federal and state law.³⁷

There are a number of federal statutes that establish federal filing systems for perfecting transfers or assignments for various forms of intangible property, some of which possibly include security interests.³⁸ State laws that either interfere with or are contrary to such federal laws are preempted by the United States constitution's supremacy clause. The UCC therefore makes it clear that Article 9 is displaced to the extent that a statute, regulation or treaty of the United States preempts its application.³⁹ The uncertainty in intellectual property secured transactions arises from a lack of clarity with respect to whether federal law or the UCC controls perfecting security interests in intellectual property. The authorities interpreting the federal framework governing intellectual property rights and applicable provisions of the UCC have not provided uniform guidance and limited case law on the issue provides little comfort.⁴⁰

³⁶ Uniform Commercial Code § 9-102(a)(42). See Official Comment 5(d) to § 9-102(a)(42). See also Holt v. United States, 13 UCC Rep. Serv. 336, 337 (D.D.C. 1973) (finding a patent to be a general intangible).

³⁷ Singer at *2. See also R. Nimmer, Commercial Asset-Based Financing, Volume 3, at Chapter 22 (2001).

³⁸ See, e.g., 35 U.S.C. § 261 (patents); 17 U.S.C. §§ 101-603 (copyrights); 15 U.S.C. §§ 1051-1128 (trademarks).

³⁹ Singer at *2-*3 (citing Rev. UCC 9-109(c)(1)); accord, Rev. UCC § 9-311(a)(1) (providing that a financing statement is "not necessary or effective" when federal law preempts its application through an alternative scheme).

⁴⁰ Singer at *3.

In Moldo v. Matsco, Inc. (In re Cybernteic Services Inc.),⁴¹ the Ninth Circuit ruled that a creditor's security interest in a patent trumped the interest of a bankruptcy trustee, even though the creditor did not record its interest with the U.S. Patent and Trademark Office ("PTO").⁴² In this matter, Cybernetic Services, Inc. granted to Matsco Inc. and Matsco Financial Corp. (collectively "Matsco") a blanket security interest in all of its assets, including "general intangibles." Matsco filed its security interest with the California Secretary of State in accordance with the California Commercial Code. Matsco did not file any form of documentation with the PTO. Later, Cybernetic Services Inc. was forced into a Chapter 7 liquidation. As is often the case with many technology companies, the primary asset of the bankruptcy estate was a patent on technology that the debtor developed.⁴³

In the bankruptcy court, the trustee did not dispute the fact that the description of "general intangibles" was sufficient to create a security interest in the patent. The trustee did, however, contend that Matsco's failure to record its interest with the PTO rendered the estate's right to the patent superior by virtue of the trustee's status as a hypothetical lien creditor.⁴⁴ The trustee, contending that Matsco was unperfected, asserted that the Patent Act preempted Article 9's filing requirements and required a federal filing. The Patent Act requires that any "assignment," "grant" and "conveyance" be recorded in the PTO to be

⁴¹ 252 F.3d 1039 (9th Cir. 2001), *cert. denied*, Moldo v. Matsco, Inc., 534 U.S. 1130, 122 S. Ct. 1069, 151 L. Ed. 2d 972 (2002).

⁴² 252 F.3d at 1059; accord, Chesapeake Fiber Packaging Corp. v. Sebro Packaging Corp., 143 B.R. 360 (D. Md. 1992), *aff'd*, 8 F.3d 817 (4th Cir. 1993); and City Bank & Trust Co. v. Otto Fabric, Inc., 83 B.R. 780 (D. Kan. 1988).

⁴³ Singer at *4.

⁴⁴ See the rights granted to the trustee to exercise the rights of certain creditors and/or *bona fide* purchasers under 11 U.S.C. § 544.

effective against a subsequent “purchaser” or “mortgagee.”⁴⁵ The trustee contended that this recording provision requires a patent security interest-holder to record that interest with the PTO to be perfected as to a subsequent lien creditor.⁴⁶

The court of appeals rejected the trustee’s argument and ruled in favor of Matsco. The court analyzed the text, context and structure of the Patent Act’s recording provisions in light of governing case law and concluded that the terms “assignment,” “grant” and “conveyance” all contemplate the transfer of an *ownership* interest only. The court observed that Supreme Court precedent differentiated between those transfers that involved the patent’s title (ownership interests that are required to be recorded) and those that amounted to “mere licenses” (less than ownership interests that are not required to be recorded). The court reasoned that a security interest in a patent was similar to a license and did not represent the kind of conveyance of an interest that was required to be recorded with the PTO. Similarly, the court found that the Patent Act renders unrecorded conveyances void as against only a subsequent “purchaser” or “mortgagee,” which, as a hypothetical lien creditor, the trustee was not.⁴⁷

The court also opined that the applicable PTO regulations supported its interpretation of the Patent Act. It observed that the regulations require all “assignments” to be recorded in the PTO and that filing “other documents affecting title to applications, patents or registrations” was permissive.⁴⁸

⁴⁵ See 35 U.S.C. § 261.

⁴⁶ Singer at *5.

⁴⁷ Singer at *6.

⁴⁸ Singer at *7 (citing Moldo v. Matsco, Inc. (In re Cybernteic Services Inc.), 252 F.3d 1039, 1057-67 (9th Cir. 2001) (quoting 37 C.F.R. § 3.11(a)).

For full protection a creditor is best served by making a dual filing both under Article 9 and under the Patent Act.⁴⁹ Arguably, state filing, provides a creditor claiming an interest in a patent with superior rights only against a subsequent *lien creditor or bankruptcy trustee*. And also arguably, if the secured creditor also wishes to have priority over later *voluntary assignees of title* to the patent (purchasers and perhaps exclusive licensees), the secured party must also record an assignment with the PTO. Secured creditors and the counsel that represent them should remain cognizant of the important role that the federal recording system plays in the realm of secured transactions, particularly where intangible property rights, such as patents, serve as collateral.⁵⁰ Dual filing, both under Article 9 and with the PTO, is the safest course.

B. Patent Holder's Perspective

A patent license is an agreement allowing the licensee to use a patent. It does not transfer any *ownership* interest in the patent. In most circumstances, a patent license is an "executory contract." Generally patent licenses are contracts interpreted under and governed by state law. However, federal common law controls the assignability of patent licenses depending on whether the license is "exclusive" or "non-exclusive." Generally, non-exclusive patent license is construed as only a personal interest in the patent that cannot be assigned unless the patent holder expressly consents. But the Bankruptcy Code has a policy of "free assignability" of executory contracts, as an essential aspect of reorganization,⁵¹

⁴⁹ See Nimmer, *op. cit.*, at § 22.08. As Nimmer, *op. cit.*, points out, the filing with the PTO would be in the form of a collateral assignment.

⁵⁰ Singer at *9-*11.

⁵¹ Generally, a bankruptcy trustee or debtor-in-possession may assume and assign an executory contract despite a contractual prohibition on assignment, unless (1) the contract is sufficiently personal that applicable law excuses a party other than the debtor from accepting performance from, or rendering performance to, an entity other than the debtor or debtor-in-possession (and such party does not consent to such assumption or

which is at odds with the fundamental policy of the federal patent system that seeks to motivate the inventor by allowing the inventor the exclusive right to the invention for a period of years.⁵² Ordinarily, a bankruptcy trustee or debtor-in-possession may assume or assign an executory contract without the consent of the other party to the contract even though the executory contract purports to restrict assignment.⁵³ The Ninth Circuit examined these conflicting policies in Everex Systems, Inc. v. Cadtrack Corp. (In re CFLC, Inc.).⁵⁴ The debtor paid a lump sum fee for a royalty-free, worldwide, non-exclusive license to use certain computer graphics technology. The license agreement specified that the license was non-transferable; that it extended to any company more than 50 percent owned by the debtor; that it conferred on the debtor no right to sublicense; that it could be terminated by the patent holder upon an event of bankruptcy; and that the license agreement was to be construed in accordance with California law.⁵⁵

During the course of its bankruptcy proceeding, the debtor sold off certain divisions, subsidiaries and other assets. The debtor ultimately received approval to sell substantially all of its remaining assets to a third party. The parties to the sale agreement sought assumption and assignment of designated executory contracts, including the key computer graphics technology license. Predictably, the patent holder/licensor objected to the assignment. The

assignment, or (2) the executory contract is a contract to make a loan, or extend other debt financing or financial accommodation, to or for the benefit of the debtor, or to issue a security of the debtor. See 11 U.S.C. § 365(c) and (f). See also the discussion below.

⁵² Henschel at *2.

⁵³ Henschel at 3 (citing 11 U.S.C. §§ 365(a) and 365(f)(1)). See also footnote 51 above.

⁵⁴ 89 F.3d 673 (9th Cir. 1996).

⁵⁵ Henschel at *2 (citing Everex Systems, Inc. v. Cadtrack Corp. (In re CFLC Inc.), 89 F.3d 673 (9th Cir. 1996)).

bankruptcy court denied the motion for assumption and assignment; the district court affirmed that decision.⁵⁶

The Ninth Circuit examined the conflict between the “free assignment” policies of the Bankruptcy Code and the federal common law policy of protecting patent holders. Section 365(c) provides an exception to Section 365’s otherwise broad assumption and assignment powers, stating in relevant part:

The trustee may not assume or assign any executory contract or unexpired lease of the debtor, whether or not such contract or lease prohibits or restricts assignment of rights or delegation of duties, if

(1)(A) applicable law excuses a party, other than the debtor, to such contract or lease from accepting performance from or rendering performance to an entity other than the debtor or the debtor-in-possession, whether or not such contract or lease prohibits or restricts assignment of rights or delegation of duties; and

(B) such party does not consent to such assumption or assignment⁵⁷

The application of the exception set forth in Section 365(c) depends, by its terms, on the “applicable law.” However, the Bankruptcy Code does not tell us which law, whether state or federal, is the “applicable law.” The statutes governing patents are basically silent on the issue of licenses. Patent licenses are generally a matter of state contract law, except where state law would be inconsistent with the aims of federal patent policy.⁵⁸

The Ninth Circuit, in agreement with the Sixth Circuit and the Seventh Circuit, citing PPG Industries Inc. v. Guardian Industries Corp.⁵⁹ stated that “the fundamental policy of the patent system is to ‘encourage the creation and disclosure of new, useful and non-obvious

⁵⁶ Henschel at *2-*3.

⁵⁷ See also footnote 51 above.

⁵⁸ Henschel at *3-*5 (citing In re CFLC, Inc.).

⁵⁹ 597 F.2d 1090 (6th Cir.), *cert. denied*, 444 U.S. 930, 100 S.Ct. 272, 62 L.Ed.2d 87 (1979).

advances in technology and design’ by granting the inventor the reward of the ‘exclusive right to practice the invention for a period of years.’”⁶⁰ Allowing free assignability of non-exclusive patent licenses would undermine the reward of the inventor’s control of the practice of the patent that encourages invention because a party seeking to use the patented invention could seek an assignment of any existing patent license from a licensee instead of seeking a license from the patent holder. If non-exclusive patent licenses are freely assignable, licensees might become competitors with the license-patent holder in the market for licenses under the patents. Even though the patent holder could probably control the absolute number of licenses in existence under a free-assignability regime, it would lose the ability to control the *identity* of its licensees, an issue perhaps more important than the *number* of licensees. For example, a license might in that regime be assigned to the patent holder’s most feared competitor, to whom the patent holder itself might never grant a license.⁶¹ In sum, the court held that under applicable law the patent holder would be excused from accepting performance from, or rendering performance to, anyone other than the debtor/licensee, in the absence of any express agreement by the patent holder to the assignment.⁶²

A later First Circuit opinion, however, left the “back door” open for access to technology licensed to a debtor.⁶³ In Institut Pasteur v. Cambridge Biotech Corp.,⁶⁴ the

⁶⁰ Henschel at *5 (quoting from 89 F.3d 673, 679).

⁶¹ Henschel at *6 (citing 89 F.3d 673, 679).

⁶² Henschel at *6.

⁶³ Henschel at *6-*7.

⁶⁴ 104 F.3d 489 (1st Cir.), *cert. denied*, 521 U.S. 1120, 117 S.Ct. 2511, 138 L.Ed.2d 1014 (1997).

debtor proposed a plan of reorganization under which the stock of the reorganized debtor would be sold to a company in direct competition with the patent holder. This is the “son of” the nightmare scenario contemplated by the Ninth Circuit in In re CFLC, Inc. in which the patent holder would lose the ability to control the identity of the entity exercising the license rights.⁶⁵

In this case the debtor (Cambridge) and the patent holder (Pasteur) entered into cross-license agreements, whereby each acquired a non-exclusive perpetual license to use some of the technology patented or licensed by the other. Each cross-license broadly prohibited the licensee from assigning or sublicensing to others.⁶⁶

The debtor proposed a reorganization plan under which it would assume both cross-licenses, continue to operate using Pasteur’s patented procedures, and sell all of the debtor’s stock to a subsidiary of Pasteur’s direct competitor in international biotechnology sales. Pasteur objected to the plan on the basis that to permit the assumption of the cross-licenses and sale of the debtor’s stock was a *de facto* assignment of the right to use Pasteur’s patented technology without its consent, in violation of federal common law.⁶⁷

While the Court appeared to concede that the federal common law rule of presumptive non-assignability of non-exclusive patent licenses qualified as an “applicable law” within the meaning of Section 365(c)(1)(A); and it agreed that Pasteur could not be compelled to accept performance under the license from any entity other than the debtor

⁶⁵ Henschel at *7.

⁶⁶ Henschel at *7 (citing Institut Pasteur v. Cambridge Biotech Corp., 104 F.3d 489, 490 (1st Cir. 1997)).

⁶⁷ Henschel at *8 (citing Institut Pasteur v. Cambridge Biotech Corp., 104 F.3d 489, 490-491 (1st Cir. 1997)).

party with whom it originally contracted,⁶⁸ the court nevertheless allowed assumption of the cross-licenses.

The court relied on an “actual performance” test adopted in Summit Inv. & Dev. Corp. v. Leroux,⁶⁹ for the application of Sections 365(c) and (e) on a case-by-case basis. The First Circuit disagreed with the In re CFLC, Inc. Court on the basis that the plan in In re CFLC, Inc. provided for an assignment of the license to “an entirely different corporation,” whereas the debtor in Institut Pasteur intended to utilize the patented technology by assumption as the same corporate entity that operated pre-petition.⁷⁰ Absent compelling grounds for disregarding its corporate form, therefore, the debtor’s separate legal identity, and its ownership of the patent cross-licenses, survive without interruption notwithstanding repeated and even drastic changes in ownership.⁷¹

The court suggested that the patent holder could have dealt with the prospect of a change of ownership in or control of the licensee in drafting the license agreement. One wonders though, whether a bankruptcy court sympathetic to a reorganized debtor’s need to use licensed technology might construe provision like those as unenforceable *ipso facto* bankruptcy clauses.⁷²

⁶⁸ Henschel at *8-*9.

⁶⁹ 69 F.3d 608 (1st Cir. 1995).

⁷⁰ Henschel at *9 (citing Institut Pasteur v. Cambridge Biotech Corp., 104 F.3d 489, 493-94 (1st Cir. 1997)).

⁷¹ Henschel at *9 (citing Institut Pasteur v. Cambridge Biotech Corp., 104 F.3d 489, 493-94 (1st Cir. 1997)).

⁷² Henschel at *10. See also 11 U.S.C. § 365(e)(1) that invalidates certain provisions in certain executory contracts that purport to terminate the executory contract upon the happening of specified events, the so-called *ipso facto* clauses.

The “back door” has been closed in the Ninth Circuit.⁷³ In Catapult Entertainment,⁷⁴ the debtor (Catapult) had entered into a non-exclusive patent license with Perlman. As part of a plan of reorganization, Catapult filed a motion with the bankruptcy court seeking to assume the non-exclusive patent license. The bankruptcy court held that the debtor could assume the non-exclusive patent licenses over Perlman’s objection; the District Court affirmed, but the Ninth Circuit reversed. The Ninth Circuit reasoned that the plain language of 11 U.S.C. § 365(c)(1) links non-assignability under “applicable law” with the prohibition on assumption in bankruptcy. The court held that since federal patent law makes non-exclusive patent licenses personal and non-delegable, §. 365(c) is satisfied and as a consequence the debtor was barred from assuming the Perlman license absent Perlman’s consent.⁷⁵

Should the Ninth Circuit Rule prevail, the interest of the patent holder will be protected at the expense of creditors,⁷⁶ while it appears that the First Circuit leaves the back door open for the strategic acquisition of otherwise inaccessible patented technology by industry competitors.⁷⁷

⁷³ Hesse, Gregory G., Column: *On the Edge: Ninth Circuit Slams Shut the “Back Door” Access to Patented Technology*, 1999 ABI JNL. Lexis 41 (April 1999).

⁷⁴ Perlman v. Catapult Entertainment (In re Catapult Entertainment), 165 F.3d 747 (9th Cir.), *cert. denied*, 528 U.S. 924, 120 S.Ct. 369, 145 L. Ed. 2d 248 (1999).

⁷⁵ Hesse at *17.

⁷⁶ Hesse at *18.

⁷⁷ Henschel at *10.

VI. Copyrights

Copyright law follows much of the same pattern as patent law. Federal copyright law is found in 17 U.S.C. § 1010 *et seq.* and grants a limited monopoly to the copyright owner to exploit his or her creation.

The Copyright Act establishes a priority scheme for interests in registered copyrights.⁷⁸ Creators and owners of copyrightable materials, however, are not *required* to register those materials with the U.S. Copyright Office to receive certain benefits of copyright protection.⁷⁹ Owners of copyrightable materials such as computer codes and programs often choose not to register their works in order to protect trade secrets. Thus when copyrightable materials are not registered, the Copyright Act provisions on recordation and priority among conflicting transfers⁸⁰ do not apply and the Copyright Act appears to provide no procedure for recording a security interest in unregistered, copyrightable materials.⁸¹ There is a split of authority on how a lender can perfect a security interest in unregistered copyrightable material. Some courts have held that lenders can perfect a security interest in unregistered copyrightable material by filing a financing statement under the Uniform Commercial Code. But other courts have held that perfecting a security interest in *any* copyrightable material must be accomplished under the Copyright Act.⁸²

⁷⁸ 17 U.S.C. § 205.

⁷⁹ 17 U.S.C. § 408(a).

⁸⁰ See 17 U.S.C. § 205.

⁸¹ White, Bruce H., *A Secured Creditor's Rights to Intellectual Property Licensed by a Debtor in Bankruptcy*, 2001 ABI JNL. Lexis 91, May 2001.

⁸² Vogel, Justin M., Note: *Perfecting Security Interests in Unregistered Copyrights: Preemption of the Federal Copyright Act and How Filing in Accordance with Article 9 Leads to the Creation of a Bankruptcy "Force Play,"* 10 Am. Bankr. Inst. L. Rev. 463, Spring 2002. See also Zenith Productions, Ltd. v. AEG Acquisition Corp. (In re AEG Acquisition Corp.), 161 B.R. 50, (B.A.P. 9th Cir. 1993); and In re Avalon, 209 B.R. 517 (Bankr. D. Ariz. 1997).

Over recent years, several District Court decisions have debated the correct procedures for a lender to perfect a security interest in a copyright, specifically whether Article 9, the Federal Copyright Act or some combination thereof controls perfection. In National Peregrine, Inc. v. Capitol Fed. Savings and Loan Ass'n of Denver (In re Peregrine Entertainment, Ltd.),⁸³ the court concluded that a state recordation system pertaining to interests in copyrights are preempted by the Federal Copyright Act, and therefore, a security interest in a copyright can be perfected only by an appropriate filing with the United States Copyright Office.⁸⁴ However, the court in Aercon Engineering Inc. v. Silicon Valley Bank (In re World Aux. Power),⁸⁵ while agreeing with Peregrine that perfecting a security interest in a *registered* copyright must be done at the federal level, concluded that the Copyright Act's recording provisions are not comprehensive as applied to *unregistered* copyrights and, consequently, do not preempt state law systems for perfecting a security interest in an *unregistered* copyright.⁸⁶ This area of law remains unclear at best. Accordingly, dual filing, both under the Copyright Act and Article 9, is the recommended approach to fully protect a lender.⁸⁷

⁸³ 116 B.R. 194 (C.D. Calif. 1990).

⁸⁴ See also In re Avalon, 209 B.R. 517 (Bankr. D. Ariz. 1997).

⁸⁵ 244 B.R. 149 (Bankr. N.D. Calif. 1999), *aff'd*, 303 F.3d 1120 (N.D. Calif. 2002).

⁸⁶ Vogel at 464; see also the District Court's opinion, 303 F.3d at 1120.

⁸⁷ Rev. Article 9, Rev. 9-109(c), says that Rev. Article 9 defers to federal law only to the extent that Rev. Article 9 is specifically preempted, effectively rejecting the analysis of Peregrine. See Weise, S., *The Financing of Intellectual Property Under Revised UCC Article 9*, 74 Chi-Kent L. Rev. 1077, 1079 (1999). Rev. Article 9's approach continues the uncertainty about the proper manner of perfecting security interests in copyrights under Rev. Article 9. See Nimmer, *op. cit.*, at § 22.09, 2001 Supp.

VII. Mergers and Acquisitions

As the stock market identifies unsuccessful tech companies and prices their stocks accordingly, mergers and acquisitions transactions have emerged as a form of wealth creation for more stable companies. For example, throughout 2000, successful dot.coms acquired unsuccessful dot.com companies (or their assets) at record setting rates. The first quarter of 2000 saw more than \$200 billion in Internet mergers and acquisitions transactions. This period of activity is a model to create value from corporate restructurings.⁸⁸

The over leveraged state of many U.S. corporations presents opportunities for well-capitalized corporations to realize value from corporate restructurings. Such value may be created in several ways. A well-capitalized corporation might acquire a business unit or the entire company from an over leveraged corporation through a Chapter 11 sale or a sale outside of bankruptcy proceedings. A corporation might also consider purchasing distressed debt and exchange such debt for greater value, such as a controlling equity interest in the reorganized debtor, in a Chapter 11 restructuring or a sale outside of bankruptcy proceedings.

There are two fundamental methods of selling or acquiring assets of a debtor in a Chapter 11 case. Assets may be sold outside of a plan of reorganization pursuant to Section 363 of the Bankruptcy Code or a sale can be effected under a plan of reorganization pursuant to Section 1129.⁸⁹ The procedures, benefits and detriments of each approach vary.

⁸⁸ Reilly at Lexis 101.

⁸⁹ Weil, Gotshal & Manges LLC at 11-4.

VIII. The Intersection of Bankruptcy, Online Businesses and Privacy

One potentially valuable asset of a failed dot.com⁹⁰ is the accumulated databases of consumer information that dotcoms frequently obtain. Traditionally, business owners have been able to treat consumer information databases just like any other business asset. As a consequence, consumer information databases are candidates for purchase, sale, depreciation, use as security, or otherwise to be treated as any other business asset. However, due to consumer privacy concerns, there is a growing body of laws and regulations restricting the legitimate uses of consumer information that go beyond the scope of this analysis.⁹¹

The technological development of the Internet marketplace that have made e-commerce possible have also enhanced the ability of companies to collect, store, transfer, and analyze vast amounts of data from consumers who visit their websites. As a result, the Internet marketplace harbors greater risks to consumer privacy than ever before.⁹²

The policies of obtaining a maximum and equitable distribution for creditors and ensuring a “fresh start” for individual debtors are at the core of federal bankruptcy law. As a consequence, it is the main duty of bankruptcy trustees to collect and reduce to money the property of the estate for which the trustee serves, and close such estate as expeditiously as is compatible with the best interests of parties in interests. Many dot.coms have accumulated substantial databases of consumer information, which can be extremely valuable. Thus, a

⁹⁰ As is often the case in technology companies, this issue exists for *any* failed consumer business, but the prevalence of, and technological ease of compiling, customer data in online transactions magnify this issue.

⁹¹ Wingate, John M., Comment: *The New Economania: Consumer Privacy, Bankruptcy, and Venture Capital at Odds in the Internet Marketplace*, 9 Geo. Mason L. Rev. 895-897 (Spring 2001).

⁹² Wingate at 898-900.

trustee seeking to maximize a bankrupt companies estate will attempt to sell consumer databases whenever permitted by law.⁹³

These databases, however, often contain personal consumer data that was acquired in the context of a posted condition of confidentiality. Consumers rely on contract law principles for protection in the event of a bankruptcy arguing that posted confidentiality provisions constitute ongoing contractual obligations that are a part of the online transaction. But contract law fails to provide complete protection in the bankruptcy arena as debtors may reject or assume executory contractual obligations.⁹⁴

A clear rule of law essential to guide the actions of Internet companies and the courts has not emerged though many are familiar with this issue in the aftermath of the Toysmart.com bankruptcy.⁹⁵

Prior to the commencement of bankruptcy, the company overseeing the sale of Toysmart's assets placed an ad offering to sell Toysmart's customer information database. Opposition to the proposed sale was based on the company's privacy policy, which promised, "[w]hen you register with toysmart.com, you can rest assured that your information will never be shared with a third party." The Federal Trade Commission brought suit to enjoin the sale of Toysmart's customer list, alleging that such a sale would violate Section 5(a) of the FTC Act, which prohibits unfair or deceptive trade practices. The Commission argued that such a sale would directly contradict the representation made in the privacy policy and that the representation was a deceptive trade practice. The district court,

⁹³ Wingate at 912-913.

⁹⁴ See the discussion at Section II of this paper.

⁹⁵ Beckmann, Richard A., Comment: *Privacy Policies and Empty Promises: Closing the "Toysmart Loophole,"* 62 *U. Pitt. L. Rev.* 765 (Summer 2001).

however, refused to hear the merits of the case believing that the dispute was properly before the bankruptcy court.⁹⁶

The Commission eventually settled its charges against toysmart. Under the settlement, Toysmart was not permitted to sell the customer information as a stand-alone asset but was permitted to sell the information as part of an ongoing business. The agreement further required that Toysmart only sell to a "Qualified Buyer" that expressly agreed both to be Toysmart's successor-in-interest with regard to customer lists and to handle the information in accordance with Toysmart's privacy policy.⁹⁷

The FTC settlement was opposed in the bankruptcy court by creditors and the state attorneys general on behalf of consumers; however, before the bankruptcy court decided whether to approve the settlement, Toysmart withdrew its application to sell the customer list because it considered the offers that it had received to be insufficient.⁹⁸ Without a buyer, the bankruptcy court refused to rule on whether the list could be sold or the type of restrictions that might be imposed. Thus, the question regarding whether consumer information collected with a promise of privacy can be sold, remains unanswered.⁹⁹

LOUIMDMS/195098.8

⁹⁶ Beckmann at 767-770.

⁹⁷ Beckmann at 767-770.

⁹⁸ Beckmann at 769.

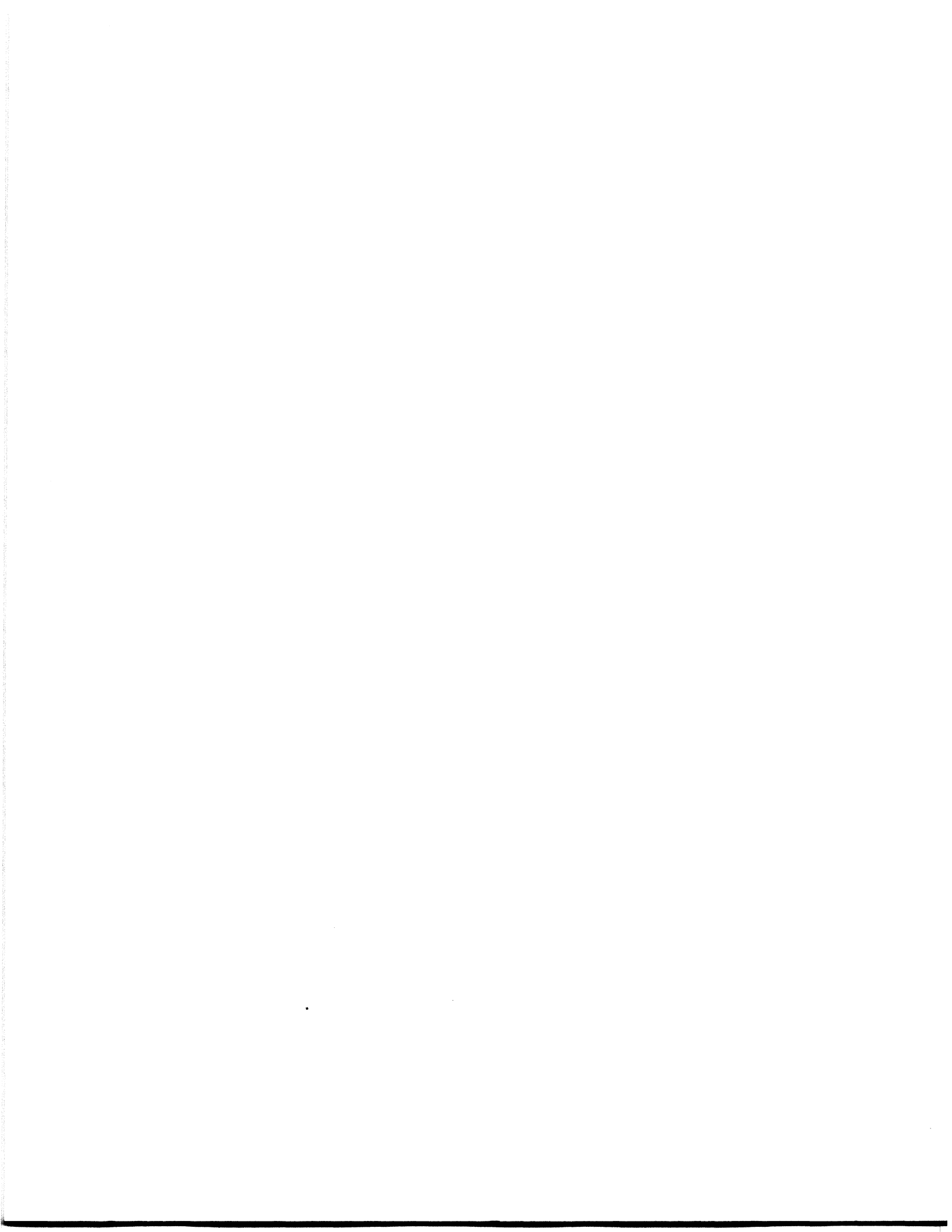
⁹⁹ Beckmann at 767-770.

**GOING GLOBAL:
ISSUES TO CONSIDER WHEN CONDUCTING
BUSINESS THROUGH CYBERSPACE**

*Gregory R. Mues
Frost Brown Todd LLC
Louisville, Kentucky*

Copyright 2002, Gregory R. Mues

SECTION J



GOING GLOBAL:

Issues to Consider When Conducting Business Worldwide Through Cyberspace

*Gregory R. Mues
Frost Brown Todd LLC
Louisville, Kentucky*

Table of Contents

| | |
|--|-------------|
| Slide Presentation..... | J-1 |
| Outline..... | J-19 |
| I. Electronic Signature in Global Context..... | J-19 |
| A. The UNCITRAL Model..... | J-21 |
| B. The European Union Directive..... | J-22 |
| C. The Global Direction..... | J-24 |
| D. Practical Realities..... | J-24 |
| II. Privacy and International Data Transmission..... | J-25 |
| A. The Problem with Data Transmission..... | J-25 |
| B. “Safe Harbor”..... | J-26 |
| C. Safe Harbor Principles..... | J-27 |
| 1. Notice..... | J-27 |
| 2. Choice/Opt Out..... | J-27 |
| 3. Further Transfer..... | J-27 |
| 4. Access to Data..... | J-27 |
| 5. Data Security..... | J-27 |
| 6. Data Integrity..... | J-28 |
| 7. Enforcement..... | J-28 |
| 8. Federal Trade Commission..... | J-28 |
| D. Alternatives to Safe Harbor..... | J-30 |
| 1. Consent..... | J-30 |
| 2. Necessary for Contract Performance..... | J-30 |
| 3. Contract..... | J-31 |
| 4. Adoption of a Compliance Policy..... | J-31 |
| E. Steps to Take..... | J-32 |

| | | |
|------|------------------------------|------|
| III. | Overall Considerations..... | J-33 |
| A. | All Websites Are Global..... | J-33 |
| B. | Sale Restrictions..... | J-33 |
| C. | Consumer Protection..... | J-34 |
| D. | Content Restrictions..... | J-34 |
| E. | Product Regulation..... | J-34 |
| F. | Export Control | J-35 |
| G. | Terms of Use Agreement..... | J-35 |

Appendices..... J-37

| | | |
|----|--|-------|
| 1. | <i>UNCITRAL Model Law on Electronic Commerce with Guide to Enactment</i> (table of contents only; for full document, see http://www.uncitral.org/english/textys/electcom/ml-ecomm.htm)..... | J-37 |
| 2. | <i>The Electronic Commerce and Information, Consumer Protection Amendment and Manitoba Evidence Act</i> (table of contents and explanatory note only; for full document, contact G. Mues)..... | J-41 |
| 3. | <i>Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures</i> | J-45 |
| 4. | <i>Draft Electronic Signature Law, Germany (passed February 15, 2001)</i> (cover sheet and table of contents only; for full document, contact G. Mues)..... | J-54 |
| 5. | <i>The Electronic Signatures Regulations 2002, United Kingdom (effective March 8, 2002)</i> (cover sheet only; for full document, see http://www.legislation.hms.gov.uk/si/si2002/20020318.htm)..... | J-57 |
| 6. | <i>Law Concerning Electronic Signatures and Certification Services—Japan (unofficial translation)</i> | J-58 |
| 7. | <i>Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data</i> | J-82 |
| 8. | <i>U.S. Department of Commerce “Safe Harbor” Overview</i> (for more information, see http://www.export.gov/safeharbor)..... | J-104 |
| 9. | <i>Commission Decision of 27 December 2001 on Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries, Under Directive 95/46/EC</i> | J-108 |

GOING GLOBAL

- A. TWO SPECIFIC ISSUES
 - GLOBAL E-SIGNATURES
 - GLOBAL DATA TRANSMISSION

- B. GENERAL (BUT CRITICAL) CONSIDERATIONS
 - GLOBAL WEBSITES??
 - ARE YOU REALLY READY FOR GLOBAL BUSINESS IN CYBERSPACE

GOING GLOBAL

ELECTRONIC SIGNATURES IN GLOBAL CONTEXT

A. PURPOSE

- Signature is expression of intent to be bound by terms of signed documents
- Signature may be required to satisfy specific laws requiring a signature for enforcement
- Signature serves as an authentication and security device to trace origins and verify integrity of signed document

B. SAME PURPOSES PREVAIL IN ELECTRONIC ENVIRONMENT

C. BUT WHAT IS AN E-SIGNATURE??

GOING GLOBAL

E-SIGNATURES COULD BE MANY THINGS

- Typed name at end of e-mail
- Digital image of actual signature
- A PIN number
- Retinal scan
- Fingerprint
- Mouse Click (e.g. "I accept" button)
- Digital ID created through cryptography
- Etc.

AUTHENTICITY AND SECURITY OF E-SIGNATURES IS CRITICAL IN GLOBAL
E-COMMERCE

GOING GLOBAL

- Domestically Security of E-Signatures is left to the Agreement or Procedure (if any) Established Between the Parties
- Chapter 369 of the KRS Provides:

“(1) An electronic record or electronic signature is attributable to a person if it was the act of the person. The act of the person may be shown in any manner, including a showing of the efficacy of any security procedure applied to determine the person to which the electronic record or electronic signature was attributable.

(2) The effect of an electronic record or electronic signature attributed to a person under subsection (1) of this section is determined from the context and surrounding circumstances at the time of its creation, execution, or adoption, including the parties’ agreement, if any, and otherwise as provided by law.”

- DOMESTIC APPROACH TO AUTHENTICITY IS LARGELY ONE OF FACT/CIRCUMSTANCE

GOING GLOBAL

- THIS IS NOT THE CASE ON INTERNATIONAL FRONT – SECURITY PROCEDURES ARE TRENDING TOWARDS THE MANDATORY
- THE UNCITRAL MODEL (1996)
 - Model Law on Electronic Commerce
 - Would not replace existing law on contract formation/enforceability
 - Give recognition to E-signatures as the functional equivalent of handwriting
 - (Under Article 7 concept of Security was included by requiring that an E-signature be “Reliable”
- UNCITRAL MODEL NOT WIDELY ADOPTED BY HAS SERVED GOOD PURPOSE
 - Similarities to UETA
 - Served as Canadian approach

GOING GLOBAL

- THE EUROPEAN UNION MODEL
 - 1999 EU Directive On E-Signatures (Directive 1999/93/EC)
 - Great detail on security of E-signatures
- E-Signatures (As conceptualized by the UETA and KRS) would not be given recognition. An E-signature must be an “Advanced Electronic Signature” as defined in the directive to merit recognition/receive legal effect.
- An “Advance Electronic Signature” is one based on a “Qualified Certificate” and would have to be created by a “Secure-Signature-Creation-Device” – both as specified in the Directive.

GOING GLOBAL

- EU Directive and Resulting member State Laws impose a system of third party providers of Qualified Certificates
 - Liable for accuracy of Certificate content
 - Certificate meets State law requirements
 - Identified signatory is authentic
 - Recognition of Qualified Certificate issued from Non-EU member countries
 - Provider must meet Directive requirements

OR

- EU certificate provider guarantees the Certificate

OR

- Certificate or the provider is recognized under an international agreement with the EU

GOING GLOBAL

- GLOBAL DIRECTION OF E-SIGNATURES IS CLEARLY TO MIMIC THE EU
 - Clearly trend is Far East
 - Former USSR States likewise

- E-COMMERCE IN/WITH EU AND OTHER FOREIGN ENTITIES
 - Have you investigated the need for qualified certificates Re your E-signature?
 - Have you established an E-signature and an arrangement with a Qualified Certificate provider?

GOING GLOBAL

PRIVACY ISSUES

- RAPID DEVELOPMENT OF PRIVACY AND DATA TRANSMISSION LAWS GLOBALLY
- MOST VEXING PROBLEM FOR US ENTITIES, ESPECIALLY MULTINATIONALS, IS EU DATA PROTECTION DIRECTIVE (EU DIRECTIVE 95/46/EC).
- DIRECTIVE SETS OUT MANY RESTRICTIONS/RIGHTS OF INDIVIDUALS AS TO PERSONAL DATA

GOING GLOBAL

- PROHIBITION CAUSING GREATEST DIFFICULTY IS THAT (WITH FEW EXCEPTIONS) FORBIDDING TRANSFER OF PERSONAL DATA OUTSIDE THE EEA TO ANY COUNTRY WHICH EU DETERMINES DOES NOT PROVIDE “ADEQUATE LEVEL OF PROTECTION”

- HOW CAN YOU DO BUSINESS UNDER THIS KIND OF CLOUD?
 - Employee data

 - B2C Data

 - Etc.

 - Severe penalties

GOING GLOBAL

- US/EU SAFE HARBOR ARRANGEMENT
 - Clinton administration initiative
 - Largely administered by FTC
 - EU recognition (Commission Decisions of July 20, 2000)
- VOLUNTARY SIGN UP TO ADOPT/ADHERE TO DATA PROTECTION PROCESSES WHICH MIMIC THOSE OF EU. SELF CERTIFY TO COMMERCE DEPARTMENT AND LISTED ON COMMERCE WEBSITE.
- IF IN SAFE-HARBOR DEEMED TO OFFER ADEQUATE PROTECTION TO TRANSMITTED DATA.

GOING GLOBAL

- SAFE HARBOR PRINCIPLES:
 - Notice
 - Choice/Op out
 - Further transfer
 - Access to data
 - Data security
 - Data integrity
 - Enforcement
 - FTC

- SAFE HARBOR DOES NOT COVER SECTORS OUTSIDE FTC OVERSIGHT
 - e.g. Banks, S&L's, Brokerage

GOING GLOBAL

- ALTERNATIVES TO SAFE HARBOR?
- (1) – Consent Of Individual
 - Could be implied if individual requests transfer
 - Best to get express (affirmative disclosure and express “I Agree”)
- (2) – Necessary For Contract Performance
 - Ongoing question is: What is necessary
- (3) – Approved Contractual Clauses
 - Commission decision December 27, 2001
 - Approved draft clauses to cover data transmission
- (4) – Adoption of a Compliance Policy
 - Applicable to transmission with a related group
 - Would not cover onward transmission to unrelated entities

GOING GLOBAL

- STEPS TO BE TAKEN
 - Audit current cross border data flows
 - Enter for safe harbor?
 - Consider safe harbor alternatives
 - Monitor compliance
 - Monitor countries on EU “Adequate Protection” list

GOING GLOBAL

GENERAL (BUT CRITICAL) CONSIDERATIONS

- HAVE YOU CONSCIOUSLY DECIDED/PLANNED TO CONDUCT INTERNATIONAL BUSINESS VIA THE INTERNET (B2B, B2C)
- DO YOU HAVE A WEBSITE DESIGNED FOR
 - B2B, B2C
 - Information dispersal
 - Information gathering
- IS YOUR WEBSITE BEING ACCESSED BY NON-US PARTIES

GOING GLOBAL

- DECISION TO CONDUCT GLOBAL BUSINESS VIA INTERNET MUST BE DELIBERATE AND TARGETED BY COUNTRY
- PRACTICALLY SPEAKING INDIVIDUAL COUNTRY WEBSITES ARE NEEDED TO ADDRESS ALL OF THE SAME COMMERCIAL AND LEGAL REQUIREMENTS APPLICABLE TO THE PAPER WORLD

GOING GLOBAL

- BUSINESS WEBSITE MUST BE DESIGNED TO ADDRESS
 - Language
 - Sales restrictions
 - Local privacy requirements
 - Local E-Signatures/E-Commerce laws
 - Consumer protection laws
 - Product compliance with local codes
 - Delivery terms
 - Payment terms and method (currency considerations)
 - Pricing (including cost of compliance)
 - U.S. export control compliance
 - Tax consequences (e.g. VAT, Permanent Establishment)

GOING GLOBAL

- TRANSITION FROM TRADITIONAL DOCUMENTARY TRANSACTION FLOW TO INTERNET BUSINESS IS FRAUGHT WITH TRAPS.
- EACH TARGET COUNTRY MUST BE THOROUGHLY RESEARCHED PRIOR TO OPENING A WEBSITE FOR BUSINESS

GOING GLOBAL: ISSUES
TO CONSIDER WHEN CONDUCTING BUSINESS
WORLDWIDE THROUGH CYBERSPACED

I. ELECTRONIC SIGNATURES IN GLOBAL CONTEXT

Signatures, and this traditionally means in the handwriting of the signor, serve many purposes in any given transaction such as:

- An expression of intent to be bound by and comply with the terms of the signed document
- Satisfaction of Laws that require certain kinds of documents to be signed in order to be enforceable
- Authentication and Security devices to verify the integrity of a document and to trace its origin to a specific person or entity.

In the electronic environment the purposes of a "signature" are the same and this can be said to apply in virtually all jurisdictions. However, a "signature" in the electronic environment can be many things given the basic impediment to hand signing.

For example, an electronic signature could be:

- A name typed at the end of an e-mail message or purchase order
- A digital image of an actual signature at the end of an electronically transmitted document
- A password or personal identification (PIN) number maintained by the recipient of a communication
- A retinal scan

- A fingerprint
- A voice print
- A mouse click (like clicking an "I agree" box on a computer screen)
- A "digital signature" created through cryptography.

There are many others conceivable, but in the e-commerce area the security related purposes of identity and integrity are critical if this kind of commerce is to work. Before one takes the step of executing payment to a web-based supplier or, visa versa, before a supplier makes shipment to a web-based customer (B2B or B2C), there needs to be sufficient faith in the identity/security aspects of the electronics that the mouse click or the digital image or the typed name really is that of the other party claiming to be who he is.

Domestically, federal and state legislation has given legal effect to digital signatures but the element of the security and authenticity of these signatures is not specifically addressed. These laws enforce the use of electronic signatures (and records) but say little, if anything, about security procedures. This is the approach taken by the Federal E-SIGN law (Electronic Signatures in the Global and National Commerce Act, 15 U.S.C. 7001 *et seq.* and in the UETA (Uniform Electronic Transactions Act) approved by the National Conference of Commissioners on Uniform State Laws on July 23, 1999. The UETA has provided the model for domestic state statutes.

The e-signature situation has developed differently on the international front where the issue of authenticity and security has been specifically addressed.

A. THE UNCITRAL MODEL

The United Nations Commission on International Trade Law (UNCITRAL) concluded the UNCITRAL Model Law on Electronic Commerce in 1996 (General Assembly Resolution 51/162 of 16 December 1996). This attached at Tab 1 for reference.

The object of the UNCITRAL model is to provide a draft that a given country may use to enact its own legislation, not to replace any existing laws on contract formation or enforceability, but rather to give legal recognition of electronic documents, records and signatures as being the functional equivalent of paper records under existing national law.

As to e-signatures Article 7 of the UNCITRAL model provides:

" (1) Where the law requires a signature of a person, that requirement is met in relation to a data message if:

- (a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and
- (b) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

(3) The provisions of this article do not apply to the following: [...]." (**emphasis added**)

Thus under the UNCITRAL model the concept of security has been incorporated by use of the word "reliable" to describe the method used to tie the electronic signature to the actual person using such signature. This method is left to be determined by the adopting country

involved including any relevant agreement between the e-transacting parties as to security measures.

The UNCITRAL model has served its purpose. Similarities can be seen with the UETA and it has been adopted in modified form by at least three Canadian provinces. Attached for reference is the Manitoba enactment under Tab 2.

On balance, however, the UNCITRAL model has not gotten wide international acceptance. The European Union approach has been much more widely embraced, probably because it has addressed the security requirement of e-signatures with much greater specificity than the UNCITRAL draft and certainly more than the UETA.

B. THE EUROPEAN UNION DIRECTIVE

In 1999, the European Union (EU) passed a Directive on electronic signatures which goes into much greater detail on the security of e-signatures than other international forerunners. This is Directive 1999/93/EC of December 13, 1999 on a Community framework for electronic signatures, attached under Tab 3.

The object of this Directive is to require the EU member states to give legal recognition of electronic signatures under their respective natural laws. However, it is very important to note that it is not "electronic signatures", as defined in the Directive, which are given recognition but rather "advanced electronic signatures" under Article 5. The differences are evident under Directive's Article 2 which states:

"For the purpose of this Directive:

1. 'electronic signature' means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication;
2. 'advanced electronic signature' means an electronic signature which meets the following requirements:

- (a) it is uniquely linked to the signatory;
- (b) it is capable of identifying the signatory;
- (c) it is created using means that the signatory can maintain under his sole control; and
- (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;"

Furthermore under Article 5 in order for an "advanced electronic signature" to be given legal effect it must be based on a "qualified certificate" and would have to be created by a secure-signature creation device" as both terms are described in Article 2(6) and (10) respectively:

- "6. 'secure-signature-creation device; means a signature-creation device which meets the requirements laid down in Annex III;
- 10. 'qualified certificate' means a certificate which meets the requirements laid down in Annex I and is provided by a certification-service-provider who fulfills the requirements laid down in annex II."

As can be seen from the above, the EU e-signature regime is based on the use of technologies that can create a secure e-signature, accompanied by a third party qualified certificate provider who attests to the authenticity of the particular e-signature. Under Directive Article 6, the certificate provider is liable for damage caused by reliance on the certificate as to the accuracy of its content; that it meets the requirements of the specific law governing such certificate; that the signatory identified is valid.

While the Directive is an internal EU measure, Article 7 addresses recognition of certificates issued by certification providers of third countries. These are to be given legally equivalent treatment to EU issued certificates if:

- "(a) the certification-service-provider fulfils the requirements laid down in this Directive and has been accredited under a voluntary accreditation scheme established in a Member State; or
- (b) a certification-service-provider established within the Community which fulfils the requirements laid down in this Directive guarantees the certificate; or
- (c) the certificate or the certification-service-provider is recognized under a bilateral or multilateral agreement between the Community and third countries or international organizations."

Unlike EU Regulations, EU Directives are not self executing. Directives are what the term implies, directions to the member states to implement the provisions of the Directive into their respective national laws. The basic tenets of the Directive are to be respected but differences (for example in level of Fines) can result member to member.

Attached for comparison under Tab 4 and Tab 5 respectfully, are the German and United Kingdom enactment of the Directive. Both adhere to the tents of the Directive but differ in their amalgamation into the national law.

C. THE GLOBAL DIRECTION

The global trend in e-signature legislation is clearly to parallel that of the EU. For example, attached under Tab 6 is the Japanese "Law Governing Electronic Signatures and Certification Services" (Unofficial Translation). This mimics the EU pre-occupation with e-signator security and goes beyond in the creation of investigative processes and investigative bodies in oversight of certificate providers. Singapore and Korea, two more major U.S. trade partners have as well embraced the EU approach. We can expect this global trend to continue.

D. PRACTICAL REALITIES

The practical reality of the differing international approaches to recognition of e-signatures is, of necessity, to accommodate them.

As an actual or potential U.S. entity engaging in cross border activities, be it simple exporting, all the way through to local investment with manufacturing, delivery and service infrastructure, one needs to research the e-contracting law of the target jurisdiction. There is but little choice to understand the e-contracting/e-signature regimes of the target market. One can then structure internet transactions to fully comply with the local requirements.

For example, if e-commerce is going to be conducted with customers/consumers in EU member countries, and elsewhere with similar e-commerce laws, then it would make sense to install the requisite secure signature creation devices and contract for third party certification services to support such transactions. If any issues arise as to the applicability of local law, one would certainly want to be assured that a valid signature has been established if needed to prove the existence and enforcement of an agreement, among other things.

II. PRIVACY AND INTERNATIONAL DATA TRANSMISSION

The development of privacy and data transmission laws around the globe has been wide and rapid. The most vexing issue for US based entities, especially multinationals, resulting from this development has been the EU Data Protection Directive's restrictive impact on data flow between the EU and the United States. This EU Directive 95/46/EC is attached under TAB 7.

The Data Protection Directive required European Union (EU) countries to implement equivalent national legislation by 24 October 1998. Most EU countries have now complied.

A. The Problem With Data Transmission

Broadly speaking, the Directive sets out eight principles which organisations must observe in use of personal data. Personal data is identifying information about individuals such as name, contact details, email address etc. The Directive also gives individuals rights in relation

to their personal data. These include the right to access personal data held by an organisation, the right to object to direct marketing and the right to compensation for contravention of the principles.

Difficulty between the EU and US arose in relation to the prohibition, with few limited exceptions, on the transfer of personal data outside the European Economic Area (EEA) to a country which the EU determines does not afford an adequate level of protection to that data. The EEA is made up of the 15 EU Member States together with Iceland, Liechtenstein and Norway. EU officials have stated that the majority of countries outside the EEA, including the US, have inadequate data protection regulation.

The consequences of this prohibition pose a serious threat to worldwide trade. In the global economy, where companies freely need to transfer personal data from country to country, a restriction of this sort is unacceptable. For example, a French based branch of a US company would be unable to transfer data about its employees to its US head office.

Penalties for non-compliance with the eight principle are strict and can lead to the offending party being de-registered. Any subsequent use by a company of personal data would result in the commission of a criminal offence.

B. 'Safe Harbor'

After much debate, a EU/US solution came in the form of a 'Safe Harbor' arrangement under the Clinton Administration.

However, since the introduction of the Safe Harbor arrangement in November 2000 and despite an expectation that many US companies would sign up to it, relatively few companies have done so. The Bush administration has expressed reservations about the arrangement.

Against this history, it remains to be seen whether the Safe Harbor arrangement plays any significant part in solving the problems of data transfer from Europe to the US.

Nevertheless, the Safe Harbor should be considered as is an option. It provides for the voluntary 'signing up' by companies in the US to adherence to a set of data protection principles which largely reflect those which apply in Europe. Companies can do this in a number of ways – they can, for example, develop their own policy which meets those standards or they can comply with existing US sector regulation which provides equivalent standards.

Those companies which are in the Safe Harbor will be deemed to provide adequate protection to personal data transferred from the EEA. This means that a company in the EEA can freely transfer data to Safe Harbor companies.

Once the US company has implemented the necessary standards, it must self-certify its compliance to the US Department of Commerce. Self-certified companies will be listed by the Department of Commerce on its website at www.export.gov/safeharbor. Companies which fail to self-certify annually will be removed from the Safe Harbor list. The overview pages from the Commerce Department website are attached under TAB 8, along with the EU Commission Decision of July 26, 2000 on the agreement.

C. Safe Harbor Principles

The Safe Harbor principles are as follows:

Notice

Organisations must notify individuals

- about the purposes for which their data has been collected;
- the use to which that information will be put;

- how the organisation can be contacted with any inquiries or complaints;
- the types of third parties to which it discloses information; and
- the choices and means the organisation offers for limiting the use and disclosure of data.

Choice/Opt Out

Organisations must give individuals choice (opt out) as to whether their personal data can be disclosed to a third party or used for a purpose which is incompatible with the purpose for which it was originally collected.

Further Transfer

If an organisation wishes to disclose information to a downstream third party, it must apply the notice and choice principles i.e. tell the individual what it wishes to do and give the individual the option to refuse.

Access To Data

Individuals must be permitted to access personal information held about them by an organisation. The individual also has the right to correct, amend or delete that information where it is inaccurate.

Data Security

Organisations must take reasonable precautions to protect personal information from loss, misuse, unauthorized access, disclosure etc.

Data Integrity

Personal information collected must be relevant for the purposes for which it is to be used. An organisation should also take reasonable steps to ensure that data is reliable for its intended use, accurate, complete and current.

Enforcement

In order to ensure compliance with the Safe Harbor principles, organisations must put in place a dispute resolution system to investigate individual complaints and disputes.

To provide further guidance, the Department of Commerce has issued a set of frequently asked questions and answers (FAQs) that clarify and supplement the SafeHarbor principles. These can be found at www.export.gov/safeharbor/SafeHarborDocuments.htm

Federal Trade Commission

Generally, the US policing function will be done by the Federal Trade Commission (FTC) which will be able to take action against companies for unfair trade practices under the Federal Trade Commission Act (FCTA) if companies fail to comply with their published privacy statements. The FTC has power to require an offending party to stop carrying out offending behavior.

The Safe Harbor arrangement does not extend to financial institutions or the telecommunications sector and other sectors not under the purview of the FTC.

Financial institutions for this purpose include banks, savings and loan institutions. The FTC does not have jurisdiction over financial services companies and cannot enforce any of the Safe Harbor principles. Financial institutions will have to rely on other acceptable procedures for transferring data as described below.

D. Alternatives to Safe Harbor

If the US importer of data does not sign up to the Safe Harbor, or if the Safe Harbor procedure is not available, there are alternative approaches which can be taken.

1. Consent

An exception allows the transfer of personal data outside the EEA if the individual who is the subject of that data consents to the transfer.

If the transfer is at the request of the individual, his/her consent can be implied. In other circumstances, the best way to get consent is to use a document which the individual normally returns (such as an order form) and provide a mechanism whereby the individual is told that their personal data may be transferred outside the EEA and given the opportunity to withhold their consent by clicking a box. Ultimately, however, the individual is completely within his/her rights to refuse to consent to his/her personal data being transferred to a country with inadequate data protection legislation. Without the benefit of a general exemption such as the SafeHarbor principle, a company therefore remains at risk of the withholding of consent by certain individuals.

2. Necessary for Contract Performance

Transfer of data outside the EEA is exempted if it is 'necessary for the performance of a contract' between the business and the individual. The ongoing question under this exception is whether the transfer can be said to be 'necessary'. 'Necessary' is likely to be narrowly construed and businesses should consider other justifications for transfer of data if they do not believe that the transfer can be said to be absolutely necessary for performance of the contract in question.

3. Contract

Where exceptions are not practical, EU-based companies can transfer data outside the EEA if they impose contractual obligations on entities to whom they transfer personal data.

These clauses are designed to assure adequate protection for the data. Key provisions are:

- the data importer must not disclose the data to any other entity (except where there is a legal or regulatory obligation);
- the data importer will give the individual rights of access, correction etc.;
- the data importer will respond to questions from the individuals.

Pursuant to Commission Decision of December 27, 2001 (under TAB 9), the European Commission has issued draft contract clauses which the EU would find as compliant with the Directive. These clauses have been widely criticised. Data importers are jointly liable with data exporters for damages arising from unlawful processing of data. These clauses are likely to set the standard for contractual obligations which need to be imposed on data importers outside the EEA by companies based in the EEA.

4. Adoption of a Compliance Policy

The option of adopting a data protection compliance policy is more suitable for use by a multinational company or group of companies. The policy should set standards for data protection which are required to be complied with by all in the multinational group. The standards (which should satisfy the EU requirement for adequate protection of data) will allow data to be freely transferred throughout the group. A 'master contract' may need to be entered into by the group of companies to ensure compliance with the policy.

Note, however, that a group compliance policy only addresses transfer of data within the group. Transfer of data to non-group companies may need to be handled by the contract clause option (if other data transfer options are not available).

E. Steps To Take

The prohibition on transfer of data outside the EEA applies as of October 24, 2001. To the extent not already done, the following steps would be in order:

- carry out an audit of the transfer of data practices of the business to determine whether data is transferred outside the EEA
- identify the countries to which data is transferred;
- if data is transferred to the US, consider having the importing companies signed up to Safe Harbor. If not, consider alternative compliance steps as outlined above. In many cases, the contract and compliance policy options will constitute appropriate solutions;
- if data is transferred outside the EEA but to countries other than the US, consider the compliance steps as outlined above. Remember that SafeHarbor is not an option. In many cases, the solution will be contractual and/or require the adoption of a compliance policy.

Companies should also keep abreast of which countries have been deemed by the EU to offer 'adequate protection'. This is likely to be a piecemeal by the European Commission going forward.

III. OVERALL CONSIDERATIONS

We have focused on just two issues with doing international business through cyberspace. This topic encompasses numerous additional issues that can only be touched upon as a checklist in deciding to open one's websites for international transactions. The following are some of these issues.

A. All Websites Are Global

All websites are global – because they can be accessed anywhere. But most websites are not truly global. Language, culture, distance, markets, logistics – all affect a commercial website's ability to transact business from outside the United States in a manner which is compliant with the host of local national legal requirements.

To market on the web requires recognition that one is operating in scores of markets. Without this mindset, a US website is simply a US site broadcast worldwide, without the real ability to reach global customers but can create a major non-compliance pitfall for the site owner.

Reaching a global market means adapting to language, culture, law, regulation and logistics that enable goods and services to be sold to customers in far-flung locations.

B. Sale Restrictions

Countries limit what can be sold to their residents. For example, in Germany, the price of books may not be discounted. Gambling is illegal in many areas, which affects give-aways and prize contests offered on the web. Charging interest can be illegal in Islamic countries. Websites cannot practically block particular browsers from seeing such content. An international website must be designed to limit the terms of any offer to areas where purchase is

valid, and this means a thorough legal research of each market intended to be opened by the website.

C. Consumer Protection

Local consumer protection laws protect in-country internet customers, and each country or state has its own regulations that may limit the terms of a sale. For example, requiring a consumer to arbitrate a dispute in a distant location may not be enforceable. A website operator should carefully review terms of sale to ensure that they respect consumer protection laws in any jurisdiction where an internet sale is intended to occur.

D. Content Restrictions

Local restrictions can arise in surprising ways. Yahoo was charged by the French Government with marketing Nazi memorabilia to French residents, something illegal in France. While it was impractical to block French users from having access to Yahoo auction sites, Yahoo worked out a solution with France that makes auctioned Nazi items unavailable to French residents. Advertising effective in one area may be totally inappropriate in another. Web marketers should seriously consider having separate URL's and sites for discrete market areas of the world. Through use of subdomains (e.g. de for Germany, fr for France), a company could have a website tailored specifically to particular national markets.

E. Product Regulation

The sale of one's US compatible product offshore may not be possible. The world is replete with country specific product and service codes/standards. Does the US domestic product/service meet those codes. Has the website marketer taken the cost of such compliance into consideration before opening its website for business. In many cases, a non-compliant product is subject to impoundment at the border. At a minimum there should be a disclaimer of

its fitness for any particular purpose the user may have in mind. If the item has health or safety issues associated with it, the website and order information should be clear about the limitations of its use. For any potentially dangerous product, safety warnings in the consumer's language should be included, again as is adequate under local law.

F. Export Control

All products are subject to some degree of export control under various US export control laws and regulations. The principal law is the Export Administration Act and its attendant regulations. Export controls address the type of product/service/technology and destination along with some general overarching restrictions regardless of product/technology type, such as the US embargo of Cuba. Accordingly, one needs to perform an audit of its products under the U.S. export control regime prior to offering these on any global or country specific website.

G. Terms of Use Agreement

The key to a good commercial website is a Terms of Use Agreement. This should state clearly the basis on which a purchaser of goods or services may do business with the site. There are four basic purposes of a Terms of Use Agreement.

1. The website can set conditions and restrictions on its relationship with a user.
2. The website can comply with the applicable local laws and regulations and manage potential liabilities to users.
3. The intellectual property of the website owner can be protected.
4. Confidence in the site's usage can be increased.

This can only be achieved if a Terms of Use Agreement is enforceable. The most effective way to enforce a Terms of Use Agreement is for it to be understandable and

affirmatively agreed by the user. Thus, for example as discussed above, "I agree" procedure required for European websites to obtain consent of users for use of personal data.

Internationally, relying on implied or tacit agreement to terms of use is very risky. In many countries an affirmative demonstration is needed of agreement to terms and conditions.

Taxation and domain name protection are further considerations when designing a truly global website. Careful consideration and planning is needed for a website operator to avoid unwanted tax exposure. Are you prepared to cope with the cost and infrastructure needed to comply with value added tax (VAT) systems prevalent throughout the world. Protecting domain names is essential, requiring a website operator to make sure that others are not pirating a brand or tradename by variations at a primary domain level or with subdomain URL's.

In general, in designing B2B, B2C websites for international business, all of the aspects of doing such business "on paper" need to be incorporated into the website design/operation, along with the additional issues of privacy, etc. that have come to the fore via growth of e-commerce.

LOUIMDMS/193084.1

10/2/2002 1:34 PM



UNITED NATIONS COMMISSION ON INTERNATIONAL TRADE LAW (UNCITRAL)

UNCITRAL Model Law on Electronic Commerce with Guide to Enactment

1996

with additional article 5 bis as adopted in 1998

CONTENTS

GENERAL ASSEMBLY RESOLUTION 51/162 OF 16 DECEMBER 1996 UNCITRAL MODEL LAW ON ELECTRONIC COMMERCE

Part one. Electronic commerce in general

Chapter I. General provisions

- Article 1. Sphere of application
- Article 2. Definitions
- Article 3. Interpretation
- Article 4. Variation by agreement

Chapter II. Application of legal requirements to data messages

- Article 5. Legal recognition of data messages
- Article 5 bis. Incorporation by reference
- Article 6. Writing
- Article 7. Signature
- Article 8. Original
- Article 9. Admissibility and evidential weight of data messages
- Article 10. Retention of data messages

Chapter III. Communication of data messages

- Article 11. Formation and validity of contracts
- Article 12. Recognition by parties of data messages
- Article 13. Attribution of data messages
- Article 14. Acknowledgement of receipt
- Article 15. Time and place of dispatch and receipt of data messages

Part two. Electronic commerce in specific areas

Chapter I. Carriage of goods

- Article 16. Actions related to contracts of carriage of goods
- Article 17. Transport documents

| | Paragraphs |
|--|-------------|
| GUIDE TO ENACTMENT OF THE UNCITRAL MODEL LAW ON ELECTRONIC COMMERCE | 1-150 |
| Purpose of this Guide | 1 |
| I. Introduction to the Model Law | 2-23 |
| A. Objectives | 2-6 |
| B. Scope | 7-10 |
| C. Structure | 11-12 |
| D. A "framework" law to be supplemented by technical regulations | 13-14 |
| E. The "functional-equivalent" approach | 15-18 |
| F. Default rules and mandatory law | 19-21 |
| G. Assistance from UNCITRAL secretariat | 22-23 |
| II. Article-by-article remarks | 24-122 |
| Part one. Electronic commerce in general | 24-107 |
| Chapter I. General provisions | 24-45 |
| Article 1. Sphere of application | 24-29 |
| Article 2. Definitions | 30-40 |
| Article 3. Interpretation | 41-43 |
| Article 4. Variation by agreement | 44-45 |
| Chapter II. Application of legal requirements to data messages | 46-75 |
| Article 5. Legal recognition of data messages | 46 |
| Article 5bis. Incorporation by reference | 46-1 - 46-7 |
| Article 6. Writing | 47-52 |

| | |
|---|---------|
| Article 7. Signature | 53-61 |
| Article 8. Original | 62-69 |
| Article 9. Admissibility and evidential weight of data messages | 70-71 |
| Article 10. Retention of data messages | 72-75 |
| Chapter III. Communication of data messages | 76-107 |
| Article 11. Formation and validity of contracts | 76-80 |
| Article 12. Recognition by parties of data messages | 81-82 |
| Article 13. Attribution of data messages | 83-92 |
| Article 14. Acknowledgement of receipt | 93-99 |
| Article 15. Time and place of dispatch and receipt of data messages | 100-107 |
| Part two. Electronic commerce in specific areas | 108-122 |
| Chapter I. Carriage of goods | 110-122 |
| Article 16. Actions related to contracts of carriage of goods | 111-112 |
| Article 17. Transport documents | 113-122 |
| III. History and background of the Model Law | 123-150 |

Resolution adopted by the General Assembly
[on the report of the Sixth Committee (A/51/628)]
51/162 Model Law on Electronic Commerce adopted by the United Nations Commission on
International Trade Law

The General Assembly,

Recalling its resolution 2205 (XXI) of 17 December 1966, by which it created the United Nations Commission on International Trade Law, with a mandate to further the progressive harmonization and unification of the law of international trade and in that respect to bear in mind the interests of all peoples, in particular those of developing countries, in the extensive development of international trade,

Noting that an increasing number of transactions in international trade are carried out by means of electronic data interchange and other means of communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information,

Recalling the recommendation on the legal value of computer records adopted by the Commission at

its eighteenth session, in 1985,⁽¹⁾ and paragraph 5(b) of General Assembly resolution 40/71 of 11 December 1985, in which the Assembly called upon Governments and international organizations to take action, where appropriate, in conformity with the recommendation of the Commission,⁽¹⁾ so as to ensure legal security in the context of the widest possible use of automated data processing in international trade,

Convinced that the establishment of a model law facilitating the use of electronic commerce that is acceptable to States with different legal, social and economic systems, could contribute significantly to the development of harmonious international economic relations,

Noting that the Model Law on Electronic Commerce was adopted by the Commission at its twenty-ninth session after consideration of the observations of Governments and interested organizations,

Believing that the adoption of the Model Law on Electronic Commerce by the Commission will assist all States significantly in enhancing their legislation governing the use of alternatives to paper-based methods of communication and storage of information and in formulating such legislation where none currently exists,

1. *Expresses* its appreciation to the United Nations Commission on International Trade Law for completing and adopting the Model Law on Electronic Commerce contained in the annex to the present resolution and for preparing the Guide to Enactment of the Model Law;
2. *Recommends* that all States give favourable consideration to the Model Law when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper-based methods of communication and storage of information;
3. *Recommends* also that all efforts be made to ensure that the Model Law, together with the Guide, become generally known and available.

85th plenary meeting
16 December 1996

UNCITRAL Model Law on Electronic Commerce

[Original: Arabic, Chinese, English, French, Russian, Spanish]

Part one. Electronic commerce in general

Chapter I. General provisions

Article 1. Sphere of application*

This Law** applies to any kind of information in the form of a data message used in the context*** of commercial**** activities.

* The Commission suggests the following text for States that might wish to limit the applicability of this Law to international data messages:

"This Law applies to a data message as defined in paragraph (1) of article 2 where the data message relates to international commerce."

** This Law does not override any rule of law intended for the protection of consumers.

**THE ELECTRONIC COMMERCE AND
INFORMATION, CONSUMER PROTECTION
AMENDMENT AND MANITOBA EVIDENCE
AMENDMENT ACT**

TABLE OF CONTENTS

**PART 1
GENERAL**

INTERPRETATION AND APPLICATION

- 1 Definitions
- 2 No application to negotiable instruments
- 3 No effect on laws re electronic means
- 4 Use of electronic documents not mandatory
- 5 Crown bound

**PRODUCTION, INSPECTION OR
CERTIFICATION OF
ELECTRONIC INFORMATION**

- 6 Production or inspection of electronic information
- 7 Certified copies of electronic information

**PART 2
USING ELECTRONIC MEANS
UNDER DESIGNATED LAWS**

GENERAL

- 8 Purpose
- 9 No effect on non-designated laws
- 10 General power to use electronic means

WRITING

- 11 Requirement for information to be in writing
- 12 Information required to be provided in writing

SIGNATURE

- 13 Requirement for signature

**LOI SUR LE COMMERCE ET
L'INFORMATION ÉLECTRONIQUES,
MODIFIANT LA LOI SUR LA PROTECTION
DU CONSOMMATEUR ET LA LOI SUR LA
PREUVE AU MANITOBA**

TABLE DES MATIÈRES

**PARTIE 1
DISPOSITIONS GÉNÉRALES**

DÉFINITIONS ET CHAMP D'APPLICATION

- 1 Définitions
- 2 Inapplication aux titres négociables
- 3 Effet sur les règles de droit
- 4 Emploi facultatif de documents électroniques
- 5 Obligation de la Couronne

**PRODUCTION, INSPECTION OU ATTESTATION
DE L'INFORMATION ÉLECTRONIQUE**

- 6 Production ou inspection de l'information électronique
- 7 Copies certifiées conformes de l'information électronique

**PARTIE 2
EMPLOI DE MOYENS ÉLECTRONIQUES
SOUS LE RÉGIME DE LOIS DÉSIGNÉES**

DISPOSITIONS GÉNÉRALES

- 8 But
- 9 Absence d'effet sur les lois non désignées
- 10 Pouvoir général d'emploi de moyens électroniques

RENSEIGNEMENTS ÉCRITS

- 11 Obligation de mettre les renseignements par écrit
- 12 Renseignements devant être fournis par écrit

SIGNATURE

- 13 Exigence relative à la signature

ORIGINAL DOCUMENTS

- 14 Requirement re originals

RETAINING DOCUMENTS

- 15 Requirement to retain information or documents

ADDITIONAL COPIES

- 16 Additional copies not required

REGULATIONS AND APPROVALS

- 17 Power to prescribe or approve electronic form
18 Regulations

**PART 3
ELECTRONIC CONTRACTS
AND COMMUNICATIONS**

- 19 Formation and operation of contracts
20 Electronic agents
21 Time and place of sending or receiving

**PART 4
CONTRACTS FOR CARRIAGE OF GOODS**

- 22 Actions related to contracts of carriage of goods
23 Use of electronic means

**PART 5
STREAMLINED PROCEDURES
FOR BUSINESS ENTITIES**

- 24 Definitions
25 Purposes
26 Common business identifiers
27 Combined forms
28 Integration of business information systems
29 Disclosure of information
30 Regulations
31 Agreements with governmental or other bodies

DOCUMENTS ORIGINAUX

- 14 Exigence relative aux documents originaux

CONSERVATION DES DOCUMENTS

- 15 Exigence relative à la conservation des renseignements ou des documents

COPIES SUPPLÉMENTAIRES

- 16 Copies supplémentaires non obligatoires

RÈGLEMENTS ET APPROBATIONS

- 17 Pouvoir de prescrire ou d'approuver la forme électronique
18 Règlements

**PARTIE 3
CONTRATS ET COMMUNICATIONS
ÉLECTRONIQUES**

- 19 Conclusion et exécution des contrats
20 Agents électroniques
21 Moment et lieu d'expédition ou de réception

**PARTIE 4
CONTRATS DE TRANSPORT DE
MARCHANDISES**

- 22 Actes ayant trait aux contrats de transport de marchandises
23 Emploi de moyens électroniques

**PARTIE 5
RATIONALISATION DES MÉTHODES
POUR LES ENTREPRISES**

- 24 Définitions
25 Objet
26 Identificateurs communs
27 Formules combinées
28 Intégration des systèmes d'information
29 Divulgence de renseignements
30 Règlements
31 Conventions — organismes gouvernementaux ou autres

**PART 6
AMENDMENTS TO
THE CONSUMER PROTECTION ACT**

32 - 36 C.C.S.M. c. C200 amended

**PART 7
AMENDMENTS TO
THE MANITOBA EVIDENCE ACT**

37 - 38 C.C.S.M. c. E150 amended

**PART 8
CITATION AND
COMING INTO FORCE**

39 C.C.S.M. reference
40 Coming into force

**PARTIE 6
MODIFICATIONS À LA LOI SUR LA
PROTECTION DU CONSOMMATEUR**

32-36 Modification du c. C200 de la *C.P.L.M.*

**PARTIE 7
MODIFICATIONS À LA
LOI SUR LA PREUVE AU MANITOBA**

37-38 Modification du c. E150 de la *C.P.L.M.*

**PARTIE 8
TITRE ET ENTRÉE EN VIGUEUR**

39 *Codification permanente*
40 *Entrée en vigueur*

EXPLANATORY NOTE

This Bill provides a set of rules designed to give legal recognition to electronic documents and communications.

Part 1 contains definitions and application rules. It also contains rules to enable a person to satisfy a legal requirement to produce for inspection, or provide a certified copy of, a document that happens to be in electronic form.

Part 2 enables, but does not require, the use of electronic means to comply with a number of other legal requirements under designated laws, such as a requirement to provide information in writing or in a specified form or a requirement for a signature. By designating laws for the purpose of this Part, the government will be able to facilitate and regulate electronic filing.

Part 3 gives legal recognition to contracts that are formed using one or more electronic documents. It provides a limited right to cancel a contract when a person makes a mistake in dealing with an electronic agent of another person. It also contains rules for establishing the time and place of sending and receiving electronic documents in connection with contracts.

Part 4 makes special provision for contracts relating to the carriage of goods, to permit the use of electronic documents in a field that has traditionally depended on unique paper documents.

Part 5 allows regulatory requirements applicable to business entities to be streamlined by providing for the use of common business identifiers, combined forms, integrated information systems and integrated filing and payment procedures.

Part 6 amends *The Consumer Protection Act*

- by limiting a consumer's liability when credit card information is lost or stolen;
- by giving consumers certain cancellation rights relating to Internet purchases; and
- by requiring a credit card issuer to reverse a credit card charge for an Internet purchase if the vendor fails to provide a refund after a consumer has exercised such a cancellation right.

Part 7 makes amendments to the *The Manitoba Evidence Act* that parallel recent amendments to the *Canada Evidence Act*. They deal with the admissibility of electronic documents and establish evidentiary presumptions about electronic signatures and the integrity of electronic documents.

NOTE EXPLICATIVE

Le présent projet de loi établit un jeu de règles visant à donner une reconnaissance juridique aux documents et aux communications électroniques.

La partie 1 contient les définitions et les règles d'application. Elle contient également des règles permettant de satisfaire à l'exigence juridique de produire, pour examen, un document qui se trouve dans une forme électronique ou d'en fournir une copie certifiée conforme.

La partie 2 permet, mais n'exige pas, l'emploi de moyens électroniques pour satisfaire à un certain nombre d'autres exigences juridiques que prévoient des lois désignées, comme l'exigence de fournir des renseignements par écrit ou dans une forme précisée ou l'exigence relative à la signature. En désignant des lois pour l'application de cette partie, le gouvernement sera en mesure de faciliter et de réglementer le dépôt électronique.

La partie 3 donne une reconnaissance juridique aux contrats conclus au moyen d'au moins un document électronique. Elle prévoit un droit limité d'annuler un contrat en cas d'erreur dans les négociations avec l'agent électronique de quelqu'un d'autre. Elle comporte également des règles visant la détermination de l'heure et du lieu d'expédition et de réception de documents électroniques en rapport avec des contrats.

La partie 4 établit des dispositions spéciales pour les contrats de transport de marchandises, dispositions qui visent à permettre l'emploi de documents électroniques dans un domaine qui ne recourait jusqu'à maintenant qu'à des documents papier.

La partie 5 permet de rationaliser les exigences réglementaires applicables aux entreprises par l'établissement de dispositions prévoyant l'emploi d'identificateurs communs, de formules combinées, de systèmes d'information intégrés et de méthodes intégrées de dépôt et de paiement.

La partie 6 modifie la *Loi sur la protection du consommateur* :

- en limitant la responsabilité des consommateurs en cas de perte ou de vol de leur carte de crédit;
- en leur donnant certains droits d'annulation relativement aux achats par Internet;
- en obligeant les émetteurs de cartes de crédit à annuler les frais des achats faits par Internet dans les cas où les vendeurs ne remboursent pas les consommateurs qui ont exercé un tel droit d'annulation.

La partie 7 apporte des modifications à la *Loi sur la preuve au Manitoba*, modifications qui calquent celles apportées récemment à la *Loi sur la preuve au Canada*. Ces modifications portent sur l'admissibilité en preuve des documents électroniques et établissent des présomptions de

DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 13 December 1999
on a Community framework for electronic signatures

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Articles 47(2), 55 and 95 thereof,

Having regard to the proposal from the Commission ⁽¹⁾,

Having regard to the opinion of the Economic and Social Committee ⁽²⁾,

Having regard to the opinion of the Committee of the Regions ⁽³⁾,

Acting in accordance with the procedure laid down in Article 251 of the Treaty ⁽⁴⁾,

Whereas:

- (1) On 16 April 1997 the Commission presented to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions a Communication on a European Initiative in Electronic Commerce;
- (2) On 8 October 1997 the Commission presented to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions a Communication on ensuring security and trust in electronic communication — towards a European framework for digital signatures and encryption;
- (3) On 1 December 1997 the Council invited the Commission to submit as soon as possible a proposal for a Directive of the European Parliament and of the Council on digital signatures;
- (4) Electronic communication and commerce necessitate 'electronic signatures' and related services allowing data authentication; divergent rules with respect to legal recognition of electronic signatures and the accreditation of certification-service providers in the Member States may create a significant barrier to the use of electronic communications and electronic commerce; on the other hand, a clear Community framework regarding the conditions applying to electronic signatures will strengthen confidence in, and general acceptance of, the new technologies; legislation in the Member States should not hinder the free movement of goods and services in the internal market;
- (5) The interoperability of electronic-signature products should be promoted; in accordance with Article 14 of the Treaty, the internal market comprises an area without internal frontiers in which the free movement of goods is ensured; essential requirements specific to electronic-signature products must be met in order to ensure free movement within the internal market and to build trust in electronic signatures, without prejudice to Council Regulation (EC) No 3381/94 of 19 December 1994 setting up a Community regime for the control of exports of dual-use goods ⁽⁵⁾ and Council Decision 94/942/CFSP of 19 December 1994 on the joint action adopted by the Council concerning the control of exports of dual-use goods ⁽⁶⁾;
- (6) This Directive does not harmonise the provision of services with respect to the confidentiality of information where they are covered by national provisions concerned with public policy or public security;
- (7) The internal market ensures the free movement of persons, as a result of which citizens and residents of the European Union increasingly need to deal with authorities in Member States other than the one in which they reside; the availability of electronic communication could be of great service in this respect;
- (8) Rapid technological development and the global character of the Internet necessitate an approach which is open to various technologies and services capable of authenticating data electronically;
- (9) Electronic signatures will be used in a large variety of circumstances and applications, resulting in a wide range of new services and products related to or using electronic signatures; the definition of such products and services should not be limited to the issuance and management of certificates, but should also encompass any other service and product using, or ancillary to, electronic signatures, such as registration services, time-stamping services, directory services, computing services or consultancy services related to electronic signatures;
- (10) The internal market enables certification-service-providers to develop their cross-border activities with a view to increasing their competitiveness, and thus to offer consumers and businesses new opportunities to exchange information and trade electronically in a secure way, regardless of frontiers; in order to stimulate the Community-wide provision of certification services over open networks, certification-service-providers should be free to provide their services without prior authorisation; prior authorisation means not only any

⁽¹⁾ OJ C 325, 23.10.1998, p. 5.

⁽²⁾ OJ C 40, 15.2.1999, p. 29.

⁽³⁾ OJ C 93, 6.4.1999, p. 33.

⁽⁴⁾ Opinion of the European Parliament of 13 January 1999 (OJ C 104, 14.4.1999, p. 49), Council Common Position of 28 June 1999 (OJ C 243, 27.8.1999, p. 33) and Decision of the European Parliament of 27 October 1999 (not yet published in the Official Journal), Council Decision of 30 November 1999.

⁽⁵⁾ OJ L 367, 31.12.1994, p. 1. Regulation as amended by Regulation (EC) No 837/95 (OJ L 90, 21.4.1995, p. 1).

⁽⁶⁾ OJ L 367, 31.12.1994, p. 8. Decision as last amended by Decision 99/193/CFSP (OJ L 73, 19.3.1999, p. 1).

- permission whereby the certification-service-provider concerned has to obtain a decision by national authorities before being allowed to provide its certification services, but also any other measures having the same effect;
- (11) Voluntary accreditation schemes aiming at an enhanced level of service-provision may offer certification-service-providers the appropriate framework for developing further their services towards the levels of trust, security and quality demanded by the evolving market; such schemes should encourage the development of best practice among certification-service-providers; certification-service-providers should be left free to adhere to and benefit from such accreditation schemes;
- (12) Certification services can be offered either by a public entity or a legal or natural person, when it is established in accordance with the national law; whereas Member States should not prohibit certification-service-providers from operating outside voluntary accreditation schemes; it should be ensured that such accreditation schemes do not reduce competition for certification services;
- (13) Member States may decide how they ensure the supervision of compliance with the provisions laid down in this Directive; this Directive does not preclude the establishment of private-sector-based supervision systems; this Directive does not oblige certification-service-providers to apply to be supervised under any applicable accreditation scheme;
- (14) It is important to strike a balance between consumer and business needs;
- (15) Annex III covers requirements for secure signature-creation devices to ensure the functionality of advanced electronic signatures; it does not cover the entire system environment in which such devices operate; the functioning of the internal market requires the Commission and the Member States to act swiftly to enable the bodies charged with the conformity assessment of secure signature devices with Annex III to be designated; in order to meet market needs conformity assessment must be timely and efficient;
- (16) This Directive contributes to the use and legal recognition of electronic signatures within the Community; a regulatory framework is not needed for electronic signatures exclusively used within systems, which are based on voluntary agreements under private law between a specified number of participants; the freedom of parties to agree among themselves the terms and conditions under which they accept electronically signed data should be respected to the extent allowed by national law; the legal effectiveness of electronic signatures used in such systems and their admissibility as evidence in legal proceedings should be recognised;
- (17) This Directive does not seek to harmonise national rules concerning contract law, particularly the formation and performance of contracts, or other formalities of a non-contractual nature concerning signatures; for this reason the provisions concerning the legal effect of electronic signatures should be without prejudice to requirements regarding form laid down in national law with regard to the conclusion of contracts or the rules determining where a contract is concluded;
- (18) The storage and copying of signature-creation data could cause a threat to the legal validity of electronic signatures;
- (19) Electronic signatures will be used in the public sector within national and Community administrations and in communications between such administrations and with citizens and economic operators, for example in the public procurement, taxation, social security, health and justice systems;
- (20) Harmonised criteria relating to the legal effects of electronic signatures will preserve a coherent legal framework across the Community; national law lays down different requirements for the legal validity of handwritten signatures; whereas certificates can be used to confirm the identity of a person signing electronically; advanced electronic signatures based on qualified certificates aim at a higher level of security; advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device can be regarded as legally equivalent to handwritten signatures only if the requirements for handwritten signatures are fulfilled;
- (21) In order to contribute to the general acceptance of electronic authentication methods it has to be ensured that electronic signatures can be used as evidence in legal proceedings in all Member States; the legal recognition of electronic signatures should be based upon objective criteria and not be linked to authorisation of the certification-service-provider involved; national law governs the legal spheres in which electronic documents and electronic signatures may be used; this Directive is without prejudice to the power of a national court to make a ruling regarding conformity with the requirements of this Directive and does not affect national rules regarding the unfettered judicial consideration of evidence;
- (22) Certification-service-providers providing certification-services to the public are subject to national rules regarding liability;
- (23) The development of international electronic commerce requires cross-border arrangements involving third countries; in order to ensure interoperability at a global level, agreements on multilateral rules with third countries on mutual recognition of certification services could be beneficial;

- (24) In order to increase user confidence in electronic communication and electronic commerce, certification-service-providers must observe data protection legislation and individual privacy;
- (25) Provisions on the use of pseudonyms in certificates should not prevent Member States from requiring identification of persons pursuant to Community or national law;
- (26) The measures necessary for the implementation of this Directive are to be adopted in accordance with Council Decision 1999/468/EC of 28 June 1999 laying down the procedures for the exercise of implementing powers conferred on the Commission ⁽¹⁾;
- (27) Two years after its implementation the Commission will carry out a review of this Directive so as, *inter alia*, to ensure that the advance of technology or changes in the legal environment have not created barriers to achieving the aims stated in this Directive; it should examine the implications of associated technical areas and submit a report to the European Parliament and the Council on this subject;
- (28) In accordance with the principles of subsidiarity and proportionality as set out in Article 5 of the Treaty, the objective of creating a harmonised legal framework for the provision of electronic signatures and related services cannot be sufficiently achieved by the Member States and can therefore be better achieved by the Community; this Directive does not go beyond what is necessary to achieve that objective,
2. 'advanced electronic signature' means an electronic signature which meets the following requirements:
- it is uniquely linked to the signatory;
 - it is capable of identifying the signatory;
 - it is created using means that the signatory can maintain under his sole control; and
 - it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;
3. 'signatory' means a person who holds a signature-creation device and acts either on his own behalf or on behalf of the natural or legal person or entity he represents;
4. 'signature-creation data' means unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature;
5. 'signature-creation device' means configured software or hardware used to implement the signature-creation data;
6. 'secure-signature-creation device' means a signature-creation device which meets the requirements laid down in Annex III;
7. 'signature-verification-data' means data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature;
8. 'signature-verification device' means configured software or hardware used to implement the signature-verification-data;
9. 'certificate' means an electronic attestation which links signature-verification data to a person and confirms the identity of that person;
10. 'qualified certificate' means a certificate which meets the requirements laid down in Annex I and is provided by a certification-service-provider who fulfils the requirements laid down in Annex II;
11. 'certification-service-provider' means an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures;
12. 'electronic-signature product' means hardware or software, or relevant components thereof, which are intended to be used by a certification-service-provider for the provision of electronic-signature services or are intended to be used for the creation or verification of electronic signatures;
13. 'voluntary accreditation' means any permission, setting out rights and obligations specific to the provision of certification services, to be granted upon request by the certification-service-provider concerned, by the public or private body charged with the elaboration of, and supervision of compliance with, such rights and obligations, where the certification-service-provider is not entitled to exercise the rights stemming from the permission until it has received the decision by the body.

HAVE ADOPTED THIS DIRECTIVE:

Article 1

Scope

The purpose of this Directive is to facilitate the use of electronic signatures and to contribute to their legal recognition. It establishes a legal framework for electronic signatures and certain certification-services in order to ensure the proper functioning of the internal market.

It does not cover aspects related to the conclusion and validity of contracts or other legal obligations where there are requirements as regards form prescribed by national or Community law nor does it affect rules and limits, contained in national or Community law, governing the use of documents.

Article 2

Definitions

For the purpose of this Directive:

- 'electronic signature' means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication;

⁽¹⁾ OJ L 184, 17.7.1999, p. 23.

Article 3

Market access

1. Member States shall not make the provision of certification services subject to prior authorisation.
2. Without prejudice to the provisions of paragraph 1, Member States may introduce or maintain voluntary accreditation schemes aiming at enhanced levels of certification-service provision. All conditions related to such schemes must be objective, transparent, proportionate and non-discriminatory. Member States may not limit the number of accredited certification-service-providers for reasons which fall within the scope of this Directive.
3. Each Member State shall ensure the establishment of an appropriate system that allows for supervision of certification-service-providers which are established on its territory and issue qualified certificates to the public.
4. The conformity of secure signature-creation-devices with the requirements laid down in Annex III shall be determined by appropriate public or private bodies designated by Member States. The Commission shall, pursuant to the procedure laid down in Article 9, establish criteria for Member States to determine whether a body should be designated.

A determination of conformity with the requirements laid down in Annex III made by the bodies referred to in the first subparagraph shall be recognised by all Member States.

5. The Commission may, in accordance with the procedure laid down in Article 9, establish and publish reference numbers of generally recognised standards for electronic-signature products in the *Official Journal of the European Communities*. Member States shall presume that there is compliance with the requirements laid down in Annex II, point (f), and Annex III when an electronic signature product meets those standards.
6. Member States and the Commission shall work together to promote the development and use of signature-verification devices in the light of the recommendations for secure signature-verification laid down in Annex IV and in the interests of the consumer.
7. Member States may make the use of electronic signatures in the public sector subject to possible additional requirements. Such requirements shall be objective, transparent, proportionate and non-discriminatory and shall relate only to the specific characteristics of the application concerned. Such requirements may not constitute an obstacle to cross-border services for citizens.

Article 4

Internal market principles

1. Each Member State shall apply the national provisions which it adopts pursuant to this Directive to certification-service-providers established on its territory and to the services

which they provide. Member States may not restrict the provision of certification-services originating in another Member State in the fields covered by this Directive.

2. Member States shall ensure that electronic-signature products which comply with this Directive are permitted to circulate freely in the internal market.

Article 5

Legal effects of electronic signatures

1. Member States shall ensure that advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device:
 - (a) satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data; and
 - (b) are admissible as evidence in legal proceedings.
2. Member States shall ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is:
 - in electronic form, or
 - not based upon a qualified certificate, or
 - not based upon a qualified certificate issued by an accredited certification-service-provider, or
 - not created by a secure signature-creation device.

Article 6

Liability

1. As a minimum, Member States shall ensure that by issuing a certificate as a qualified certificate to the public or by guaranteeing such a certificate to the public a certification-service-provider is liable for damage caused to any entity or legal or natural person who reasonably relies on that certificate:
 - (a) as regards the accuracy at the time of issuance of all information contained in the qualified certificate and as regards the fact that the certificate contains all the details prescribed for a qualified certificate;
 - (b) for assurance that at the time of the issuance of the certificate, the signatory identified in the qualified certificate held the signature-creation data corresponding to the signature-verification data given or identified in the certificate;
 - (c) for assurance that the signature-creation data and the signature-verification data can be used in a complementary manner in cases where the certification-service-provider generates them both;

unless the certification-service-provider proves that he has not acted negligently.

2. As a minimum Member States shall ensure that a certification-service-provider who has issued a certificate as a qualified certificate to the public is liable for damage caused to any entity or legal or natural person who reasonably relies on the certificate for failure to register revocation of the certificate unless the certification-service-provider proves that he has not acted negligently.

3. Member States shall ensure that a certification-service-provider may indicate in a qualified certificate limitations on the use of that certificate, provided that the limitations are recognisable to third parties. The certification-service-provider shall not be liable for damage arising from use of a qualified certificate which exceeds the limitations placed on it.

4. Member States shall ensure that a certification-service-provider may indicate in the qualified certificate a limit on the value of transactions for which the certificate can be used, provided that the limit is recognisable to third parties.

The certification-service-provider shall not be liable for damage resulting from this maximum limit being exceeded.

5. The provisions of paragraphs 1 to 4 shall be without prejudice to Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts⁽¹⁾.

Article 7

International aspects

1. Member States shall ensure that certificates which are issued as qualified certificates to the public by a certification-service-provider established in a third country are recognised as legally equivalent to certificates issued by a certification-service-provider established within the Community if:

- (a) the certification-service-provider fulfils the requirements laid down in this Directive and has been accredited under a voluntary accreditation scheme established in a Member State; or
- (b) a certification-service-provider established within the Community which fulfils the requirements laid down in this Directive guarantees the certificate; or
- (c) the certificate or the certification-service-provider is recognised under a bilateral or multilateral agreement between the Community and third countries or international organisations.

2. In order to facilitate cross-border certification services with third countries and legal recognition of advanced electronic signatures originating in third countries, the Commission shall make proposals, where appropriate, to achieve the effective implementation of standards and international agreements applicable to certification services. In particular, and where necessary, it shall submit proposals to the Council for appropriate mandates for the negotiation of bilateral and multilateral agreements with third countries and international organisations. The Council shall decide by qualified majority.

⁽¹⁾ OJ L 95, 21.4.1993, p. 29.

3. Whenever the Commission is informed of any difficulties encountered by Community undertakings with respect to market access in third countries, it may, if necessary, submit proposals to the Council for an appropriate mandate for the negotiation of comparable rights for Community undertakings in these third countries. The Council shall decide by qualified majority.

Measures taken pursuant to this paragraph shall be without prejudice to the obligations of the Community and of the Member States under relevant international agreements.

Article 8

Data protection

1. Member States shall ensure that certification-service-providers and national bodies responsible for accreditation or supervision comply with the requirements laid down in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data⁽²⁾.

2. Member States shall ensure that a certification-service-provider which issues certificates to the public may collect personal data only directly from the data subject, or after the explicit consent of the data subject, and only insofar as it is necessary for the purposes of issuing and maintaining the certificate. The data may not be collected or processed for any other purposes without the explicit consent of the data subject.

3. Without prejudice to the legal effect given to pseudonyms under national law, Member States shall not prevent certification service providers from indicating in the certificate a pseudonym instead of the signatory's name.

Article 9

Committee

1. The Commission shall be assisted by an 'Electronic-Signature Committee', hereinafter referred to as 'the committee'.

2. Where reference is made to this paragraph, Articles 4 and 7 of Decision 1999/468/EC shall apply, having regard to the provisions of Article 8 thereof.

The period laid down in Article 4(3) of Decision 1999/468/EC shall be set at three months.

3. The Committee shall adopt its own rules of procedure.

Article 10

Tasks of the committee

The committee shall clarify the requirements laid down in the Annexes of this Directive, the criteria referred to in Article 3(4) and the generally recognised standards for electronic signature products established and published pursuant to Article 3(5), in accordance with the procedure laid down in Article 9(2).

⁽²⁾ OJ L 281, 23.11.1995, p. 31.

*Article 11***Notification**

1. Member States shall notify to the Commission and the other Member States the following:

- (a) information on national voluntary accreditation schemes, including any additional requirements pursuant to Article 3(7);
- (b) the names and addresses of the national bodies responsible for accreditation and supervision as well as of the bodies referred to in Article 3(4);
- (c) the names and addresses of all accredited national certification service providers.

2. Any information supplied under paragraph 1 and changes in respect of that information shall be notified by the Member States as soon as possible.

*Article 12***Review**

1. The Commission shall review the operation of this Directive and report thereon to the European Parliament and to the Council by 19 July 2003 at the latest.

2. The review shall inter alia assess whether the scope of this Directive should be modified, taking account of technological, market and legal developments. The report shall in particular include an assessment, on the basis of experience gained, of aspects of harmonisation. The report shall be accompanied, where appropriate, by legislative proposals.

*Article 13***Implementation**

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive before 19 July 2001. They shall forthwith inform the Commission thereof.

When Member States adopt these measures, they shall contain a reference to this Directive or shall be accompanied by such a reference on the occasion of their official publication. The methods of making such reference shall be laid down by the Member States.

2. Member States shall communicate to the Commission the text of the main provisions of domestic law which they adopt in the field governed by this Directive.

*Article 14***Entry into force**

This Directive shall enter into force on the day of its publication in the *Official Journal of the European Communities*

*Article 15***Addressees**

This Directive is addressed to the Member States.

Done at Brussels, 13 December 1999.

For the European Parliament
The President
N. FONTAINE

For the Council
The President
S. HASSI

ANNEX I

Requirements for qualified certificates

Qualified certificates must contain:

- (a) an indication that the certificate is issued as a qualified certificate;
 - (b) the identification of the certification-service-provider and the State in which it is established;
 - (c) the name of the signatory or a pseudonym, which shall be identified as such;
 - (d) provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended;
 - (e) signature-verification data which correspond to signature-creation data under the control of the signatory;
 - (f) an indication of the beginning and end of the period of validity of the certificate;
 - (g) the identity code of the certificate;
 - (h) the advanced electronic signature of the certification-service-provider issuing it;
 - (i) limitations on the scope of use of the certificate, if applicable; and
 - (j) limits on the value of transactions for which the certificate can be used, if applicable.
-

ANNEX II

Requirements for certification-service-providers issuing qualified certificates

Certification-service-providers must:

- (a) demonstrate the reliability necessary for providing certification services;
- (b) ensure the operation of a prompt and secure directory and a secure and immediate revocation service;
- (c) ensure that the date and time when a certificate is issued or revoked can be determined precisely;
- (d) verify, by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a qualified certificate is issued;
- (e) employ personnel who possess the expert knowledge, experience, and qualifications necessary for the services provided, in particular competence at managerial level, expertise in electronic signature technology and familiarity with proper security procedures; they must also apply administrative and management procedures which are adequate and correspond to recognised standards;
- (f) use trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the process supported by them;
- (g) take measures against forgery of certificates, and, in cases where the certification-service-provider generates signature-creation data, guarantee confidentiality during the process of generating such data;
- (h) maintain sufficient financial resources to operate in conformity with the requirements laid down in the Directive, in particular to bear the risk of liability for damages, for example, by obtaining appropriate insurance;
- (i) record all relevant information concerning a qualified certificate for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings. Such recording may be done electronically;
- (j) not store or copy signature-creation data of the person to whom the certification-service-provider provided key management services;
- (k) before entering into a contractual relationship with a person seeking a certificate to support his electronic signature inform that person by a durable means of communication of the precise terms and conditions regarding the use of the certificate, including any limitations on its use, the existence of a voluntary accreditation scheme and procedures for complaints and dispute settlement. Such information, which may be transmitted electronically, must be in writing and in readily understandable language. Relevant parts of this information must also be made available on request to third-parties relying on the certificate;
- (l) use trustworthy systems to store certificates in a verifiable form so that:
 - only authorised persons can make entries and changes,
 - information can be checked for authenticity,
 - certificates are publicly available for retrieval in only those cases for which the certificate-holder's consent has been obtained, and
 - any technical changes compromising these security requirements are apparent to the operator.

ANNEX III**Requirements for secure signature-creation devices**

1. Secure signature-creation devices must, by appropriate technical and procedural means, ensure at the least that:
 - (a) the signature-creation-data used for signature generation can practically occur only once, and that their secrecy is reasonably assured;
 - (b) the signature-creation-data used for signature generation cannot, with reasonable assurance, be derived and the signature is protected against forgery using currently available technology;
 - (c) the signature-creation-data used for signature generation can be reliably protected by the legitimate signatory against the use of others.
2. Secure signature-creation devices must not alter the data to be signed or prevent such data from being presented to the signatory prior to the signature process.

ANNEX IV**Recommendations for secure signature verification**

During the signature-verification process it should be ensured with reasonable certainty that:

- (a) the data used for verifying the signature correspond to the data displayed to the verifier;
 - (b) the signature is reliably verified and the result of that verification is correctly displayed;
 - (c) the verifier can, as necessary, reliably establish the contents of the signed data;
 - (d) the authenticity and validity of the certificate required at the time of signature verification are reliably verified;
 - (e) the result of verification and the signatory's identity are correctly displayed;
 - (f) the use of a pseudonym is clearly indicated; and
 - (g) any security-relevant changes can be detected.
-

Draft
of a Law on the Framework Conditions
for Electronic Signatures
and to Amend Other Regulations
(in the version decided by the Cabinet on 16 August 2000)

PASSED FEB. 15, 2001

The German Parliament has decided the following legislation:

Article 1

Law on Framework Conditions for Electronic Signatures (Signatures Law - SigG) ¹

Contents

Section One: General Regulations

- § 1 Purpose and Area of Application
- § 2 Definition of Terms
- § 3 Competent Authority

Section Two: Certification-Service Providers

- § 4 General Requirements
- § 5 Issue of Qualified Certificates
- § 6 Obligation to Provide Information
- § 7 Contents of Qualified Certificates
- § 8 Invalidating Qualified Certificates
- § 9 Qualified Time Stamps
- § 10 Documentation
- § 11 Liability
- § 12 Cover
- § 13 Cessation of Operations
- § 14 Data Protection

Section Three: Voluntary Accreditation

¹ The obligation to provide information under Directive 98/34/EC of the European Parliament and the Council of 22 June 1998 on an information procedure in the field of norms and technical requirements (OJ EC No. L 204, p. 37 of 21 July 1998), last amended by Directive 98/48/EC of the European Parliament and the Council of 20 July 1998 (OJ EC No. L 217, p. 18 of 5 August 1998) and the obligation to provide information under

§ 15 Voluntary Accreditation of Certification-Service Providers

§ 16 Certificates from the Competent Authority

Section Four: Technical Security

§ 17 Products for Electronic Signatures

§ 18 Recognition of Testing and Confirmation Offices

Section Five: Supervision

§ 19 Supervision Measures

§ 20 Obligatory Cooperation

Section Six: Final Regulations

§ 21 Fines

§ 22 Costs and Contributions

§ 23 Foreign Electronic Signatures and Products for Electronic Signatures

§ 24 Legal Regulations

§ 25 Transitional Regulations

Directive 1999/93/EC of the European Parliament and the Council of 13 December 1999 on Community framework conditions for electronic signatures (OJ EC 2000 No. L 13, p. 2) have been observed.

Statutory Instrument 2002 No. 318

The Electronic Signatures Regulations 2002

© Crown Copyright 2002

The legislation contained on this web site is subject to Crown Copyright protection. It may be reproduced free of charge provided that it is reproduced accurately and that the source and copyright status of the material is made evident to users.

It should be noted that the right to reproduce the text of Statutory Instruments does not extend to the Royal Arms and the Queen's Printer imprints.

The text of this Internet version of the Statutory Instrument has been prepared to reflect the text as it was Made. The authoritative version is the Queen's Printer copy published by The Stationery Office Limited as the **The Electronic Signatures Regulations 2002**, ISBN 0 11 039401 1. Purchase this item. For details of how to obtain an official copy see How to obtain The Stationery Office Limited titles.

To ensure fast access over slow connections, large documents have been segmented into "chunks". Where you see a "continue" button at the bottom of the page of text, this indicates that there is another chunk of text available.

STATUTORY INSTRUMENTS

2002 No. 318

ELECTRONIC COMMUNICATIONS

The Electronic Signatures Regulations 2002

| | |
|-------------------------------|---------------------------|
| <i>Made</i> | <i>13th February 2002</i> |
| <i>Laid before Parliament</i> | <i>14th February 2002</i> |
| <i>Coming into force</i> | <i>8th March 2002</i> |

The Secretary of State, being designated^[1] for the purpose of section 2(2) of the European Communities Act 1972^[2] in relation to electronic signatures, in exercise of the powers conferred on her by the said section 2(2), hereby makes the following Regulations:

Citation and commencement

1. These Regulations may be cited as the Electronic Signatures Regulations 2002 and shall come into force on 8th March 2002.

Law Concerning Electronic Signatures and Certification Services (Unofficial Translation)

Contents

- Chapter 1: General provisions (Article 1 and Article 2)
- Chapter 2: Presumption of the authenticity of an electro-magnetic records (Article 3)
- Chapter 3: Accreditation, etc. of designated certification services
 - Section 1: Accreditation of designated certification services (Article 4 through Article 14)
 - Section 2: Accreditation of designated certification services provided in foreign countries (Article 15 and Article 16)
- Chapter 4: Designated investigating organization, etc.
 - Section 1: Designated investigating organization (Article 17 through Article 30)
 - Section 2: Approved investigating organization (Article 31 and Article 32)
- Chapter 5: Miscellaneous provisions (Article 33 through Article 40)
- Chapter 6: Penalties (Article 41 through Article 47)
- Supplemental provisions

Chapter 1: General provisions

Article 1 Purpose

This law aims to promote the diffusion of information using electronic methods and information processing through securing the smooth utilization of electronic signatures, and thereby to contribute to the improvement of the citizen's quality of life and the sound development of the national economy, by establishing such provisions as the presumption of the authenticity of electro-magnetic records, the provisions for accreditation with regard to designated certification services and the prescription of other necessary matters concerning electronic signatures.

Article 2 Definitions

For the purpose of this law, "electronic signature" shall mean a measure taken with regard to information that can be recorded in an electro-magnetic record (here and hereinafter, any record which is produced by electronic, magnetic, or any other means

unrecognizable by natural perceptive function, and is used for data-processing by a computer) and to which both of the following requirements applies:

- i. is a measure to indicate that the information was created by the person who performed the measure; and
 - ii. is a measure that can confirm whether or not any alteration of the information has been performed.
2. For the purpose of this law, "certification service" shall mean a service that, in compliance with either the request of a person who uses such service (hereinafter referred to as "user") with regard to the electronic signature that he himself performs or the request of another person, certifies that an item used to confirm that the user performed an electronic signature belongs to the user.
3. For the purpose of this law, "designated certification service" shall mean a certification service that is performed with regard to those electronic signatures that conform to the standards prescribed by the ordinance of the related ministries as ones that, according to the method thereof, can only be substantially performed by that person.

Chapter 2: Presumption of the authenticity of an electro-magnetic record

Article 3

An electro-magnetic record which is made in order to express information (with the exception of one drawn by a public official in the exercise of his official functions) shall be presumed to be authentic if an electronic signature (limited to those that, if based on the proper control of the codes and objects necessary to perform the signature, only that person can substantially perform) is performed by the principal in relation to information recorded in the electro-magnetic record.

Chapter 3: Accreditation, etc. of designated certification services

Section 1: Accreditation of designated certification services

Article 4 Accreditation

A person seeking to perform or has been performing designated certification service may receive an accreditation from the related ministers.

2. A person seeking to receive an accreditation stipulated in the preceding paragraph shall, in accordance with the prescriptions of the ordinance of the related ministries, file with the related ministers an application form that states the following facts as well as other documents prescribed by the ordinance of the related ministries:
 - i. the name and address, and if a organization, the name of its representative;
 - ii. an outline of the facilities used for the service applied for accreditation, and
 - iii. the method of implementation of the service applied for accreditation.
3. When the related ministers have granted the accreditation stipulated in paragraph 1, the ministers shall make an announcement of that fact.

Article 5 Disqualification provisions

A person to whom any of the following numbered items applies may not receive the accreditation stipulated in paragraph 1 of the preceding article:

- i. a person who has been sentenced to a penalty of imprisonment or greater (including an equivalent penalty pursuant to the laws and regulations of a foreign country) or who has been sentenced to a penalty pursuant to this Law and with respect to whom fewer than two years have passed since the day on which either the enforcement of said penalty finished or the person came to be no longer subject thereto;
- ii. a person whose accreditation has been revoked pursuant to the provisions of either Article 14, paragraph 1 or Article 16, paragraph 1, and with respect to whom fewer than two years have passed since the day of the revocation; or
- iii. an organization for whom either of the preceding numbered items applies to any director performing the service.

Article 6 Requirements of accreditation

The related ministers shall grant an accreditation only when they find that the application for accreditation stipulated in Article 4, paragraph 1 conforms to all of the following requirements:

- i. the facilities including (hardware, and software) used for the service applied for accreditation conform to requirements prescribed by the ordinance of the related ministries;
 - ii. the confirmation in the service applied for accreditation of the identity of the user is performed through a method prescribed by the ordinance of the related ministries; and
 - iii. in addition to the facts listed in the preceding numbered items, the service applied for accreditation is performed through a method that conforms with requirements prescribed by the ordinance of the related ministries.
2. In conducting the review for the purposes of the accreditation stipulated in Article 4, paragraph 1, the related ministers shall, in accordance with the prescriptions of the ordinance of the related ministries, perform on-site investigation of the system involved in the implementation of the service applied for accreditation.

Article 7 Renewal of accreditation

If the accreditation stipulated in Article 4, paragraph 1 is not renewed for each term of no less than one year prescribed by Cabinet Order, the accreditation shall become null and void upon the passing of the term.

2. The provisions of Article 4, paragraph 2 and those of the preceding two articles shall be applied, mutatis mutandis, to the renewal of accreditation provided for in the preceding paragraph.

Article 8 Succession

If a person who has received the accreditation stipulated in Article 4, paragraph 1 (hereinafter referred to as an “accredited certification service provider”) transfers all of the business that performs the accredited certification service, or if there is a

succession or merger with respect to the accredited certification service provider, the person who obtained all of such business by transfer, the successor (here and hereinafter in this article, in a case where there are two or more successors, if, by the agreement of all such successors, a successor is chosen to succeed to the business, that person), or the organization that continues in existence after the merger or the organization established by the merger shall succeed to the standing of such accredited certification service provider. However, the foregoing shall not apply if any of the numbered items of Article 5 apply to the person who obtained all of such business by transfer, the successor, or the organization that continues in existence after the merger or the organization established by the merger.

Article 9 Accreditation, etc. of changes

If an accredited certification service provider seeks to change an item stipulated in Article 4, paragraph 2, numbered item 2 or numbered item 3, it must receive the accreditation of related ministers. However, the foregoing shall not apply with respect to slight changes prescribed by order of the related ministries.

2. A person seeking to receive the accreditation of change stipulated in the preceding paragraph shall, in accordance with the prescriptions of the ordinance of the related ministries, file with the related ministers an application form that states the facts concerning the change as well as other documents prescribed by the ordinance of the related ministries.
3. The provisions of Article 4, paragraph 3 and those of Article 6 shall be applied, mutatis mutandis, to the accreditation of change provided for in paragraph 1.
4. If there is a change in a fact provided for in Article 4, paragraph 2, numbered item 1, an accredited certification service provider shall give notice of that fact to the related ministers without delay.

Article 10 Discontinuance

If an accredited certification service provider seeks to discontinue its accredited service, it must, in accordance with the prescriptions of the ordinance of the related ministries, give advance notice of that fact to the related ministers without delay.

2. When the related ministers have received the notice pursuant to the provision of the preceding paragraph, they shall make an announcement of that fact.

Article 11 Books and records

An accredited certification service provider shall, in accordance with the prescriptions of the ordinance of the related ministries, create and preserve books and records relating to its accredited service.

Article 12 Proper use of information relating to the confirmation of the identity of users

An accredited certification service provider shall not use the information it learns through the confirmation of the identity of users for its accredited service for any purpose other than those necessary for the provision of the accredited service.

Article 13 Mark

An accredited certification service provider may, in accordance with the prescriptions of the ordinance of the related ministries, place a mark to the effect that its service has received accreditation on an electronic certificate, etc. (here and in the following paragraph, this shall mean an electro-magnetic record or other means prescribed by the ordinance of the related ministries as one used for the sake of the certification service, created to verify that an item used to confirm that a user performed an electronic signature belongs to the user.)

2. Except for the cases stipulated in the preceding paragraph, no person shall place the mark provided for in the preceding paragraph or any mark not clearly distinguishable therefrom on any electronic certificate, etc.

Article 14 Revocation of accreditation

If any of the following numbered items applies to an accredited certification service provider, the related ministers may revoke such accreditation:

- i. if Article 5, numbered item 1 or numbered item 3 becomes applicable;
- ii. if the accredited certification service provider fails to conform to any numbered

- item of Article 6, paragraph 1; or
- iii. if the accredited certification service provider violates any provision of Article 9, paragraph 1, Article 11, Article 12, or Article 13, paragraph 2; or
 - iii. if the accredited certification service provider receives the accreditation provided for in Article 4, paragraph 1 or the accreditation of change stipulated in Article 9, paragraph 1 through any improper means.
2. When related ministers have revoked an accreditation pursuant to the provisions of the preceding paragraph, they shall make an announcement of that fact.

Section 2: Accreditation of designated certification service located in foreign countries

Article 15 Accreditation of foreign certification service etc.

A person seeking to perform the designated certification service by means of an office located in a foreign country may receive the accreditation from the related ministers.

2. The provisions of Article 4, paragraph 2 and paragraph 3 as well as those of Article 5 through Article 7 shall be applied mutatis mutandis to the accreditation provided for in the preceding paragraph, and the provisions of Article 8 through Article 13 shall be applied mutatis mutandis to the person who has received the accreditation provided for in the preceding paragraph (hereinafter referred to as “accredited foreign certification service provider”). In such a case, the term “no person” in Article 13, paragraph 2 shall be read as “no accredited foreign certification service provider”.
3. If the related ministers find that persons seeking to receive the accreditation provided for in paragraph 1, a renewal thereof or the accreditation of change stipulated in Article 9, paragraph 1 as applied mutatis mutandis in the preceding paragraph are persons who perform certification service by means of offices in the foreign country pursuant to provisions concerning certification service based on the laws and regulations of the foreign country that are similar to the provisions for accreditation stipulated in Article 4, paragraph 1, and that it is necessary to

faithfully perform a treaty that Japan has entered into with said foreign country or another international agreement(including administrative agreement) , they may require such persons to file documents that state facts prescribed by the ordinance of the related ministries instead of the investigation pursuant to the provisions of Article 6, paragraph 2 (including cases where they are applied mutatis mutandis in Article 7, paragraph 2 and Aeticle 9, paragraph 3, as applied mutatis mutandis in the preceding paragraph).

4. When, in the case as stipulated in the preceding paragraph, the documents are received from such persons, the related ministers shall, taking the documents into account, perform an examination for the purpose of the accreditation provided for in paragraph 1, a renewal thereof or the accreditation of change provided for Article 9, paragraph 1 as applied mutatis mutandis in paragraph 2.

Article 16 Revocation of accreditation

If any of the following numbered items applies to an accredited foreign certification service provider, the related ministers may revoke such accreditation:

- i. if Article 5, numbered item 1 or numbered item 3, as applied mutatis mutandis in the preceding article, paragraph 2, becomes applicable;
- ii. if the accredited certification service provider fails to conform to any numbered item of Article 6, paragraph 1 as applied mutatis mutandis in the preceding article, paragraph 2;
- iii. if the accredited foreign certification service provider violates any provision of Article 9, paragraph 1 or paragraph 4, Article 11, Article 12, or Article 13, paragraph 2 as applied mutatis mutandis in the preceding article, paragraph 2;
- iv. if the accredited certification service provider receives the accreditation stipulated in the preceding article, paragraph 1 or the accreditation of change provided for in Article 9, paragraph 1 as applied mutatis mutandis in the preceding article, paragraph 2 through any improper means.
- v. in a case where the related ministers have sought to compel the report of an accredited foreign certification service provider pursuant to the provisions of Article 35, paragraph 1 as applied mutatis mutandis in Article 35, paragraph 3, and either such report is not filed or a false report is filed; or
- vi. in a case where the related ministers have sought to have their staff member conduct an inspection at the business office, administrative office or other place

of business of an accredited foreign certification service provider pursuant to the provisions of Article 35, paragraph 1 as applied mutatis mutandis in Article 35, paragraph 3, and said accredited foreign certification service provider either refuses, obstructs, or evades such inspection or refuses to answer or provides false answers in response to questions posed pursuant to the provisions of the same paragraph.

2. When they have revoked an accreditation pursuant to the provisions of the preceding paragraph, the related ministers shall make an announcement of that fact.

Chapter 4: Designated investigating organization, etc.

Section 1: Designated investigating organization

Article 17 Investigation by a designated investigating organization

The related ministers may have the person they designate (hereinafter referred to as “designated investigating organization”) conduct the whole or part of the investigation pursuant to the provisions of Article 6, paragraph 2 (including cases where they are applied mutatis mutandis in Article 7, paragraph 2 [including cases where it is applied mutatis mutandis in Article 15, paragraph 2], Article 9, paragraph 3 [including cases where it is applied mutatis mutandis in Article 15, paragraph 2], and Article 15, paragraph 2) (hereinafter referred to, with the exception of the following section, as “investigation”).

2. If related ministers have the designated investigating organization conduct the whole or part of the investigation pursuant to the provisions of the preceding paragraph, they shall not conduct the whole or part of said investigation. In this case, the related ministers shall perform an examination in consideration of the results of the investigation that the designated investigating organization gives notice of pursuant to the provisions of paragraph 4 for the purpose of the accreditation provided for in Article 4, paragraph 1 or a renewal thereof, the accreditation of change provided for Article 9, paragraph 1 (including cases where it is applied mutatis mutandis in Article 15, paragraph 2) or the accreditation provided for in Article 15, paragraph 1 or renewal thereof.

3. When the related ministers have the designated investigating organization conduct the whole or part of the investigation pursuant to the provisions of paragraph 1, the person seeking to receive the accreditation provided for in Article 4, paragraph 1 or a renewal thereof, the accreditation of change provided for Article 9, paragraph 1 (including cases where it is applied mutatis mutandis in Article 15, paragraph 2) or the accreditation stipulated in Article 15, paragraph 1 or renewal thereof shall, in accordance with the prescriptions of the ordinance of the related ministries, file with the designated investigating organization an application with respect to the investigation that the designated investigating organization performs notwithstanding the provisions of Article 4, paragraph 2 (including cases where they are applied mutatis mutandis in Article 7, paragraph 2 [including cases where this is applied mutatis mutandis in Article 15, paragraph 2] and Article 15, paragraph 2) and Article 9, paragraph 2 (including cases where they are applied mutatis mutandis in Article 15, paragraph 2).
4. When the designated investigating organization has conducted the investigation upon the application provided for in the preceding paragraph, it shall, in accordance with the prescriptions of the ordinance of the related ministries, give notice of the results of the investigation to the related ministers without delay.

Article 18 Designation

Designation pursuant to the provisions of the preceding article, paragraph 1 (hereinafter referred to as “designation”) shall, in accordance with the prescriptions of the ordinance of the related ministries, be made upon the application of the person seeking to conduct the investigation (with the exception of a person seeking to conduct it by means of an office located in a foreign country).

Article 19 Disqualification provisions

A person to whom any of the following numbered items applies may not receive designation:

- i. a person who has been sentenced to a penalty of imprisonment or greater or who has been sentenced to a penalty pursuant to this Law and with respect to whom fewer than two years have passed since the day on which either the enforcement

- of the penalty finished or the person came to be no longer subject thereto;
- ii. a person whose designation has been revoked pursuant to the provisions of Article 29, paragraph 1, or whose approval has been revoked pursuant to the provisions of Article 32, paragraph 1, and with respect to whom fewer than two years have passed since the day of said revocation; or
- iii. an organization for whom either of the preceding numbered items applies to any director performing said service.

Article 20 Standards of designation

The related ministers shall grant designation upon the application only when they find that it conforms to all of the following numbered items:

- i. it possesses the financial base and technological ability sufficient to competently and smoothly implement the investigation service;
- ii. if an organization, there is no risk that its board members or the makeup of constituents prescribed by the ordinance of the related ministries in accordance with organization type will interfere with the fair implementation of the investigation;
- iii. if it performs a service other than the investigation service, there is no risk that the investigation will become unfair through the performance of such a service; and
- iv. a proper and smooth implementation of the investigation upon the application will not be impeded as a result of designation.

Article 21 Announcement, etc. of designation

When they have made a designation, the related ministers shall announce the name and address of the designated investigating organization and the location of its office performing the investigation service.

- 2. If the designated investigation organization seeks to change its name, address or the location of its office performing the investigation service, it must give notice of such fact to related ministers two weeks in advance of the day on which it seeks to make such change.
- 3. Upon the receipt of the notice stipulated in the preceding paragraph, the related

ministers shall make an announcement of that fact.

Article 22 **Renewal of designation**

If the designation is not renewed for each term of five years or more but less than ten years prescribed by Cabinet Order, the designation shall become null and void upon the passing of said term.

2. The provisions of Article 18 through Article 20 shall be applied, mutatis mutandis, to the renewal of designation provided for in the preceding paragraph.

Article 23 **Duty of confidentiality, etc.**

The board members (here, in the following paragraph as well as in Article 43 and Article 45, if the designated investigating organization is not an organization, the person who received said designation) and staff members of the designated investigating organization, as well as persons who formerly held such positions, shall not disclose any secrets that they learned in connection with the investigation service.

2. For the purposes of the application of the Criminal Law (Law No. 45 of 1907) and other penalties, the directors and staff members of a designated investigating organization engaging in the investigation service are deemed public officials pursuant to laws and regulations.

Article 24 **Duty of investigation**

When the designated investigating organization is requested to conduct an investigation, it shall conduct the investigation without delay unless there is a valid reason not to.

Article 25 **Investigation service regulations**

The designated investigating organization shall prescribe rules concerning the investigation service (hereinafter referred to as "investigation service rules") and obtain the authorization of the related ministers. The same procedure shall apply to amendments to the investigation service rules.

2. Matters to be prescribed in the investigation service rules shall be prescribed by the ordinance of the related ministries.
3. If the related ministers find that investigation service rules authorized pursuant to paragraph 1 have become inappropriate for the fair implementation of investigations, they may order that such investigation service rules be amended.

Article 26 Books and records

The designated investigating organization shall, in accordance with the prescriptions of the ordinance of the related ministries, prepare and preserve books and record facts concerning the investigation service as being prescribed by the ordinance of the related ministries.

Article 27 Order to conform

If related ministers find that a designated investigating organization is not in conformity with Article 20, numbered items 1 through 3, they may order that such designated investigating organization take measures necessary to conform to these provisions.

Article 28 Suspension and abrogation of service

Unless it receives the authorization of related ministers, a designated investigating organization may not suspend or abrogate the whole or part of its investigation service.

2. When he has given the authorization stipulated in the preceding paragraph, the related ministers shall make an announcement of that fact.

Article 29 Revocation, etc. of designation

If the related ministers find that any of the following numbered items apply to a designated investigating organization, they may revoke such designation, or they may order that the whole or part of the investigation service be suspended for a prescribed period:

- i. if there is a violation of any provision of this section;
 - ii. if Article 19, numbered item 1 or numbered item 3 becomes applicable;
 - iii. if investigation service is performed in violation of the investigation service regulations authorized pursuant to Article 25, paragraph 1;
 - iv. if there is a violation of any order pursuant to the provisions of Article 25, paragraph 3 or Article 27; or
 - v. if designation is received by any improper means.
2. When they have revoked a designation or ordered that the whole or part of the investigation service be suspended for a prescribed period pursuant to the provisions of the preceding paragraph, the related ministers shall make an announcement of that fact.

Article 30 **Implementation of the investigation service by related ministers**

If the designated investigating organization suspends the whole or part of the investigation service pursuant to the provisions of Article 28, paragraph 1; if the designated investigating organization is ordered to suspend the whole or part of the investigation service pursuant to the provisions of the preceding article, paragraph 1; or if the designated investigating organization becomes unable to conduct the whole or part of the investigation service due to a natural disaster or other ground, the related ministers shall, notwithstanding the provisions of Article 17, paragraph 2, conduct the whole or part of the investigation service when they find it necessary.

2. When the related ministers decide to conduct the investigation service pursuant to the provisions of the preceding paragraph, or decide to no longer conduct the investigation service that it is conducting pursuant to the provisions of the same paragraph, they shall make an announcement of that fact in advance.
3. For the cases when the related ministers decide to conduct the investigation service pursuant to the provisions of paragraph 1, permit the abrogation of the investigation service pursuant to the provisions of Article 28, paragraph 1, or revoke a designation pursuant to the provisions of the preceding article, paragraph 1, the ordinance of the related ministries shall prescribe necessary matters including taking over of the investigation service.

Section 2: Approved investigating organization

Article 31 Approval, etc. of approved investigating organization

When the related ministers receive an application from a person (limited to one seeking to conduct its business by means of an office located in a foreign country) seeking to conduct the whole or part of the investigation pursuant to the provisions of Article 6, paragraph 2 as applied mutatis mutandis in Article 15, paragraph 2 (including cases where they are applied mutatis mutandis in Article 7, paragraph 2 and Article 9, paragraph 3 as applied mutatis mutandis in Article 15, paragraph 2) (hereinafter in this section referred to as "investigation"), they may approve such petition in accordance with the prescriptions of the ordinance of the related ministries

2. When the related ministers grant the approval provided for in the preceding paragraph, a person seeking to receive the accreditation stipulated in Article 15, paragraph 1, a renewal thereof or the accreditation of change provided for Article 9, paragraph 1 as applied mutatis mutandis in Article 15, paragraph 2 may, in accordance with the prescriptions of the ordinance of the related ministries, apply the person who received the approval provided for in the preceding paragraph (hereinafter referred to as "approved investigating organization") with respect to the investigations that the approved investigating organization conducts notwithstanding the provisions of Article 4, paragraph 2 as applied mutatis mutandis in Article 15, paragraph 2 (including cases where they are applied mutatis mutandis in Article 7, paragraph 2 as applied mutatis mutandis in Article 15, paragraph 2) and those of Article 9, paragraph 2 and Article 17, paragraph 3 as applied mutatis mutandis in Article 15, paragraph 2. In this case, the related ministers shall perform a review in consideration of the results of the investigation that the approved investigating organization gives notice of pursuant to the provisions of the following paragraph for the purpose of the accreditation provided for in Article 15, paragraph 1, a renewal thereof or the accreditation of change provided for Article 9, paragraph 1 as applied mutatis mutandis in Article 15, paragraph 2).
3. When the approved investigating organization has conducted the investigation associated with the petition provided for in the preceding paragraph, it shall, in accordance with the prescriptions of the orders of the related ministries, give notice

of the results of said investigation to the related ministers without delay.

4. If an approved investigative organ suspends or abrogates the whole or part of the investigation service, it must give notice of that fact to related the ministers without delay.
5. When they have received the notice provided for in the preceding paragraph, related ministers shall make an announcement of that fact.
6. The provisions of Article 19 through Article 22 shall be applied mutatis mutandis to the approval provided for in paragraph 1, and the provisions of Article 24 through Article 27 shall be applied mutatis mutandis to the approved investigating organization. In this case, the term "order" in Article 25 paragraph 3 and in Article 27 shall be read as "request".

Article 32 Revocation of approval

If any of the following numbered items applies to an approved investigation organ, related ministers may revoke such approval:

- i. if there is a violation of a provision of the preceding article, paragraph 3 or 4, or a provision of Article 21, paragraph 2, Article 24, Article 25, paragraph 1, or Article 26 as applied mutatis mutandis in the preceding article, paragraph 6;
- ii. if Article 19, numbered item 1 or numbered item 3, as applied mutatis mutandis in the preceding article, paragraph 6, becomes applicable;
- iii. if investigation service is performed in violation of the investigation service regulations authorized pursuant to Article 25, paragraph 1 as applied mutatis mutandis in the preceding article, paragraph 6;
- iv. if there is a failure to comply with any request pursuant to the provisions of Article 25, paragraph 3 or Article 27 as applied mutatis mutandis in the preceding article, paragraph 6;
- v. if the approval stipulated in the preceding article, paragraph 1 is received by any improper means;
- vi. in a case where the related ministers find that any of the preceding numbered items applies to the approved investigating organization and requests that the whole or part of the investigation service be suspended for a prescribed period,

- the approved investigating organization fails to comply with such request;
- vii. in a case where the related ministers have sought to compel the report of an approved investigating organization pursuant to the provisions of Article 35, paragraph 2 as applied mutatis mutandis in Article 35, paragraph 3, and either such report is not filed or a false report is filed; or
 - viii. in a case where the related ministers have sought to have its staff member conduct an inspection at the administrative office of an approved investigating organization pursuant to the provisions of Article 35, paragraph 2 as applied mutatis mutandis in Article 35, paragraph 3, and said approved investigating organization either refuses, obstructs, or evades such inspection or refuses to answer or provides false answers in response to questions posed pursuant to the provisions of the same paragraph.
2. When the related ministers has revoked a approval pursuant to the provisions of the preceding paragraph, the related ministers shall make an announcement of that fact.

Chapter 5: Miscellaneous provisions

Article 33 Support, etc. for designated certification service

In order to promote the smooth implementation of the accreditation provisions concerning the designated certification service, the related ministers shall conduct surveys and research with respect to the evaluation of the technologies associated with electronic signatures and certification services and strive to provide necessary information, advice and other support to persons performing designated certification service and users.

Article 34 Measures by the national government

Through public education activities and public information activities, the national government shall strive to deepen the citizens' understanding of electronic signatures and certification services.

Article 35 Collection of reports and on-site inspections

The related ministers may, to the extent necessary to enforce this Law, compel an

accredited certification service provider to report on its accredited service or have its staff official enter the business office, administrative office or other place of business of an accredited certification service provider, and inspect the status of service, facilities, books and records and other objects associated with its accredited business as well as ask questions of the persons concerned.

2. The related ministers may, to the extent necessary to enforce this Law, compel a designated investigating organization to report on its service or have its staff official enter the administrative office of a designated investigating organization and inspect the status of service, books and records and other objects as well as ask questions of the persons concerned.
3. The provisions of paragraph 1 shall be applied mutatis mutandis to accredited foreign certification service providers and the provisions of the preceding paragraph shall be applied mutatis mutandis to approved investigating organizations.
4. A staff official who conducts an on-site inspection pursuant to the provisions of paragraph 1 or paragraph 2 (including cases where they are applied respectively in the preceding paragraph) shall carry a proof of his/her identity and present it to persons concerned.
5. The authority to conduct on-site inspections pursuant to the provisions of paragraph 1 and paragraph 2 (including cases where they are applied respectively in paragraph 3) shall not be interpreted as recognized for the purpose of criminal investigations.

Article 36 Fees

Persons listed in the following numbered items shall pay to the national government fees in the amounts prescribed by Cabinet Order, which will be determined in consideration of actual costs.

- i. a person seeking to receive an accreditation stipulated in Article 4, paragraph 1 or renewal thereof;
- ii. a person seeking to receive an accreditation of change stipulated in Article 9, paragraph 1 (including cases where it is applied mutatis mutandis in Article 15,

- paragraph 2); and
- iii. a person seeking to receive an accreditation stipulated in Article 15, paragraph 1 or renewal thereof.
2. A person seeking to receive an investigation performed by a designated investigating organization shall, in accordance with the prescription of a Cabinet Order, pay to the designated investigating organization a fee in the amount that the organization prescribes with the authorization of the related ministers.

Article 37 Relationship between related ministers and the National Public Safety Commission

When the National Public Safety Commission finds it necessary to prevent serious harm associated with the verification of users from occurring in connection with the accredited service of an accredited certification service provider or an accredited foreign certification service provider, the Commission may request the related ministers to take necessary measures.

Article 38 Request for review

A person who objects with respect to a disposition or omission a designated investigating organization pursuant to the provisions of this Law may request that the related ministers conduct a review pursuant to the Administrative Appeal Law (Law No. 160 of 1962)

Article 39 Interim measures

In the event that a Cabinet Order or ordinance of the related ministries pursuant to the provisions of this Law is enacted, amended or repealed, necessary interim measures (including interim measures pertaining to penalties) in the respective forms of Cabinet Order and ordinance of the related ministries may be prescribed within a scope determined to be reasonably necessary in accordance with such enactment, amendment or repeal.

Article 40 The related ministers, etc.

The term “the related minister” as used in this Law refers to the Minister of General Affairs, the Minister of Justice, and the Minister of Economy and Industry; however, the reference “the related ministers” in Article 33 refers to the Minister of General Affairs and the Minister of Economy and Industry.

2. The term “ordinance of the related ministries” as used in this Law refers to an ordinance jointly issued by the Minister of General Affairs, the Minister of Justice, and the Minister of Economy and Industry.

Chapter 6: Penalties

Article 41

A person who makes a false application before an accredited certification service provider or accredited foreign certification service provider in connection with its accredited certification service and thereby causes an untrue certification shall be punished with penal servitude for not more than three years or a fine of not more than two million yen.

2. Attempts of the crimes mentioned in the preceding paragraph shall be punished.
3. The crimes mentioned in the preceding two paragraphs shall comply with the precedents of the Criminal Law, Article 2.

Article 42

A person to whom any of the following numbered items applies shall be punished to no more than one year of penal servitude or a fine of not more than one million yen:

- i. a person who violates a provision of Article 13, paragraph 2;
- ii. a person who discloses a secret that he learned in connection with his duties in violation of a provision of Article 23, paragraph 1.

Article 43

If an order to suspend service pursuant to the provisions of Article 29, paragraph 1 is violated, an officer or staff member of a designated investigative organ that commits

the act of violation shall be punished to no more than one year of penal servitude or a fine of not more than one million yen.

Article 44

A person to whom any of the following numbered items applies shall be punished to a fine of not more than three hundred thousand yen:

- i. a person who changes a fact provided for in Article 4, paragraph 2, numbered item 2 or numbered item 3 in violation of a provision of Article 9, paragraph 1;
- ii. a person who fails to create or preserve the accounting books and records pursuant to the provisions of Article 11, or who creates false accounting books and records; or
- iii. a person who fails to file a report pursuant to the provisions of Article 35, paragraph 1, or files a false such report, or who refuses, obstructs, or evades an inspection pursuant to the provisions of the same paragraph, or who refuses to answer or provides false answers in response to questions posed pursuant to the provisions of the same paragraph.

Article 45

If any of the following numbered items apply, an officer or staff member of a designated investigating organization that commits the act of violation shall be punished to a fine of not more than three hundred thousand yen:

- i. when the designated investigative organ fails to create accounting book records pursuant to the provisions of Article 26, creates false records, or fails to preserve the accounting books;
- ii. when the designated investigating organization abrogates all of its investigation service in violation of a provision of Article 28, paragraph 1; or
- iii. when the designated investigative organ fails to file a report pursuant to the provisions of Article 35, paragraph 2, or files a false such report, or refuses, obstructs, or evades an inspection pursuant to the provisions of the same paragraph, or refuses to answer or provides false answers in response to questions posed pursuant to the provisions of the same paragraph.

Article 46

If any representative of an organization or any agent, servant or other employee of any of a organization or person commits, in connection with the service of such organization or person, an act in violation of Article 42, paragraph 1 or Article 44, then

in addition to the punishment of the actor, the monetary penalties provided for in each above provision shall be imposed against such organization or person.

Article 47

A person who fails to give notice pursuant to the provisions of Article 9, paragraph 4 or Article 10, paragraph 1, or who gives a false notice shall be punished to a non-penal fine of no more than one hundred thousand yen.

Supplemental provisions

Article 1 Date of enforcement

This Law shall be enforced from April 1, 2001; provided that the provisions of the following article shall be enforced from March 1, 2001, and the provisions of Supplemental Article 4 shall be enforced from the date of enforcement of the Law Concerning the Arrangement of Related Laws That Accompany the Enforcement of Laws That Revise Parts of the Commercial Code, etc. (Law No. ---- of 2000)

Article 2 Preparatory actions

Prior to the enforcement of this Law, designation pursuant to the provisions of Article 17, paragraph 1 and necessary procedures and other actions in connection therewith may be performed pursuant to the precedents of Article 18 through Article 20, Article 21, paragraph 1, and Article 25, paragraph 1 and paragraph 2.

Article 3 Examination

When five years have passed since the enforcement of this Law, the government shall examine the status of enforcement hereof and take necessary measures based on the results of such examination.

Article 4 Partial revision of the Law Concerning the Arrangement of Related Laws That Accompany the Enforcement of Laws That Revise Parts of the

Commercial Code, etc.

A part of the Law Concerning the Arrangement of Related Laws That Accompany the Enforcement of Laws That Revise Parts of the Commercial Code, etc. shall be revised as follows.

The following article shall be added following Article 150:

Article 150-2 Partial revision of the Law Concerning Electronic Signatures and Certification Services

A part of the Law Concerning Electronic Signatures and Certification Services (Law No. ____ of 2000) shall be revised as follows.

Throughout the text of Article 8, the phrase “or merger” shall be changed to , “merger or partition (limited to one that would cause succession of the whole of the business that performs service associated with such accreditation)”; the phrase “or the organization that continues in existence after the merger” shall be changed to “the organization that continues in existence after the merger”; and the phrase “or the organization that succeeds to the whole of such business through partition” shall be added after the phrase “the organization established by the merger”.



31995L0046

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
Official Journal L 281 , 23/11/1995 P. 0031 - 0050

 **MORE INFO**

TEXT:

DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 24 October 1995

on the protection of individuals with regard to the processing of personal data and on the free movement of such data

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 100a thereof,

Having regard to the proposal from the Commission (1),

Having regard to the opinion of the Economic and Social Committee (2),

Acting in accordance with the procedure referred to in Article 189b of the Treaty (3),

(1) Whereas the objectives of the Community, as laid down in the Treaty, as amended by the Treaty on European Union, include creating an ever closer union among the peoples of Europe, fostering closer relations between the States belonging to the Community, ensuring economic and social progress by common action to eliminate the barriers which divide Europe, encouraging the constant improvement of the living conditions of its peoples, preserving and strengthening peace and liberty and promoting democracy on the basis of the fundamental rights recognized in the constitution and laws of the Member States and in the European Convention for the Protection of Human Rights and Fundamental Freedoms;

(2) Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals;

(3) Whereas the establishment and functioning of an internal market in which, in accordance with Article 7a of the Treaty, the free movement of goods, persons, services and capital is ensured require not only that personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals should be safeguarded;

(4) Whereas increasingly frequent recourse is being had in the Community to the processing of personal data in the various spheres of economic and social activity; whereas the progress made in information technology is making the processing and exchange of such data considerably easier;

(5) Whereas the economic and social integration resulting from the establishment and functioning of the internal market within the meaning of Article 7a of the Treaty will necessarily lead to a substantial increase in cross-border flows of personal data between all those involved in a private or public capacity in

personal data between all those involved in a private or public capacity in economic and social activity in the Member States; whereas the exchange of personal data between undertakings in different Member States is set to increase; whereas the national authorities in the various Member States are being called upon by virtue of Community law to collaborate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State within the context of the area without internal frontiers as constituted by the internal market;

(6) Whereas, furthermore, the increase in scientific and technical cooperation and the coordinated introduction of new telecommunications networks in the Community necessitate and facilitate cross-border flows of personal data;

(7) Whereas the difference in levels of protection of the rights and freedoms of individuals, notably the right to privacy, with regard to the processing of personal data afforded in the Member States may prevent the transmission of such data from the territory of one Member State to that of another Member State; whereas this difference may therefore constitute an obstacle to the pursuit of a number of economic activities at Community level, distort competition and impede authorities in the discharge of their responsibilities under Community law; whereas this difference in levels of protection is due to the existence of a wide variety of national laws, regulations and administrative provisions;

(8) Whereas, in order to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of individuals with regard to the processing of such data must be equivalent in all Member States; whereas this objective is vital to the internal market but cannot be achieved by the Member States alone, especially in view of the scale of the divergences which currently exist between the relevant laws in the Member States and the need to coordinate the laws of the Member States so as to ensure that the cross-border flow of personal data is regulated in a consistent manner that is in keeping with the objective of the internal market as provided for in Article 7a of the Treaty; whereas Community action to approximate those laws is therefore needed;

(9) Whereas, given the equivalent protection resulting from the approximation of national laws, the Member States will no longer be able to inhibit the free movement between them of personal data on grounds relating to protection of the rights and freedoms of individuals, and in particular the right to privacy; whereas Member States will be left a margin for manoeuvre, which may, in the context of implementation of the Directive, also be exercised by the business and social partners; whereas Member States will therefore be able to specify in their national law the general conditions governing the lawfulness of data processing; whereas in doing so the Member States shall strive to improve the protection currently provided by their legislation; whereas, within the limits of this margin for manoeuvre and in accordance with Community law, disparities could arise in the implementation of the Directive, and this could have an effect on the movement of data within a Member State as well as within the Community;

(10) Whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law; whereas, for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community;

(11) Whereas the principles of the protection of the rights and freedoms of individuals, notably the right to privacy, which are contained in this Directive, give substance to and amplify those contained in the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data;

(12) Whereas the protection principles must apply to all processing of personal data by any person whose activities are governed by Community law; whereas there should be excluded the processing of data carried out by a natural person in

there should be excluded the processing of data carried out by a natural person in the exercise of activities which are exclusively personal or domestic, such as correspondence and the holding of records of addresses;

(13) Whereas the activities referred to in Titles V and VI of the Treaty on European Union regarding public safety, defence, State security or the activities of the State in the area of criminal laws fall outside the scope of Community law, without prejudice to the obligations incumbent upon Member States under Article 56 (2), Article 57 or Article 100a of the Treaty establishing the European Community; whereas the processing of personal data that is necessary to safeguard the economic well-being of the State does not fall within the scope of this Directive where such processing relates to State security matters;

(14) Whereas, given the importance of the developments under way, in the framework of the information society, of the techniques used to capture, transmit, manipulate, record, store or communicate sound and image data relating to natural persons, this Directive should be applicable to processing involving such data;

(15) Whereas the processing of such data is covered by this Directive only if it is automated or if the data processed are contained or are intended to be contained in a filing system structured according to specific criteria relating to individuals, so as to permit easy access to the personal data in question;

(16) Whereas the processing of sound and image data, such as in cases of video surveillance, does not come within the scope of this Directive if it is carried out for the purposes of public security, defence, national security or in the course of State activities relating to the area of criminal law or of other activities which do not come within the scope of Community law;

(17) Whereas, as far as the processing of sound and image data carried out for purposes of journalism or the purposes of literary or artistic expression is concerned, in particular in the audiovisual field, the principles of the Directive are to apply in a restricted manner according to the provisions laid down in Article 9;

(18) Whereas, in order to ensure that individuals are not deprived of the protection to which they are entitled under this Directive, any processing of personal data in the Community must be carried out in accordance with the law of one of the Member States; whereas, in this connection, processing carried out under the responsibility of a controller who is established in a Member State should be governed by the law of that State;

(19) Whereas establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements; whereas the legal form of such an establishment, whether simply branch or a subsidiary with a legal personality, is not the determining factor in this respect; whereas, when a single controller is established on the territory of several Member States, particularly by means of subsidiaries, he must ensure, in order to avoid any circumvention of national rules, that each of the establishments fulfils the obligations imposed by the national law applicable to its activities;

(20) Whereas the fact that the processing of data is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this Directive; whereas in these cases, the processing should be governed by the law of the Member State in which the means used are located, and there should be guarantees to ensure that the rights and obligations provided for in this Directive are respected in practice;

(21) Whereas this Directive is without prejudice to the rules of territoriality applicable in criminal matters;

(22) Whereas Member States shall more precisely define in the laws they enact or when bringing into force the measures taken under this Directive the general circumstances in which processing is lawful; whereas in particular Article 5, in conjunction with Articles 7 and 8, allows Member States, independently of general rules, to provide for special processing conditions for specific sectors and for the various categories of data covered by Article 8;

(23) Whereas Member States are empowered to ensure the implementation of the protection of individuals both by means of a general law on the protection of

protection of individuals both by means of a general law on the protection of individuals as regards the processing of personal data and by sectorial laws such as those relating, for example, to statistical institutes;

(24) Whereas the legislation concerning the protection of legal persons with regard to the processing data which concerns them is not affected by this Directive;

(25) Whereas the principles of protection must be reflected, on the one hand, in the obligations imposed on persons, public authorities, enterprises, agencies or other bodies responsible for processing, in particular regarding data quality, technical security, notification to the supervisory authority, and the circumstances under which processing can be carried out, and, on the other hand, in the right conferred on individuals, the data on whom are the subject of processing, to be informed that processing is taking place, to consult the data, to request corrections and even to object to processing in certain circumstances;

(26) Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable; whereas codes of conduct within the meaning of Article 27 may be a useful instrument for providing guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible;

(27) Whereas the protection of individuals must apply as much to automatic processing of data as to manual processing; whereas the scope of this protection must not in effect depend on the techniques used, otherwise this would create a serious risk of circumvention; whereas, nonetheless, as regards manual processing, this Directive covers only filing systems, not unstructured files; whereas, in particular, the content of a filing system must be structured according to specific criteria relating to individuals allowing easy access to the personal data; whereas, in line with the definition in Article 2 (c), the different criteria for determining the constituents of a structured set of personal data, and the different criteria governing access to such a set, may be laid down by each Member State; whereas files or sets of files as well as their cover pages, which are not structured according to specific criteria, shall under no circumstances fall within the scope of this Directive;

(28) Whereas any processing of personal data must be lawful and fair to the individuals concerned; whereas, in particular, the data must be adequate, relevant and not excessive in relation to the purposes for which they are processed; whereas such purposes must be explicit and legitimate and must be determined at the time of collection of the data; whereas the purposes of processing further to collection shall not be incompatible with the purposes as they were originally specified;

(29) Whereas the further processing of personal data for historical, statistical or scientific purposes is not generally to be considered incompatible with the purposes for which the data have previously been collected provided that Member States furnish suitable safeguards; whereas these safeguards must in particular rule out the use of the data in support of measures or decisions regarding any particular individual;

(30) Whereas, in order to be lawful, the processing of personal data must in addition be carried out with the consent of the data subject or be necessary for the conclusion or performance of a contract binding on the data subject, or as a legal requirement, or for the performance of a task carried out in the public interest or in the exercise of official authority, or in the legitimate interests of a natural or legal person, provided that the interests or the rights and freedoms of the data subject are not overriding; whereas, in particular, in order to maintain a balance between the interests involved while guaranteeing effective competition, Member

between the interests involved while guaranteeing effective competition, Member States may determine the circumstances in which personal data may be used or disclosed to a third party in the context of the legitimate ordinary business activities of companies and other bodies; whereas Member States may similarly specify the conditions under which personal data may be disclosed to a third party for the purposes of marketing whether carried out commercially or by a charitable organization or by any other association or foundation, of a political nature for example, subject to the provisions allowing a data subject to object to the processing of data regarding him, at no cost and without having to state his reasons;

(31) Whereas the processing of personal data must equally be regarded as lawful where it is carried out in order to protect an interest which is essential for the data subject's life;

(32) Whereas it is for national legislation to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public administration or another natural or legal person governed by public law, or by private law such as a professional association;

(33) Whereas data which are capable by their nature of infringing fundamental freedoms or privacy should not be processed unless the data subject gives his explicit consent; whereas, however, derogations from this prohibition must be explicitly provided for in respect of specific needs, in particular where the processing of these data is carried out for certain health-related purposes by persons subject to a legal obligation of professional secrecy or in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms;

(34) Whereas Member States must also be authorized, when justified by grounds of important public interest, to derogate from the prohibition on processing sensitive categories of data where important reasons of public interest so justify in areas such as public health and social protection - especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system - scientific research and government statistics; whereas it is incumbent on them, however, to provide specific and suitable safeguards so as to protect the fundamental rights and the privacy of individuals;

(35) Whereas, moreover, the processing of personal data by official authorities for achieving aims, laid down in constitutional law or international public law, of officially recognized religious associations is carried out on important grounds of public interest;

(36) Whereas where, in the course of electoral activities, the operation of the democratic system requires in certain Member States that political parties compile data on people's political opinion, the processing of such data may be permitted for reasons of important public interest, provided that appropriate safeguards are established;

(37) Whereas the processing of personal data for purposes of journalism or for purposes of literary or artistic expression, in particular in the audiovisual field, should qualify for exemption from the requirements of certain provisions of this Directive in so far as this is necessary to reconcile the fundamental rights of individuals with freedom of information and notably the right to receive and impart information, as guaranteed in particular in Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms; whereas Member States should therefore lay down exemptions and derogations necessary for the purpose of balance between fundamental rights as regards general measures on the legitimacy of data processing, measures on the transfer of data to third countries and the power of the supervisory authority; whereas this should not, however, lead Member States to lay down exemptions from the measures to ensure security of processing; whereas at least the supervisory authority responsible for this sector should also be provided with certain ex-post powers, e.g. to publish a regular report or to refer matters to the judicial

powers, e.g. to publish a regular report or to refer matters to the judicial authorities;

(38) Whereas, if the processing of data is to be fair, the data subject must be in a position to learn of the existence of a processing operation and, where data are collected from him, must be given accurate and full information, bearing in mind the circumstances of the collection;

(39) Whereas certain processing operations involve data which the controller has not collected directly from the data subject; whereas, furthermore, data can be legitimately disclosed to a third party, even if the disclosure was not anticipated at the time the data were collected from the data subject; whereas, in all these cases, the data subject should be informed when the data are recorded or at the latest when the data are first disclosed to a third party;

(40) Whereas, however, it is not necessary to impose this obligation of the data subject already has the information; whereas, moreover, there will be no such obligation if the recording or disclosure are expressly provided for by law or if the provision of information to the data subject proves impossible or would involve disproportionate efforts, which could be the case where processing is for historical, statistical or scientific purposes; whereas, in this regard, the number of data subjects, the age of the data, and any compensatory measures adopted may be taken into consideration;

(41) Whereas any person must be able to exercise the right of access to data relating to him which are being processed, in order to verify in particular the accuracy of the data and the lawfulness of the processing; whereas, for the same reasons, every data subject must also have the right to know the logic involved in the automatic processing of data concerning him, at least in the case of the automated decisions referred to in Article 15 (1); whereas this right must not adversely affect trade secrets or intellectual property and in particular the copyright protecting the software; whereas these considerations must not, however, result in the data subject being refused all information;

(42) Whereas Member States may, in the interest of the data subject or so as to protect the rights and freedoms of others, restrict rights of access and information; whereas they may, for example, specify that access to medical data may be obtained only through a health professional;

(43) Whereas restrictions on the rights of access and information and on certain obligations of the controller may similarly be imposed by Member States in so far as they are necessary to safeguard, for example, national security, defence, public safety, or important economic or financial interests of a Member State or the Union, as well as criminal investigations and prosecutions and action in respect of breaches of ethics in the regulated professions; whereas the list of exceptions and limitations should include the tasks of monitoring, inspection or regulation necessary in the three last-mentioned areas concerning public security, economic or financial interests and crime prevention; whereas the listing of tasks in these three areas does not affect the legitimacy of exceptions or restrictions for reasons of State security or defence;

(44) Whereas Member States may also be led, by virtue of the provisions of Community law, to derogate from the provisions of this Directive concerning the right of access, the obligation to inform individuals, and the quality of data, in order to secure certain of the purposes referred to above;

(45) Whereas, in cases where data might lawfully be processed on grounds of public interest, official authority or the legitimate interests of a natural or legal person, any data subject should nevertheless be entitled, on legitimate and compelling grounds relating to his particular situation, to object to the processing of any data relating to himself; whereas Member States may nevertheless lay down national provisions to the contrary;

(46) Whereas the protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organizational measures be taken, both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain

system and at the time of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorized processing; whereas it is incumbent on the Member States to ensure that controllers comply with these measures; whereas these measures must ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected;

(47) Whereas where a message containing personal data is transmitted by means of a telecommunications or electronic mail service, the sole purpose of which is the transmission of such messages, the controller in respect of the personal data contained in the message will normally be considered to be the person from whom the message originates, rather than the person offering the transmission services; whereas, nevertheless, those offering such services will normally be considered controllers in respect of the processing of the additional personal data necessary for the operation of the service;

(48) Whereas the procedures for notifying the supervisory authority are designed to ensure disclosure of the purposes and main features of any processing operation for the purpose of verification that the operation is in accordance with the national measures taken under this Directive;

(49) Whereas, in order to avoid unsuitable administrative formalities, exemptions from the obligation to notify and simplification of the notification required may be provided for by Member States in cases where processing is unlikely adversely to affect the rights and freedoms of data subjects, provided that it is in accordance with a measure taken by a Member State specifying its limits; whereas exemption or simplification may similarly be provided for by Member States where a person appointed by the controller ensures that the processing carried out is not likely adversely to affect the rights and freedoms of data subjects; whereas such a data protection official, whether or not an employee of the controller, must be in a position to exercise his functions in complete independence;

(50) Whereas exemption or simplification could be provided for in cases of processing operations whose sole purpose is the keeping of a register intended, according to national law, to provide information to the public and open to consultation by the public or by any person demonstrating a legitimate interest;

(51) Whereas, nevertheless, simplification or exemption from the obligation to notify shall not release the controller from any of the other obligations resulting from this Directive;

(52) Whereas, in this context, ex post facto verification by the competent authorities must in general be considered a sufficient measure;

(53) Whereas, however, certain processing operations are likely to pose specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, such as that of excluding individuals from a right, benefit or a contract, or by virtue of the specific use of new technologies; whereas it is for Member States, if they so wish, to specify such risks in their legislation;

(54) Whereas with regard to all the processing undertaken in society, the amount posing such specific risks should be very limited; whereas Member States must provide that the supervisory authority, or the data protection official in cooperation with the authority, check such processing prior to it being carried out; whereas following this prior check, the supervisory authority may, according to its national law, give an opinion or an authorization regarding the processing; whereas such checking may equally take place in the course of the preparation either of a measure of the national parliament or of a measure based on such a legislative measure, which defines the nature of the processing and lays down appropriate safeguards;

(55) Whereas, if the controller fails to respect the rights of data subjects, national legislation must provide for a judicial remedy; whereas any damage which a person may suffer as a result of unlawful processing must be compensated for by the controller, who may be exempted from liability if he proves that he is not

responsible for the damage, in particular in cases where he establishes fault on the part of the data subject or in case of force majeure; whereas sanctions must be imposed on any person, whether governed by private or public law, who fails to comply with the national measures taken under this Directive;

(56) Whereas cross-border flows of personal data are necessary to the expansion of international trade; whereas the protection of individuals guaranteed in the Community by this Directive does not stand in the way of transfers of personal data to third countries which ensure an adequate level of protection; whereas the adequacy of the level of protection afforded by a third country must be assessed in the light of all the circumstances surrounding the transfer operation or set of transfer operations;

(57) Whereas, on the other hand, the transfer of personal data to a third country which does not ensure an adequate level of protection must be prohibited;

(58) Whereas provisions should be made for exemptions from this prohibition in certain circumstances where the data subject has given his consent, where the transfer is necessary in relation to a contract or a legal claim, where protection of an important public interest so requires, for example in cases of international transfers of data between tax or customs administrations or between services competent for social security matters, or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest; whereas in this case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or if they are to be the recipients;

(59) Whereas particular measures may be taken to compensate for the lack of protection in a third country in cases where the controller offers appropriate safeguards; whereas, moreover, provision must be made for procedures for negotiations between the Community and such third countries;

(60) Whereas, in any event, transfers to third countries may be effected only in full compliance with the provisions adopted by the Member States pursuant to this Directive, and in particular Article 8 thereof;

(61) Whereas Member States and the Commission, in their respective spheres of competence, must encourage the trade associations and other representative organizations concerned to draw up codes of conduct so as to facilitate the application of this Directive, taking account of the specific characteristics of the processing carried out in certain sectors, and respecting the national provisions adopted for its implementation;

(62) Whereas the establishment in Member States of supervisory authorities, exercising their functions with complete independence, is an essential component of the protection of individuals with regard to the processing of personal data;

(63) Whereas such authorities must have the necessary means to perform their duties, including powers of investigation and intervention, particularly in cases of complaints from individuals, and powers to engage in legal proceedings; whereas such authorities must help to ensure transparency of processing in the Member States within whose jurisdiction they fall;

(64) Whereas the authorities in the different Member States will need to assist one another in performing their duties so as to ensure that the rules of protection are properly respected throughout the European Union;

(65) Whereas, at Community level, a Working Party on the Protection of Individuals with regard to the Processing of Personal Data must be set up and be completely independent in the performance of its functions; whereas, having regard to its specific nature, it must advise the Commission and, in particular, contribute to the uniform application of the national rules adopted pursuant to this Directive;

(66) Whereas, with regard to the transfer of data to third countries, the application of this Directive calls for the conferment of powers of implementation on the

of this Directive calls for the conferment of powers of implementation on the Commission and the establishment of a procedure as laid down in Council Decision 87/373/EEC (1);

(67) Whereas an agreement on a modus vivendi between the European Parliament, the Council and the Commission concerning the implementing measures for acts adopted in accordance with the procedure laid down in Article 189b of the EC Treaty was reached on 20 December 1994;

(68) Whereas the principles set out in this Directive regarding the protection of the rights and freedoms of individuals, notably their right to privacy, with regard to the processing of personal data may be supplemented or clarified, in particular as far as certain sectors are concerned, by specific rules based on those principles;

(69) Whereas Member States should be allowed a period of not more than three years from the entry into force of the national measures transposing this Directive in which to apply such new national rules progressively to all processing operations already under way; whereas, in order to facilitate their cost-effective implementation, a further period expiring 12 years after the date on which this Directive is adopted will be allowed to Member States to ensure the conformity of existing manual filing systems with certain of the Directive's provisions; whereas, where data contained in such filing systems are manually processed during this extended transition period, those systems must be brought into conformity with these provisions at the time of such processing;

(70) Whereas it is not necessary for the data subject to give his consent again so as to allow the controller to continue to process, after the national provisions taken pursuant to this Directive enter into force, any sensitive data necessary for the performance of a contract concluded on the basis of free and informed consent before the entry into force of these provisions;

(71) Whereas this Directive does not stand in the way of a Member State's regulating marketing activities aimed at consumers residing in territory in so far as such regulation does not concern the protection of individuals with regard to the processing of personal data;

(72) Whereas this Directive allows the principle of public access to official documents to be taken into account when implementing the principles set out in this Directive,

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I GENERAL PROVISIONS

Article 1

Object of the Directive

1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.

2. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.

Article 2

Definitions

For the purposes of this Directive:

(a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

(b) 'processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or

means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

(c) 'personal data filing system' ('filing system') shall mean any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

(d) 'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;

(e) 'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

(f) 'third party' shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data;

(g) 'recipient' shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients;

(h) 'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

Article 3

Scope

1. This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.

2. This Directive shall not apply to the processing of personal data:

- in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,

- by a natural person in the course of a purely personal or household activity.

Article 4

National law applicable

1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:

(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;

(b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;

(c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

2. In the circumstances referred to in paragraph 1 (c), the controller must

2. In the circumstances referred to in paragraph 1 (c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.

CHAPTER II GENERAL RULES ON THE LAWFULNESS OF THE PROCESSING OF PERSONAL DATA

Article 5

Member States shall, within the limits of the provisions of this Chapter, determine more precisely the conditions under which the processing of personal data is lawful.

SECTION I

PRINCIPLES RELATING TO DATA QUALITY

Article 6

1. Member States shall provide that personal data must be:

- (a) processed fairly and lawfully;
- (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;
- (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
- (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
- (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

2. It shall be for the controller to ensure that paragraph 1 is complied with.

SECTION II

CRITERIA FOR MAKING DATA PROCESSING LEGITIMATE

Article 7

Member States shall provide that personal data may be processed only if:

- (a) the data subject has unambiguously given his consent; or
- (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
- (c) processing is necessary for compliance with a legal obligation to which the controller is subject; or
- (d) processing is necessary in order to protect the vital interests of the data subject; or
- (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
- (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

SECTION III

SPECIAL CATEGORIES OF PROCESSING

Article 8

The processing of special categories of data

The processing of special categories of data

1. Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

2. Paragraph 1 shall not apply where:

(a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent; or

(b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or

(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or

(d) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or

(e) the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.

3. Paragraph 1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

4. Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority.

5. Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority.

Member States may provide that data relating to administrative sanctions or judgements in civil cases shall also be processed under the control of official authority.

6. Derogations from paragraph 1 provided for in paragraphs 4 and 5 shall be notified to the Commission.

7. Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed.

Article 9

Processing of personal data and freedom of expression

Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.

SECTION IV

INFORMATION TO BE GIVEN TO THE DATA SUBJECT

Article 10

Article 10

Information in cases of collection of data from the data subject

Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it:

- (a) the identity of the controller and of his representative, if any;
- (b) the purposes of the processing for which the data are intended;
- (c) any further information such as
 - the recipients or categories of recipients of the data,
 - whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,
 - the existence of the right of access to and the right to rectify the data concerning him

in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

Article 11

Information where the data have not been obtained from the data subject

1. Where the data have not been obtained from the data subject, Member States shall provide that the controller or his representative must at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed provide the data subject with at least the following information, except where he already has it:

- (a) the identity of the controller and of his representative, if any;
- (b) the purposes of the processing;
- (c) any further information such as
 - the categories of data concerned,
 - the recipients or categories of recipients,
 - the existence of the right of access to and the right to rectify the data concerning him

in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.

2. Paragraph 1 shall not apply where, in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law. In these cases Member States shall provide appropriate safeguards.

SECTION V

THE DATA SUBJECT'S RIGHT OF ACCESS TO DATA

Article 12

Right of access

Member States shall guarantee every data subject the right to obtain from the controller:

- (a) without constraint at reasonable intervals and without excessive delay or expense:
 - confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,
 - communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,
 - knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 (1);
- (b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because

which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;
(c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.

SECTION VI

EXEMPTIONS AND RESTRICTIONS

Article 13

Exemptions and restrictions

1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard:

- (a) national security;
- (b) defence;
- (c) public security;
- (d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;
- (e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;
- (f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);
- (g) the protection of the data subject or of the rights and freedoms of others.

2. Subject to adequate legal safeguards, in particular that the data are not used for taking measures or decisions regarding any particular individual, Member States may, where there is clearly no risk of breaching the privacy of the data subject, restrict by a legislative measure the rights provided for in Article 12 when data are processed solely for purposes of scientific research or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics.

SECTION VII

THE DATA SUBJECT'S RIGHT TO OBJECT

Article 14

The data subject's right to object

Member States shall grant the data subject the right:

(a) at least in the cases referred to in Article 7 (e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation.

Where there is a justified objection, the processing instigated by the controller may no longer involve those data;

(b) to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.

Member States shall take the necessary measures to ensure that data subjects are aware of the existence of the right referred to in the first subparagraph of (b).

Article 15

Automated individual decisions

1. Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.

2. Subject to the other Articles of this Directive, Member States shall provide that

2. Subject to the other Articles of this Directive, Member States shall provide that a person may be subjected to a decision of the kind referred to in paragraph 1 if that decision:

(a) is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or

(b) is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests.

SECTION VIII

CONFIDENTIALITY AND SECURITY OF PROCESSING

Article 16

Confidentiality of processing

Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law.

Article 17

Security of processing

1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.

3. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:

- the processor shall act only on instructions from the controller,
- the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.

4. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form.

SECTION IX

NOTIFICATION

Article 18

Obligation to notify the supervisory authority

1. Member States shall provide that the controller or his representative, if any, must notify the supervisory authority referred to in Article 28 before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes.

2. Member States may provide for the simplification of or exemption from notification only in the following cases and under the following conditions:

- where, for categories of processing operations which are unlikely, taking account of the data to be processed, to affect adversely the rights and freedoms of data subjects, they specify the purposes of the processing, the data or categories of data undergoing processing, the category or categories of data subject, the

data undergoing processing, the category or categories of data subject, the recipients or categories of recipient to whom the data are to be disclosed and the length of time the data are to be stored, and/or

- where the controller, in compliance with the national law which governs him, appoints a personal data protection official, responsible in particular:

- for ensuring in an independent manner the internal application of the national provisions taken pursuant to this Directive

- for keeping the register of processing operations carried out by the controller, containing the items of information referred to in Article 21 (2), thereby ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations.

3. Member States may provide that paragraph 1 does not apply to processing whose sole purpose is the keeping of a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person demonstrating a legitimate interest.

4. Member States may provide for an exemption from the obligation to notify or a simplification of the notification in the case of processing operations referred to in Article 8 (2) (d).

5. Member States may stipulate that certain or all non-automatic processing operations involving personal data shall be notified, or provide for these processing operations to be subject to simplified notification.

Article 19

Contents of notification

1. Member States shall specify the information to be given in the notification. It shall include at least:

(a) the name and address of the controller and of his representative, if any;

(b) the purpose or purposes of the processing;

(c) a description of the category or categories of data subject and of the data or categories of data relating to them;

(d) the recipients or categories of recipient to whom the data might be disclosed;

(e) proposed transfers of data to third countries;

(f) a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Article 17 to ensure security of processing.

2. Member States shall specify the procedures under which any change affecting the information referred to in paragraph 1 must be notified to the supervisory authority.

Article 20

Prior checking

1. Member States shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof.

2. Such prior checks shall be carried out by the supervisory authority following receipt of a notification from the controller or by the data protection official, who, in cases of doubt, must consult the supervisory authority.

3. Member States may also carry out such checks in the context of preparation either of a measure of the national parliament or of a measure based on such a legislative measure, which define the nature of the processing and lay down appropriate safeguards.

Article 21

Publicizing of processing operations

1. Member States shall take measures to ensure that processing operations are publicized.

2. Member States shall provide that a register of processing operations notified in

2. Member States shall provide that a register of processing operations notified in accordance with Article 18 shall be kept by the supervisory authority. The register shall contain at least the information listed in Article 19 (1) (a) to (e). The register may be inspected by any person.

3. Member States shall provide, in relation to processing operations not subject to notification, that controllers or another body appointed by the Member States make available at least the information referred to in Article 19 (1) (a) to (e) in an appropriate form to any person on request.

Member States may provide that this provision does not apply to processing whose sole purpose is the keeping of a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can provide proof of a legitimate interest.

CHAPTER III JUDICIAL REMEDIES, LIABILITY AND SANCTIONS

Article 22 Remedies

Without prejudice to any administrative remedy for which provision may be made, *inter alia* before the supervisory authority referred to in Article 28, prior to referral to the judicial authority, Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question.

Article 23 Liability

1. Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered.

2. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.

Article 24 Sanctions

The Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive.

CHAPTER IV TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

Article 25 Principles

1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

3. The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection

they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.

4. Where the Commission finds, under the procedure provided for in Article 31 (2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.

5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.

6. The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.

Member States shall take the measures necessary to comply with the Commission's decision.

Article 26

Derogations

1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on condition that:

(a) the data subject has given his consent unambiguously to the proposed transfer; or

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or

(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or

(e) the transfer is necessary in order to protect the vital interests of the data subject; or

(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

2. Without prejudice to paragraph 1, a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.

3. The Member State shall inform the Commission and the other Member States of the authorizations it grants pursuant to paragraph 2.

If a Member State or the Commission objects on justified grounds involving the protection of the privacy and fundamental rights and freedoms of individuals, the Commission shall take appropriate measures in accordance with the procedure laid down in Article 31 (2).

Member States shall take the necessary measures to comply with the Commission's decision.

Commission's decision.

4. Where the Commission decides, in accordance with the procedure referred to in Article 31 (2), that certain standard contractual clauses offer sufficient safeguards as required by paragraph 2, Member States shall take the necessary measures to comply with the Commission's decision.

CHAPTER V CODES OF CONDUCT

Article 27

1. The Member States and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to this Directive, taking account of the specific features of the various sectors.

2. Member States shall make provision for trade associations and other bodies representing other categories of controllers which have drawn up draft national codes or which have the intention of amending or extending existing national codes to be able to submit them to the opinion of the national authority. Member States shall make provision for this authority to ascertain, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives.

3. Draft Community codes, and amendments or extensions to existing Community codes, may be submitted to the Working Party referred to in Article 29. This Working Party shall determine, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives. The Commission may ensure appropriate publicity for the codes which have been approved by the Working Party.

CHAPTER VI SUPERVISORY AUTHORITY AND WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

Article 28

Supervisory authority

1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive.

These authorities shall act with complete independence in exercising the functions entrusted to them.

2. Each Member State shall provide that the supervisory authorities are consulted when drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data.

3. Each authority shall in particular be endowed with:

- investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties,
- effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions,
- the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated or to bring these violations to the attention of the judicial authorities.

Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts.

appealed against through the courts.

4. Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim.

Each supervisory authority shall, in particular, hear claims for checks on the lawfulness of data processing lodged by any person when the national provisions adopted pursuant to Article 13 of this Directive apply. The person shall at any rate be informed that a check has taken place.

5. Each supervisory authority shall draw up a report on its activities at regular intervals. The report shall be made public.

6. Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State. The supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.

7. Member States shall provide that the members and staff of the supervisory authority, even after their employment has ended, are to be subject to a duty of professional secrecy with regard to confidential information to which they have access.

Article 29

Working Party on the Protection of Individuals with regard to the Processing of Personal Data

1. A Working Party on the Protection of Individuals with regard to the Processing of Personal Data, hereinafter referred to as 'the Working Party', is hereby set up. It shall have advisory status and act independently.

2. The Working Party shall be composed of a representative of the supervisory authority or authorities designated by each Member State and of a representative of the authority or authorities established for the Community institutions and bodies, and of a representative of the Commission.

Each member of the Working Party shall be designated by the institution, authority or authorities which he represents. Where a Member State has designated more than one supervisory authority, they shall nominate a joint representative. The same shall apply to the authorities established for Community institutions and bodies.

3. The Working Party shall take decisions by a simple majority of the representatives of the supervisory authorities.

4. The Working Party shall elect its chairman. The chairman's term of office shall be two years. His appointment shall be renewable.

5. The Working Party's secretariat shall be provided by the Commission.

6. The Working Party shall adopt its own rules of procedure.

7. The Working Party shall consider items placed on its agenda by its chairman, either on his own initiative or at the request of a representative of the supervisory authorities or at the Commission's request.

Article 30

1. The Working Party shall:

(a) examine any question covering the application of the national measures adopted under this Directive in order to contribute to the uniform application of such measures;

(b) give the Commission an opinion on the level of protection in the Community and in third countries;

(c) advise the Commission on any proposed amendment of this Directive, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data and on any other proposed

persons with regard to the processing of personal data and on any other proposed Community measures affecting such rights and freedoms;

(d) give an opinion on codes of conduct drawn up at Community level.

2. If the Working Party finds that divergences likely to affect the equivalence of protection for persons with regard to the processing of personal data in the Community are arising between the laws or practices of Member States, it shall inform the Commission accordingly.

3. The Working Party may, on its own initiative, make recommendations on all matters relating to the protection of persons with regard to the processing of personal data in the Community.

4. The Working Party's opinions and recommendations shall be forwarded to the Commission and to the committee referred to in Article 31.

5. The Commission shall inform the Working Party of the action it has taken in response to its opinions and recommendations. It shall do so in a report which shall also be forwarded to the European Parliament and the Council. The report shall be made public.

6. The Working Party shall draw up an annual report on the situation regarding the protection of natural persons with regard to the processing of personal data in the Community and in third countries, which it shall transmit to the Commission, the European Parliament and the Council. The report shall be made public.

CHAPTER VII COMMUNITY IMPLEMENTING MEASURES

Article 31

The Committee

1. The Commission shall be assisted by a committee composed of the representatives of the Member States and chaired by the representative of the Commission.

2. The representative of the Commission shall submit to the committee a draft of the measures to be taken. The committee shall deliver its opinion on the draft within a time limit which the chairman may lay down according to the urgency of the matter.

The opinion shall be delivered by the majority laid down in Article 148 (2) of the Treaty. The votes of the representatives of the Member States within the committee shall be weighted in the manner set out in that Article. The chairman shall not vote.

The Commission shall adopt measures which shall apply immediately. However, if these measures are not in accordance with the opinion of the committee, they shall be communicated by the Commission to the Council forthwith. In that event:

- the Commission shall defer application of the measures which it has decided for a period of three months from the date of communication,
- the Council, acting by a qualified majority, may take a different decision within the time limit referred to in the first indent.

FINAL PROVISIONS

Article 32

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive at the latest at the end of a period of three years from the date of its adoption.

When Member States adopt these measures, they shall contain a reference to this Directive or be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by the Member States.

2. Member States shall ensure that processing already under way on the date the national provisions adopted pursuant to this Directive enter into force, is brought into conformity with these provisions within three years of this date.

By way of derogation from the preceding subparagraph, Member States may

By way of derogation from the preceding subparagraph, Member States may provide that the processing of data already held in manual filing systems on the date of entry into force of the national provisions adopted in implementation of this Directive shall be brought into conformity with Articles 6, 7 and 8 of this Directive within 12 years of the date on which it is adopted. Member States shall, however, grant the data subject the right to obtain, at his request and in particular at the time of exercising his right of access, the rectification, erasure or blocking of data which are incomplete, inaccurate or stored in a way incompatible with the legitimate purposes pursued by the controller.

3. By way of derogation from paragraph 2, Member States may provide, subject to suitable safeguards, that data kept for the sole purpose of historical research need not be brought into conformity with Articles 6, 7 and 8 of this Directive.

4. Member States shall communicate to the Commission the text of the provisions of domestic law which they adopt in the field covered by this Directive.

Article 33

The Commission shall report to the Council and the European Parliament at regular intervals, starting not later than three years after the date referred to in Article 32 (1), on the implementation of this Directive, attaching to its report, if necessary, suitable proposals for amendments. The report shall be made public. The Commission shall examine, in particular, the application of this Directive to the data processing of sound and image data relating to natural persons and shall submit any appropriate proposals which prove to be necessary, taking account of developments in information technology and in the light of the state of progress in the information society.

Article 34

This Directive is addressed to the Member States.

Done at Luxembourg, 24 October 1995.

For the European Parliament

The President

K. HAENSCH

For the Council

The President

L. ATIENZA SERNA

(1) OJ No C 277, 5. 11. 1990, p. 3 and OJ No C 311, 27. 11. 1992, p. 30.

(2) OJ No C 159, 17. 6. 1991, p. 38.

(3) Opinion of the European Parliament of 11 March 1992 (OJ No C 94, 13. 4. 1992, p. 198), confirmed on 2 December 1993 (OJ No C 342, 20. 12. 1993, p. 30); Council common position of 20 February 1995 (OJ No C 93, 13. 4. 1995, p. 1) and Decision of the European Parliament of 15 June 1995 (OJ No C 166, 3. 7. 1995).

(1) OJ No L 197, 18. 7. 1987, p. 33.



Managed b



Safe Harbor

Welcome

Safe Harbor
Overview

Safe Harbor
Documents

Safe Harbor
Workbook

Safe Harbor List

Certification
Information

Certification Form

Model Contract
Information

Data Privacy Links

Historical Documents
& Public Comments

Privacy Statements

Safe Harbor Overview

The European Commission's Directive on Data Protection went into effect in October, 1998, and would prohibit the transfer of personal data to non-European Union nations that do not meet the European "adequacy" standard for privacy protection. While the United States and the European Union share the goal of enhancing privacy protection for their citizens, the United States takes a different approach to privacy from that taken by the European Union. The United States uses a sectoral approach that relies on a mix of legislation, regulation, and self regulation. The European Union, however, relies on comprehensive legislation that, for example, requires creation of government data protection agencies, registration of data bases with those agencies, and in some instances prior approval before personal data processing may begin. As a result of these different privacy approaches, the Directive could have significantly hampered the ability of U.S. companies to engage in many trans-Atlantic transactions.

In order to bridge these different privacy approaches and provide a streamlined means for U.S. organizations to comply with the Directive, the U.S. Department of Commerce in consultation with the European Commission developed a "safe harbor" framework. The safe harbor -- approved by the EU this year -- is an important way for U.S. companies to avoid experiencing interruptions in their business dealings with the EU or facing prosecution by European authorities under European privacy laws. Certifying to the safe harbor will assure that EU organizations know that your company provides "adequate" privacy protection, as defined by the Directive.

SAFE HARBOR BENEFITS

The safe harbor provides a number of important benefits to U.S. and EU firms. Benefits for U.S. organizations participating in the safe harbor will include:

- All 15 Member States of the European Union will be bound by the European Commission's finding of adequacy
- Companies participating in the safe harbor will be deemed adequate and data flows to those companies will continue;
- Member State requirements for prior approval of data transfers either will be waived or approval will be automatically granted; and
- Claims brought by European citizens against U.S. companies will be heard in the U.S. subject to limited exceptions.

The safe harbor framework offers a simpler and cheaper means of complying with the adequacy requirements of the Directive, which should particularly benefit small and medium enterprises.

small and medium enterprises.

An EU organization can ensure that it is sending information to a U.S. organization participating in the safe harbor by viewing the public list of safe harbor organizations posted on the Department of Commerce's website (www.export.gov/safeharbor). This list will become operational at the beginning of November 2000. It will contain the names of all U.S. companies that have self-certified to the safe harbor framework. This list will be regularly updated, so that it is clear who is assured of safe harbor benefits.

HOW DOES AN ORGANIZATION JOIN?

The decision by U.S. organizations to enter the safe harbor is entirely voluntary. Organizations that decide to participate in the safe harbor must comply with the safe harbor's requirements and publicly declare that they do so. To be assured of safe harbor benefits, an organization needs to self certify annually to the Department of Commerce in writing that it agrees to adhere to the safe harbor's requirements, which includes elements such as notice, choice, access, and enforcement. It must also state in its published privacy policy statement that it adheres to the safe harbor. The Department of Commerce will maintain a list of all organizations that file self certification letters and make both the list and the self certification letters publicly available.

To qualify for the safe harbor, an organization can (1) join a self-regulatory privacy program that adheres to the safe harbor's requirements; or (2) develop its own self regulatory privacy policy that conforms to the safe harbor.

WHAT DO THE SAFE HARBOR PRINCIPLES REQUIRE?

Organizations must comply with the seven safe harbor principles. The principles require the following:

Notice: Organizations must notify individuals about the purposes for which they collect and use information about them. They must provide information about how individuals can contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information and the choices and means the organization offers for limiting its use and disclosure.

Choice: Organizations must give individuals the opportunity to choose (opt out) whether their personal information will be disclosed to a third party or used for a purpose incompatible with the purpose for which it was originally collected or subsequently authorized by the individual. For sensitive information, affirmative or explicit (opt in) choice must be given if the information is to be disclosed to a third party or used for a purpose other than its original purpose or the purpose authorized subsequently by the individual.

Onward Transfer (Transfers to Third Parties): To disclose information to a third party, organizations must apply the notice and choice principles. Where an organization wishes to transfer information to a third party that is acting as an agent(1), it may do so if it makes sure that the third party subscribes to the safe harbor principles or is subject to the Directive or another adequacy finding. As an alternative, the organization can enter into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant principles.

Access: Individuals must have access to personal information about them that an

Access: Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

Security: Organizations must take reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction.

Data integrity: Personal information must be relevant for the purposes for which it is to be used. An organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.

Enforcement: In order to ensure compliance with the safe harbor principles, there must be (a) readily available and affordable independent recourse mechanisms so that each individual's complaints and disputes can be investigated and resolved and damages awarded where the applicable law or private sector initiatives so provide; (b) procedures for verifying that the commitments companies make to adhere to the safe harbor principles have been implemented; and (c) obligations to remedy problems arising out of a failure to comply with the principles. Sanctions must be sufficiently rigorous to ensure compliance by the organization. Organizations that fail to provide annual self certification letters will no longer appear in the list of participants and safe harbor benefits will no longer be assured.

To provide further guidance, the Department of Commerce has issued a set of frequently asked questions and answers (FAQs) that clarify and supplement the safe harbor principles.

HOW AND WHERE WILL THE SAFE HARBOR BE ENFORCED?

In general, enforcement of the safe harbor will take place in the United States in accordance with U.S. law and will be carried out primarily by the private sector. Private sector self regulation and enforcement will be backed up as needed by government enforcement of the federal and state unfair and deceptive statutes. The effect of these statutes is to give an organization's safe harbor commitments the force of law vis a vis that organization.

Private Sector Enforcement: As part of their safe harbor obligations, organizations are required to have in place a dispute resolution system that will investigate and resolve individual complaints and disputes and procedures for verifying compliance. They are also required to remedy problems arising out of a failure to comply with the principles. Sanctions that dispute resolution bodies can apply must be severe enough to ensure compliance by the organization; they must include publicity for findings of non-compliance and deletion of data in certain circumstances. They may also include suspension from membership in a privacy program (and thus effectively suspension from the safe harbor) and injunctive orders.

The dispute resolution, verification, and remedy requirements can be satisfied in different ways. For example, an organization could comply with a private sector developed privacy seal program that incorporates and satisfies the safe harbor principles. If the seal program, however, only provides for dispute resolution and remedies but not verification, then the organization would have to satisfy the verification requirement in an alternative way.

Organizations can also satisfy the dispute resolution and remedy requirements

Organizations can also satisfy the dispute resolution and remedy requirements through compliance with government supervisory authorities or by committing to cooperate with data protection authorities located in Europe.

Government Enforcement: Depending on the industry sector, the Federal Trade Commission, comparable U.S. government agencies, and/or the states may provide overarching government enforcement of the safe harbor principles. Where a company relies in whole or in part on self regulation in complying with the safe harbor principles, its failure to comply with such self regulation must be actionable under federal or state law prohibiting unfair and deceptive acts or it is not eligible to join the safe harbor. At present, U.S. organizations that are subject to the jurisdiction of the Federal Trade Commission or the Department of Transportation with respect to air carriers and ticket agents may participate in the safe harbor. The Federal Trade Commission and the Department of Transportation with respect to air carriers and ticket agents have both stated in letters to the European Commission that they will take enforcement action against organizations that state that they are in compliance with the safe harbor framework but then fail to live up to their statements.

Under the Federal Trade Commission Act, for example, a company's failure to abide by commitments to implement the safe harbor principles might be considered deceptive and actionable by the Federal Trade Commission. This is the case even where an organization adhering to the safe harbor principles relies entirely on self-regulation to provide the enforcement required by the safe harbor enforcement principle. The FTC has the power to rectify such misrepresentations by seeking administrative orders and civil penalties of up to \$12,000 per day for violations.

Failure to Comply with the Safe Harbor Requirements: If an organization persistently fails to comply with the safe harbor requirements, it is no longer entitled to benefit from the safe harbor. Persistent failure to comply arises where an organization refuses to comply with a final determination by any self regulatory or government body or where such a body determines that an organization frequently fails to comply with the requirements to the point where its claim to comply is no longer credible. In these cases, the organization must promptly notify the Department of Commerce of such facts. Failure to do so may be actionable under the False Statements Act (18 U.S.C. § 1001).

The Department of Commerce will indicate on the public list it maintains of organizations self certifying adherence to the safe harbor requirements any notification it receives of persistent failure to comply and will make clear which organizations are assured and which organizations are no longer assured of safe harbor benefits.

An organization applying to participate in a self-regulatory body for the purposes of re-qualifying for the safe harbor must provide that body with full information about its prior participation in the safe harbor.

II

(Acts whose publication is not obligatory)

COMMISSION

COMMISSION DECISION

of 27 December 2001

on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC

(notified under document number C(2001) 4540)

(Text with EEA relevance)

(2002/16/EC)

THE COMMISSION OF THE EUROPEAN COMMUNITIES,

Having regard to the Treaty establishing the European Community,

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ⁽¹⁾, and in particular Article 26(4) thereof,

Whereas:

- (1) Pursuant to Directive 95/46/EC Member States are required to provide that a transfer of personal data to a third country may only take place if the third country in question ensures an adequate level of data protection and the Member States' laws, which comply with the other provisions of the Directive, are respected prior to the transfer.
- (2) However, Article 26(2) of Directive 95/46/EC provides that Member States may authorise, subject to certain safeguards, a transfer or a set of transfers of personal data to third countries which do not ensure an adequate level of protection. Such safeguards may in particular result from appropriate contractual clauses.
- (3) Pursuant to Directive 95/46/EC the level of data protection should be assessed in the light of all the circumstances surrounding the data transfer operation or set of data transfer operations. The Working Party on the Protection of Individuals with regard to the Processing of Personal Data established under that Directive ⁽²⁾ has issued guidelines to aid with the assessment ⁽³⁾.

⁽¹⁾ OJ L 281, 23.11.1995, p. 31.

⁽²⁾ The web address of the Working Party is:

http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index.htm.

⁽³⁾ **WP 4 (5020/97)**: First orientations on Transfers of Personal Data to Third Countries — Possible Ways Forward in Assessing Adequacy, a discussion document adopted by the Working Party on 26 June 1997.

WP 7 (5057/97): Working document: Judging industry self-regulation: when does it make a meaningful contribution to the level of data protection in a third country?, adopted by the Working Party on 14 January 1998.

WP 9 (5005/98): Working Document: Preliminary views on the use of contractual provisions in the context of transfers of personal data to third countries, adopted by the Working Party on 22 April 1998.

WP 12: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive, adopted by the Working Party on 24 July 1998, available on the website

http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp12en.htm hosted by the European Commission.

- (4) The standard contractual clauses relate only to data protection. The data exporter and the data importer are free to include any other clauses on business related issues which they consider as being pertinent for the contract as long as they do not contradict the standard contractual clauses.
- (5) This Decision should be without prejudice to national authorisations Member States may grant in accordance with national provisions implementing Article 26(2) of Directive 95/46/EC. This Decision only has the effect of requiring the Member States not to refuse to recognise as providing adequate safeguards the contractual clauses set out in it and does not therefore have any effect on other contractual clauses.
- (6) The scope of this Decision is limited to establishing that the clauses which it sets out may be used by a data controller established in the Community in order to adduce adequate safeguards within the meaning of Article 26(2) of Directive 95/46/EC for the transfer of personal data to a processor established in a third country.
- (7) This Decision should implement the obligation provided for in Article 17(3) of Directive 95/46/EC and does not prejudice the content of the contracts or legal acts established pursuant to that provision. However, some of the standard contractual clauses, in particular as regards the data exporter's obligations, should be included in order to increase clarity as to the provisions which may be contained in a contract between a controller and a processor.
- (8) Supervisory authorities of the Member States play a key role in this contractual mechanism in ensuring that personal data are adequately protected after the transfer. In exceptional cases where data exporters refuse or are unable to instruct the data importer properly, with an imminent risk of grave harm to the data subjects, the standard contractual clauses should allow the supervisory authorities to audit data importers and, where appropriate, take decisions which are binding on data importers. The supervisory authorities should have the power to prohibit or suspend a data transfer or a set of transfers based on the standard contractual clauses in those exceptional cases where it is established that a transfer on contractual basis is likely to have a substantial adverse effect on the warranties and obligations providing adequate protection for the data subject.
- (9) The Commission may also consider in the future whether standard contractual clauses for the transfer of personal data to data processors established in third countries not offering an adequate level of data protection, submitted by business organisations or other interested parties, offer adequate safeguards in accordance with Article 26(2) of Directive 95/46/EC.
- (10) A disclosure of personal data to a data processor established outside the Community is an international transfer protected under Chapter IV of Directive 95/46/EC. Consequently, this Decision does not cover the transfer of personal data by controllers established in the Community to controllers established outside the Community who fall within the scope of Commission Decision 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC ⁽¹⁾.
- (11) The standard contractual clauses should provide for the technical and organisational security measures ensuring a level of security appropriate to the risks represented by the processing and the nature of the data to be protected that a data processor established in a third country not providing adequate protection must apply. Parties should make provision in the contract for those technical and organisational measures which, having regard to applicable data protection law, the state of the art and the cost of their implementation, are necessary in order to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access or any other unlawful forms of processing.
- (12) In order to facilitate data flows from the Community, it is desirable that processors providing data processing services to several data controllers in the Community be allowed to apply the same technical and organisational security measures irrespective of the Member State from which the data transfer originates, in particular in those cases where the data importer receives data for further processing from different establishments of the data exporter in the Community, in which case the law of the designated Member State of establishment should apply.

⁽¹⁾ OJ L 181, 4.7.2001, p. 19.

- (13) It is appropriate to lay down the minimum information that the parties must specify in the contract dealing with the transfer. Member States should retain the power to particularise the information the parties are required to provide. The operation of this Decision should be reviewed in the light of experience.
- (14) The data importer should process the transferred personal data only on behalf of the data exporter and in accordance with his instructions and the obligations contained in the clauses. In particular the data importer should not disclose the personal data to a third party unless in accordance with certain conditions. The data exporter should instruct the data importer throughout the duration of the data processing Services to process the data in accordance with his instructions, the applicable data protection laws and the obligations contained in the clauses. The transfer of personal data to processors established outside the Community does not prejudice the fact that the processing activities should be governed in any case by the applicable data protection law.
- (15) The standard contractual clauses should be enforceable not only by the organisations which are parties to the contract, but also by the data subjects, in particular where the data subjects suffer damage as a consequence of a breach of the contract.
- (16) The data subject should be entitled to take action and, where appropriate, receive compensation from the data exporter who is the data controller of the personal data transferred. Exceptionally, the data subject should also be entitled to take action, and, where appropriate, receive compensation from the data importer in those cases, arising out of a breach by the data importer of any of his obligations referred to in the second paragraph of clause 3, where the data exporter has factually disappeared or has ceased to exist in law or has become insolvent.
- (17) In the event of a dispute between a data subject, who invokes the third-party beneficiary clause and the data importer, which is not amicably resolved, the data importer should agree to provide the data subject with the choice between mediation, arbitration or litigation. The extent to which the data subject will have an effective choice should depend on the availability of reliable and recognised systems of mediation and arbitration. Mediation by the data protection supervisory authorities of the Member State in which the data exporter is established should be an option where they provide such a service.
- (18) The contract should be governed by the law of the Member State in which the data exporter is established enabling a third-party beneficiary to enforce a contract. Data subjects should be allowed to be represented by associations or other bodies if they so wish and if authorised by national law.
- (19) The Working Party on the Protection of Individuals with regard to the processing of Personal Data established under Article 29 of Directive 95/46/EC has delivered an opinion on the level of protection provided under the standard contractual clauses annexed to this Decision, which has been taken into account in the preparation of this Decision⁽¹⁾.
- (20) The measures provided for in this Decision are in accordance with the opinion of the Committee established under Article 31 of Directive 95/46/EC,

HAS ADOPTED THIS DECISION:

Article 1

The standard contractual clauses set out in the Annex are considered as offering adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights as required by Article 26(2) of Directive 95/46/EC.

⁽¹⁾ Opinion No 7/2001 adopted by the Working Party on 13 September 2001 (DG MARKT...), available on the website 'Europa' hosted by the European Commission.

Article 2

This Decision concerns only the adequacy of protection provided by the standard contractual clauses set out in the Annex for the transfer of personal data to processors. It does not affect the application of other national provisions implementing Directive 95/46/EC that pertain to the processing of personal data within the Member States.

This Decision shall apply to the transfer of personal data by controllers established in the Community to recipients established outside the territory of the Community who act only as processors.

Article 3

For the purposes of this Decision:

- (a) the definitions in Directive 95/46/EC shall apply;
- (b) 'special categories of data' means the data referred to in Article 8 of that Directive;
- (c) 'supervisory authority' means the authority referred to in Article 28 of that Directive;
- (d) 'data exporter' means the controller who transfers the personal data;
- (e) 'data importer' means the processor established in a third country who agrees to receive from the data exporter personal data intended for processing on the data exporter's behalf after the transfer in accordance with his instructions and the terms of this Decision and who is not subject to a third country's system ensuring adequate protection;
- (f) 'applicable data protection law' means the legislation protecting the fundamental rights and freedoms of natural persons and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
- (g) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Article 4

1. Without prejudice to their powers to take action to ensure compliance with national provisions adopted pursuant to Chapters II, III, V and VI of Directive 95/46/EC, the competent authorities in the Member States may exercise their existing powers to prohibit or suspend data flows to third countries in order to protect individuals with regard to the processing of their personal data in cases where:

- (a) it is established that the law to which the data importer is subject imposes upon him requirements to derogate from the applicable data protection law which go beyond the restrictions necessary in a democratic society as provided for in Article 13 of Directive 95/46/EC where those requirements are likely to have a substantial adverse effect on the guarantees provided by the applicable data protection law and the standard contractual clauses; or
- (b) a competent authority has established that the data importer has not respected the contractual clauses in the Annex; or
- (c) there is a substantial likelihood that the standard contractual clauses in the Annex are not being or will not be complied with and the continuing transfer would create an imminent risk of grave harm to the data subjects.

2. The prohibition or suspension pursuant to paragraph 1 shall be lifted as soon as the reasons for the suspension or prohibition no longer exist.

3. When Member States adopt measures pursuant to paragraphs 1 and 2, they shall, without delay, inform the Commission which will forward the information to the other Member States.

Article 5

The Commission shall evaluate the operation of this Decision on the basis of available information three years after its notification to the Member States. It shall submit a report on the findings to the Committee established under Article 31 of Directive 95/46/EC. It shall include any evidence that could affect the evaluation concerning the adequacy of the standard contractual clauses in the Annex and any evidence that this Decision is being applied in a discriminatory way.

Article 6

This Decision shall apply from 3 April 2002.

Article 7

This Decision is addressed to the Member States.

Done at Brussels, 27 December 2001.

For the Commission
Frederik BOLKESTEIN
Member of the Commission

ANNEX

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation:

address

.....

tel.:; fax:; e-mail:

Other information needed to identify the organisation

.....

(the data exporter)

and

Name of the data importing organisation:

address

.....

tel.:; fax:; e-mail:

Other information needed to identify the organisation:

.....

(the data importer)

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

*Clause 1***Definitions**

For the purposes of the Clauses:

- (a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the Directive) (1);
- (b) 'the data exporter' shall mean the controller who transfers the personal data;
- (c) 'the data importer' shall mean the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of these Clauses and who is not subject to a third country's system ensuring to adequate protection;
- (d) 'the applicable data protection law' shall mean the legislation protecting the fundamental rights and freedoms of natural persons and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
- (e) 'technical and organisational security measures' shall mean those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

*Clause 2***Details of the transfer**

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

(1) Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

Clause 3

Third-party beneficiary clause

The data subject can enforce against the data exporter this Clause, Clause 4(b) to (h), Clause 5(a) to (c), and (g), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9, 10 and 11, as third-party beneficiaries.

The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9, 10 and 11, in cases where the data exporter has factually disappeared or has ceased to exist in law.

The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

- (a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
- (b) that he has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and these clauses;
- (c) that the data importer shall provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
- (d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
- (e) that he will ensure compliance with the security measures;
- (f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that his data could be transmitted to a third country not providing adequate protection;
- (g) that he agrees to forward the notification received from the data importer pursuant to Clause 5(b) to the data protection supervisory authority if he decides to continue the transfer or to lift his suspension;
- (h) to make available to the data subjects upon request a copy of the Clauses set out in this Annex, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures.

Clause 5

Obligations of the data importer ⁽¹⁾

The data importer agrees and warrants:

- (a) to process the personal data only on behalf of the data exporter and in compliance with his instructions and the clauses; if he cannot provide such compliance for whatever reasons, he agrees to inform promptly the data exporter of his inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (b) that he has no reason to believe that the legislation applicable to him prevents him from fulfilling the instructions received from the data exporter and his obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, he will promptly notify the change to the data exporter as soon as he is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (c) that he has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

⁽¹⁾ Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia*, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

- (d) that he shall promptly notify the data exporter about:
- (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;
 - (ii) any accidental or unauthorised access; and
 - (iii) any request received directly from the data subjects without responding to that request, unless he has been otherwise authorised to do so;
- (e) to deal promptly and properly with all inquiries from the data exporter relating to his processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
- (f) at the request of the data exporter to submit his data processing facilities for audit of the processing activities covered by the clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
- (g) to make available to the data subject upon request a copy of the Clauses set out in this Annex, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter.

Clause 6

Liability

1. The parties agree that a data subject, who has suffered damage as a result of any violation of the provisions referred to in Clause 3 is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring the action referred to in paragraph 1 arising out of a breach by the data importer of any of his obligations referred to in Clause 3 against the data exporter because the data exporter has disappeared factually or has ceased to exist in law or became insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if he were the data exporter.

3. The parties agree that if one party is held liable for a violation of the clauses committed by the other party, the latter will, to the extent to which it is liable, indemnify the first party for any cost, charge, damages, expenses or loss it has incurred.

Indemnification is contingent upon:

- (a) the data exporter promptly notifying the data importer of a claim; and
- (b) the data importer being given the possibility to cooperate with the data exporter in the defence and settlement of the claim ⁽¹⁾.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against him third-party beneficiary rights and/or claims compensation for damages under the clauses, the data importer will accept the decision of the data subject:

- (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
- (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The data importer agrees that, by agreement with the data subject, the resolution of a specific dispute can be referred to an arbitration body if the data importer is established in a country which has ratified the New York Convention on enforcement of arbitration awards.

3. The parties agree that the choice made by the data subject will not prejudice his substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

⁽¹⁾ Paragraph 3 is optional.

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely.....

Clause 10

Variation of the contract

The parties undertake not to vary or modify the terms of the Clauses.

Clause 11

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer shall, at the choice of the data exporter, return al the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that he has done so, unless legislation imposed upon the data importer prevents him from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that he will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer warrants that upon request of the data exporter and/or of the supervisory authority, hc will submit his data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

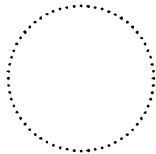
Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature



(stamp of organisation)

On behalf of the data importer:

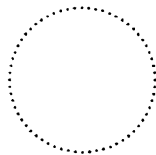
Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature



(stamp of organisation)

Appendix 1

to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties

(* The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix)

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

.....
.....
.....

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

.....
.....
.....

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

.....
.....
.....

Categories of data

The personal data transferred concern the following categories of data (please specify):

.....
.....
.....

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

.....
.....
.....

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

.....
.....
.....

DATA EXPORTER

DATA IMPORTER

Name:

Authorised signature

.....

Appendix 2

to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

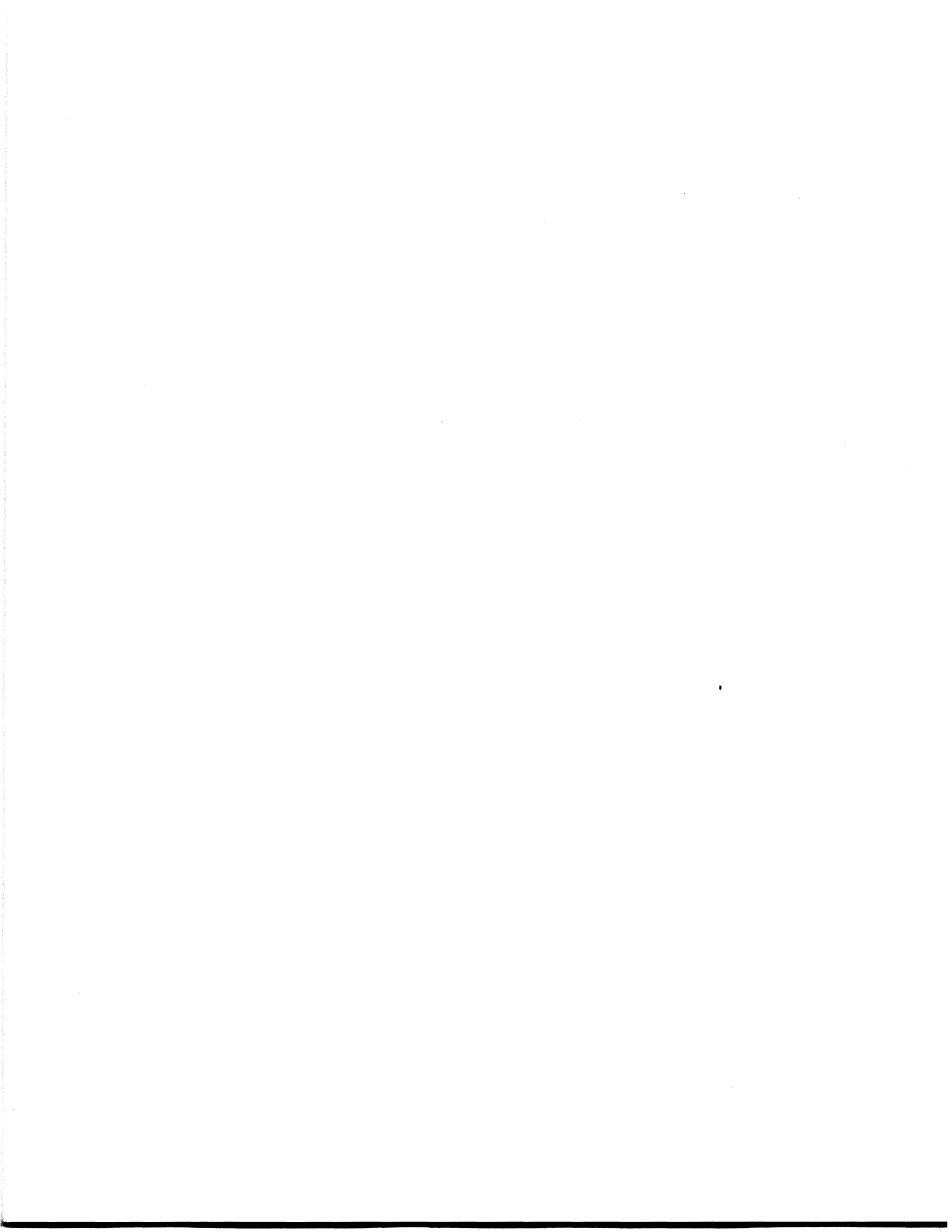
.....
.....
.....
.....

CYBER LANGUAGE:
**A FIELD GUIDE TO THE LAW OF SPIDERS,
BOTS, NETCRAWLERS AND
OTHER CYBER CRITTERS**

Kurt X. Metzmeier
Associate Director
Louis D. Brandeis School of Law Library
University of Louisville
Louisville, Kentucky

Copyright 2002, Kurt X. Metzmeier

SECTION K



CYBER LANGUAGE:
**A FIELD GUIDE TO THE LAW OF
SPIDERS, BOTS, NETCRAWLERS AND
OTHER CYBER CRITTERS**

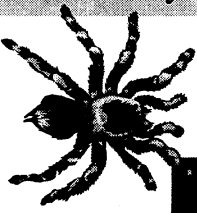
*Kurt X. Metzmeier
Associate Director
Louis D. Brandeis School of Law Library
University of Louisville
Louisville, Kentucky*

Table of Contents

| | | |
|-------------|---|------------|
| I. | Spiders, Bots and Netcrawlers..... | K-1 |
| A. | Good Bugs..... | K-1 |
| B. | Webcrawling..... | K-2 |
| C. | Robot Exclusion File..... | K-2 |
| D. | Bad Bugs..... | K-3 |
| II. | Hackers, Crackers, Lamers and Script Kiddies.... | K-3 |
| A. | Hackers v. Crackers | K-4 |
| 1. | Exploits | K-4 |
| a. | Root..... | K-4 |
| B. | Script Kiddies..... | K-5 |
| C. | War Scripts..... | K-5 |
| D. | Hactivism | K-5 |
| III. | Zombies, Worms and Hack Attacks..... | K-6 |
| A. | Zombies, Worms, Hack Attacks, Smurfing, Dos..... | K-6 |
| 1. | Ping of Death | K-7 |
| 2. | Denial of Service Attacks | K-7 |
| 3. | Distributed Denial of Service Attack..... | K-8 |
| B. | Daemons and Zombies..... | K-8 |
| C. | Hack Attacks..... | K-9 |
| D. | Example of Daemons and Zombie Attack..... | K-9 |
| E. | Hack Attack of 1998 | K-10 |

| | | |
|------------|---|-------------|
| F. | Webworms | K-11 |
| G. | WareZ & Cracks | K-11 |
| H. | Demos and Negware | K-11 |
| IV. | Spoofs, SpyWare & Spam | K-12 |
| A. | Spoof..... | K-12 |
| B. | SpyWare..... | K-12 |
| V. | Bibliography..... | K-13 |

CyberLanguage:
A Field Guide to the Law of
Spiders, Bots, Netcrawlers
and other Cyber Critters




**Spiders, Bots, and
Netcrawlers**

- Spiders, robots (or bots) and netcrawlers are all names for programs that systematically search pages on the web, building indexes of information about these pages

Good Bugs

- The most common species of spider are those that index the web for search engines.
- These beneficial bugs help us find things and cause no harm



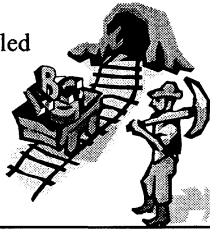
Webcrawling

- When you typing a query into a search engine and hit enter, you do not “search the web,” at least in real-time
- Rather you search a database of web information, keyed to web addresses

| | A | B | C | D |
|---|------------------------|---------|--|----------------|
| 1 | Title | Address | Keywords | Text |
| 2 | University of Kentucky | uky.edu | university,kentucky,education,academic | Welcome to th |
| 3 | University of Kentucky | :Law | college,law,admissions,legal,research | College of Law |
| 6 | University of Kentucky | :CLE | CLE,continuing,legal,education,publ | at CLE |

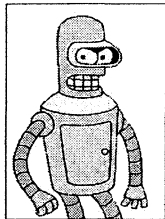
Good Bugs

- Other spiders travel the web looking for specific types of data
- This of activity is called *data-mining*



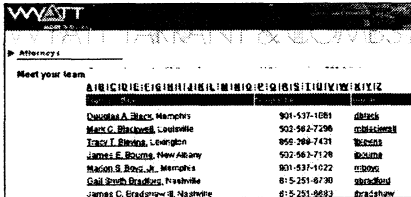
Robot Exclusion File

- *robots.txt*
- well-behaved web crawlers are supposed to look at this file to determine what **not** to index.



Bad Bugs

- Less beneficial robots crawl the web collecting email addresses for to sale to email marketers (spammers)



WVATT
ATTORNEYS AT LAW
ATTORNEY FIRM AND SERVICES

Meet your team

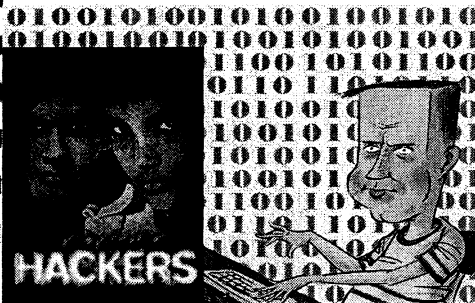
| Attorney | Phone | Area |
|-------------------------------|--------------|--------------|
| Dorinda A. Black, Memphis | 901-537-1001 | CRIMINAL |
| Mark C. Blackwell, Louisville | 502-563-7200 | CIVIL RIGHTS |
| Ernie J. Blanton, Lexington | 956-266-7431 | CRIMINAL |
| James E. Brouss, New Albany | 502-563-7129 | CRIMINAL |
| Madison S. Boyd, Jr., Memphis | 901-537-1022 | CRIMINAL |
| Carl Steph Brantley, Franklin | 615-251-8730 | CRIMINAL |
| James G. Brantley, Memphis | 901-537-8683 | CRIMINAL |

Bad Bugs

- Others search for copyrighted images, sound and video files, to copy them for infringing commercial uses
- *Napster and second generation peer-to-peer networks both use bots*



Hackers, Crackers, Lamers & Script Kiddies



Hackers v. Crackers

- hacker (hak'er)
- *n.* 1. *Slang.* Computer programmer
- 2. An individual who probes and logs on to remote computers without permission for the purpose of learning, entertainment and perhaps abuse.
- *Cf. Cracker.* A hacker with intent to harm or profit. *Usage:* "Good" hackers call "bad" hackers, crackers

Exploits

- A "exploit" is a successful "hack" worthy of bragging about
- Examples include hacking into the CIA website, knocking down a Microsoft router, etc

Root

- The goal of most exploits is to gain control of "root," the highest level of security in Unix/Linux systems.

By controlling root the hacker has complete control of a computer, or in the case of servers, the entire network



Script Kiddies

- Script Kiddie *n.* A beginner hacker, usually a juvenile, who is only capable of using simple guides, like the *Jolly Roger Cookbook*, or pre-written programs called *scripts* or *war scripts*.
- See also Lamer



War Scripts

- Pre-written hacking tools. Examples include:
 - Back Orifice -- tool for hacking Microsoft networks
 - Tribe Flood Net, trin00, Barbed Wire, etc. -- tool for knocking down web sites
- Sometimes called Warz

Hacktivism

- *n.* The use of hacker skills in the pursuit of political goals.
 - Domestic targets are often forces attending to limit Internet liberty.
 - Groups like cDc have provided war scripts to dissident hacker groups in foreign nations, esp. China. Reportedly, cDc has sent 5,000 copies of Back Orifice to Chinese dissidents.

Hacktivism

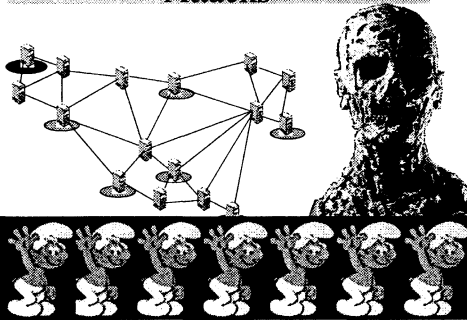
Cult of the Dead Cow (cDc) website:

- <http://www.cultdeadcow.com/>

Hacktivism website

- <http://hacktivism.com/>
- This is the website of cDc foreign minister Oxblood Ruffin

Zombies, Worms, and Hack Attacks



Zombies, Worms, Hack Attacks, Smurfing, DoS ...

- All terms related to various cracker exploits, both sophisticated and juvenile
- All designed to damage or degrade Internet service by target
- ... or the Internet itself

Ping of Death


- Hacker uses a program to send rapid stream of information (arranged in packets) to a server in the hopes of shutting is down
- Most current network security can defeat this attack
- Common script-kiddie exploit

Denial Of Service Attacks

- Hacker uses a program or script to send stream of misshapen packets to a server
- The server frantically tries to sort out the nonconforming packets, but eventually gets bogged down and either slows down or crashes

Denial of Service Attacks

- Otherwise known as a “smurf attack” or smurfing

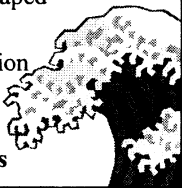


Denial of Service Attacks

- Scripts are easily found on the web & make this the amateur hackers AKA “script kiddies” weapon of choice
 - Tribe Flood Net
 - trin00
 - Stacheldraht (Barbed Wire)

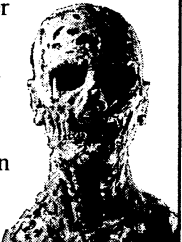
Distributed Denial of Service Attack

- The Big Kahuna of DoS attacks
- The target web site is bombarded by **multiple** computers with a steady stream of mis-shaped packets
- More sophisticated version of the simple denial of service attack
- Attack employs **zombies**



Daemons and Zombies

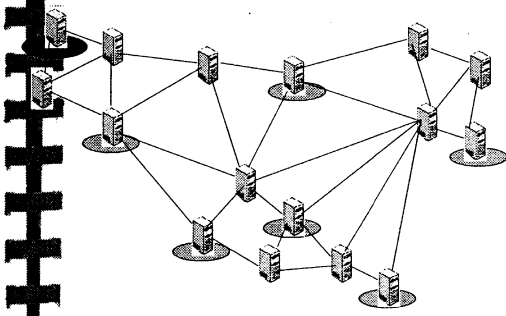
- A daemon is any Internet program that works in the background on a computer attached to the web
 - Can be any computer from a PC to a router to a server
- A zombie is an illegally installed daemon that is in the control of the hacker who installed it



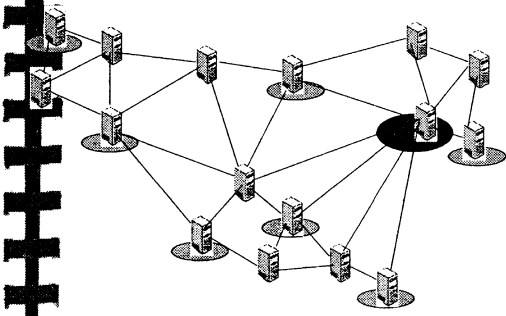
Hack Attack

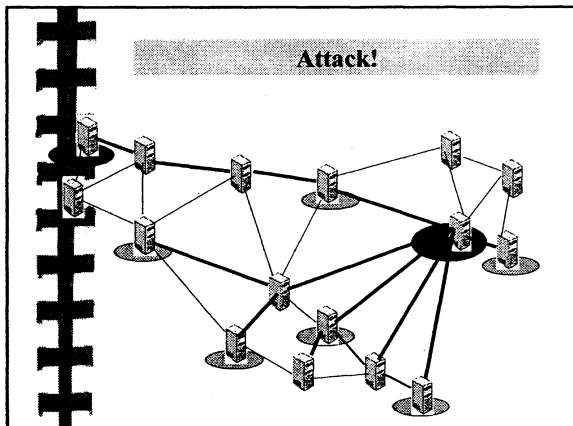
- The attackers must careful plant deamon/zombies around the web, loaded with the DoD service software
- The “general” then sends a message with the target site to the zombies, and order it to execute its program

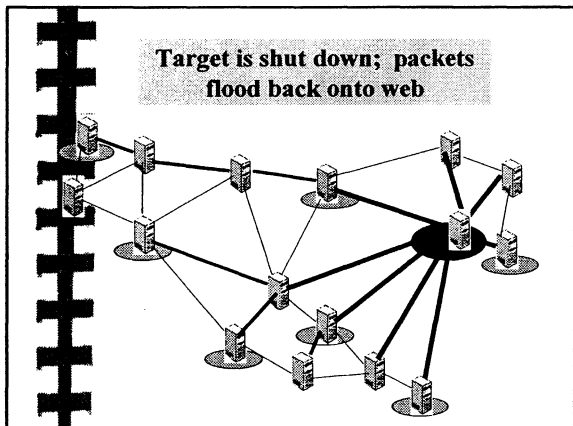
Daemons & Zombies



Target Established...







- Hack Attack of 1998**
- Monday 2-7 -- Yahoo! 3 hours
 - Tuesday 2-8 --
 - 11am PST Buy.com (on IPO day)
 - 1230pm PST stamps.com
 - 330pm PST e-bay (5.5 hours)
 - 4pm PST cnn.com (2 hrs)
 - 5pm PST amazon.com (1hr)
 - 6pm PST MSN
 - Weds 2-9
 - 430am PST ZDNet (2hrs)
 - 5am PST (E*Trade (1hr)

Web Worms

- **Worm** *n.* A program that replicates itself over a computer network, using up its resources and possibly shutting it down.
- Type of virus
- Code Red (2001), BugBear (2002)

Warez & Cracks

- **Warez** (*wârz*) *n.* Illegally traded software; usually exchanged through chat rooms and temporarily erected FTP sites on public PCs (usually in university labs or libraries).
- **Cracks** *n.* Programs designed defeat copyright protection of software

Demos & Negware

- **Demos** are demonstration versions of programs usually designed to become inoperative after a period of use (30 days; 50 uses, etc)
- **Nagware** is slang for shareware; programs that are usable but the author has for payment on the honor system
- Both are common **warez**, packaged with **cracks** to make them full-use versions

Spoofs, Spyware & Spam

- Spam n. unsolicited commercial email
- Some related issues:
 - Spoofs, spoofing
 - SpyWare



Spoof

- Spoof v. To trick a computer or user into believing something is not what it appears to be.
 - **IP Spoofing.** When a hacker tricks steals the identify of a web router to intercept traffic
 - **Email spoofing.** Common trick used by spammers to hide the origin of the emailer

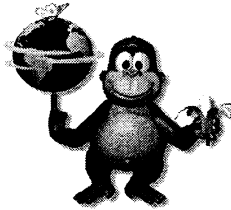
SpyWare

- Software that secretly tracks your Internet traffic and or/ the software on your system, continuously "calling home", reporting data to the software company
- Usually freeware with a useful function
- Often you opt into this extra "feature" with a click-thru license.



SpyWare

- Bonzi products (BonziBUDDY, Internet BOOST, Voice E-Mail, etc).
- Comet Cursor



Bibliography

- Webopedia
<http://www.webopedia.com/>
- NetLingo
<http://www.netlingo.com/>
- The New Hacker's Dictionary
<http://www.tuxedo.org/~esr/jargon/>
and many other places



**UPDATE ON DOMAIN NAME DISPUTES
AND NEW TLDS**

*Joseph R. Dreitler
Jones Day Reavis & Pogue
Columbus, Ohio*

Copyright 2002, Joseph R. Dreitler

SECTION L



UPDATE ON DOMAIN NAME DISPUTES AND NEW TLD'S

*Joseph R. Dreitler
Jones Day Reavis & Pogue
Columbus, Ohio*

Table of Contents

| | | |
|--------------|--|------------|
| I. | History of Domain Names and their Administration... | L-1 |
| II. | Regulation of Trademark Rights in Domain Names..... | L-1 |
| III. | How Cybersquatters Can Harm IP..... | L-1 |
| IV. | Substantive Grounds to Challenge in U.S..... | L-1 |
| | A. Trademark Infringement (15 U.S.C. § 1114)..... | L-2 |
| | B. Trademark Dilution (15 U.S.C. § 1125(c))..... | L-2 |
| | C. Lanham Act Section 43(a) (15 U.S.C. § 1125(a)) | L-2 |
| | D. Anticybersquatter Consumer Protection Act (15 U.S.C. § 1125(d)) | L-2 |
| | E. State Law | L-3 |
| V. | ICANN UDRP “Arbitration”..... | L-3 |
| VI. | Procedural Options..... | L-3 |
| | A. U.S. Litigation..... | L-3 |
| | B. Foreign Litigation | L-3 |
| VII. | Misdirection Websites... .. | L-4 |
| | A. “Typo” Squatters..... | L-4 |
| | B. Metatag Pirates..... | L-4 |
| | C. Unsavory Sites | L-4 |
| | D. Finding the Bad Guys | L-5 |
| VIII. | Search Methods..... | L-5 |
| IX. | How to Stop the Cybersquatters..... | L-5 |
| X. | Strategic Goals for Trademark Protection..... | L-5 |

| | | |
|--------------|--|------------|
| XI. | Recommended Procedures | L-5 |
| XII. | Questionably Actionable Sites | L-6 |
| XIII. | Flagrant Misuses: Terminate with Prejudice | L-6 |
| XIV. | Relevant Cases | L-6 |
| A. | <i>Hasbro, Inc. v. Internet Entertainment Group, Ltd.</i> , 40 USPQ2d 1479, 1996 U.S. Dist. LEXIS 11626 (W.D. Wash. 1996) | L-6 |
| B. | <i>Intermatic v. Toeppen</i> , 947 F. Supp. 1227 (N.D. Ill. 1996)..... | L-6 |
| C. | <i>Cardservice Int'l v. McGee</i> , 950 F. Supp. 737, (E.D. Va.), <i>aff'd</i> , 129 F.3d 1258 (4th Cir. 1997) | L-6 |
| D. | <i>Jews for Jesus v. Brodsky</i> , 993 F. Supp. 282 (D. N.J. 1998)..... | L-6 |
| E. | <i>Planned Parenthood Fed'n of America v. Bucci</i> , 1997 U.S. Dist. LEXIS 3338, 42 USPQ2d 1430 (S.D.N.Y. 1997) <i>aff'd</i> , 152 F.3d 920 (2d Cir. 1998), cert. denied, 119 S. Ct. 90 (1998)..... | L-7 |
| F. | <i>Playboy Enters, Inc. v. Welles</i> , 7 F. Supp. 2d 1098 (C.D. Cal 1997), <i>aff'd without op.</i> , 162 F.3d 1169 (9th Cir. 1998)..... | L-7 |
| G. | <i>Niton Corp. v. Radiation Monitoring Devices, Inc.</i> , 27 F. Supp. 2d 102 (D. Mass. 1998)..... | L-7 |
| H. | <i>Brookfield Communications, Inc., West Coast Entertainment Corporation</i> , 174 F.3d 1036 (9 th Cir. 1999)..... | L-7 |
| I. | <i>Promatek Industries, Ltd. v. Equitrac Corporation</i> , 300 F.3d 808 (7 th Cir. 2002)..... | L-7 |
| J. | <i>Playboy Enterprises Inc. v. Netscape Communications Corp.</i> , 55 F. Supp. 2d 1070, 1090 (C.D. Cal. 1999) | L-7 |
| K. | <i>Hasbro Inc. v. Clue Computing Inc.</i> 994 F. Supp. 34, (D. Mass. 1997), <i>aff'd</i> 232 F.3d 1 (1 st Cir. 2000)..... | L-7 |
| L. | <i>The Network Network v. CBS, Inc.</i> , 2000 WL 362016, 54 USPQ2d 1150 (C.D. Cal. 2000)..... | L-7 |
| M. | <i>Estee Lauder Inc. v. Fragrance Counter</i> , 1999 U.S. Dist. LEXIS 14825, 52 USPQ2d 1786, No. 99-CV-382 (S.D.N.Y.)..... | L-7 |
| N. | <i>Sporty's Farm v Sportsman's Market</i> , 202 F.3d 489, (2d Cir. 2000)..... | L-8 |
| O. | <i>Lucent Technologies Inc. v. lucentucks.com</i> , 95 F. Supp. 2d 528 (E.D. Va. 2000)..... | L-8 |
| P. | <i>Barcelona.com Inc. v. Excelentisimo Ayuntamiento de Barcelona</i> , 63 USPQ2d 1189 (E.D. Va. 2002)..... | L-8 |
| Q. | <i>America Online Inc. v. Huang</i> 106 F. Supp. 2d 848, 855-60 (E.D. Va. 2000)..... | L-8 |
| R. | <i>Ford Motor Co. v. Ford Financial Solutions Inc.</i> , 103 F. Supp. 2d 1126 (N.D. Iowa 2000)..... | L-8 |
| S. | <i>Bancroft & Masters Inc. v. Augusta National, Inc.</i> , 223 F.3d 1082 (9th Cir. 2000)..... | L-8 |
| T. | <i>Bird v. Parsons</i> , 62 USPQ2d 1905, 2002 FED App. 0177P (6th Cir. 2002)..... | L-8 |

| | | |
|------------|--|-------------|
| U. | <i>Heathmount A.E. Corp. v. technodome.com</i> , 106 F. Supp. 2d 860, 865-66 (E.D. Va. 2000)..... | L-8 |
| V. | <i>Shields v. Zuccarini</i> , 89 F. Supp. 2d 634 (E.D. Pa. 2000), <i>aff'd</i> No. 00-2236 (3rd Cir. 2001) | L-8 |
| W. | <i>Electronics Boutique Holdings Corp. v. Zuccarini</i> , 2000 U.S. Dist. LEXIS 15719, 56 USPQ2d 1705 (E.D. Pa. 2000) | L-8 |
| X. | <i>OBH Inc. v. Spotlight Magazine Inc.</i> , 86 F. Supp. 2d 176, 190 (W.D.N.Y. 2000) | L-9 |
| Y. | <i>Porsche Cars North America Inc. v. Spencer</i> , 2000 U.S. Dist. LEXIS 7060, 55 USPQ2d 1026 (E.D.Cal. 2000)..... | L-9 |
| Z. | <i>BigStar Entertainment Inc. v. Next Big Star Inc.</i> , 105 F. Supp. 2d 185 (S.D.N.Y. 2000)..... | L-9 |
| AA. | <i>Broadbridge Media v. Hypered</i> , 106 F. Supp. 2d 505 (S.D.N.Y. 2000) | L-9 |
| BB. | <i>Weber-Stephen Products Co. v. Armitage Hardware and Building Supply Inc.</i> , 2000 U.S. Dist. LEXIS 6335, 54 USPQ2d 1766 (N. Ill. 2000) | L-9 |
| CC. | <i>Harrods Ltd. v. Sixty Internet Domain Names</i> , 110 F. Supp. 2d 420 (E. D. Va. 2000)..... | L-9 |
| DD. | <i>eBay Inc. v. Bidder's Edge Inc.</i> , 100 F. Supp. 2d 1058 (N.D. Cal. 2000) | L-9 |
| EE. | <i>Northern Light Technology, Inc., V. Northern Lights Club</i> , 97 F. Supp. 2d 96 (D. Mass. 2000), <i>aff'd</i> 236 F.3d 57 (1st Cir. 2001)..... | L-9 |
| FF. | <i>Lucent Technologies Inc. v. Johnson</i> , 2000 U.S. Dist. LEXIS 16002, 56 USPQ2d 1637 (C. D. Cal. 2000)..... | L-9 |
| GG. | <i>Mattel Inc. v. Internet Dimensions Inc.</i> , 2000 U.S. Dist. LEXIS 9747, 55 USPQ2d 1620 (S.D.N.Y. 2000)..... | L-9 |
| HH. | <i>Virtual Works Inc. v. Volkswagen of America Inc.</i> , 238 F.3d 264 (CA 4 2001) | L-10 |
| II. | <i>Caesars World, Inc. v. Caesars-Palace.com</i> , 112 F. Supp. 2d 502, 504 (E.D. Va. 2000) | L-10 |
| JJ. | <i>Fleetboston Financial Corp. v. Fleetbostonfinancial.com</i> , 138 F. Supp. 2d 121 (D. Mass. 2001) | L-10 |
| KK. | <i>Mattel Inc. v. Barbie-Club.com</i> , 2001 U.S. Dist. LEXIS 5262, 58 USPQ2d 1798 (S.D.N.Y. 2001)..... | L-10 |
| LL. | <i>Lockheed Martin v. Network Solutions Inc.</i> , 141 F. Supp. 2d. 648 (N.D. Tex. 2001) | L-10 |
| MM. | <i>Parisi v. Netlearning Inc.</i> , 59 USPQ2d 1050 (E.D. Va. 2001)..... | L-10 |
| NN. | <i>Nike, Inc. v. Crystal International</i> , WIPO UDRP No. D2002-0352 (July 2002) | L-10 |
| XV. | Laws and Regulations Governing Domain Names | L-11 |
| A. | Uniform Domain Name Dispute Resolution Policy ("UDRP") | L-11 |
| B. | Anticybersquatting Consumer Protection Act (15 U.S.C. § 1125(d))..... | L-16 |

SECTION L

XVI. Sample Cases... L-25
AA. *Nike, Inc. v. Crystal International*, WIPO UDRP No. D2002-0352
(July 2002) L-25
BB. *Dell Computer Corporation v. MTO C.A. and Diabetes Long Life*,
WIPO UDRP No. D2002-0363 (July 2002) L-35

Update on Domain Name Disputes and New TLD's

**Joseph R. Dreitler
Jones Day Reavis & Pogue
Columbus, OH**

I. History of Domain Names and Their Administration

- Originally operated by Network Solutions, Inc. (now Verisign)
- U.S. Commerce Department later “opened” for competition creating ICANN
- More than 23 million “.com” and 30 million total names have been registered to date Country Code Top Level Domains (e.g., .uk, .jp .ru) now exist for over 240 jurisdictions, each with its own registry
- More than 170 registrars authorized to register “.com,” “.org,” “.net” domain names
- New top level domains (e.g., “.pro,” “.biz”)

II. Regulation of Trademark Rights in Domain Names

- Registrars issue names on “first come, first served” basis
- Registrars not responsible for infringing use of domain names by registrants (*Lockheed Martin v. Network Solutions Inc.*)
- Worldwide reach of the Internet means laws of many countries may be relevant

III. How Cybersquatters Can Harm IP

- Misdirect traffic to your competitors or unrelated parties goods
- Dilute your brand by associating it with unrelated goods/services
- Associate your brand with unsavory activity (e.g., pornography)
- Illegally criticize your business or practices

IV. Substantive Grounds To Challenge in U.S.

- Trademark Infringement
- Trademark Dilution
- Section 43(a) of the Lanham Act
- Anticybersquatter Consumer Protection Act (“ACPA”)
- State law

A. Trademark Infringement (15 U.S.C. Sec. 1114)

- Existence of registered trademark
- Use by defendant of “colorable imitation” of mark
- In a manner that is likely to cause confusion
- Confusion can be as to source, affiliation or endorsement
- *Brookfield*: “Initial Interest” confusion is enough
- Case law holds domain names can infringe trademarks
- Requires “commercial use” by defendant
- Provides for injunctive relief and damages

B. Trademark Dilution (15 U.S.C. Sec 1125(c))

- Mark must be both “famous” and “distinctive”
- Defendant’s use need not cause confusion: “blurring” or “tarnishment” sufficient
- Possible need to prove greater similarity than in infringement
- Relief usually limited to injunction - Supreme Court to decide this term “harm” required

C. Lanham Act Section 43(a) (15 U.S.C. Sec. 1125(a))

- Protects against infringement of unregistered common law marks, trade dress and false advertising, passing off
- Requires likelihood of confusion, endorsement or affiliation

D. Anticybersquatter Consumer Protection Act (15 U.S.C. Sec. 1125(d))

- Limited to domain names - not metatags
- Defendant must register, use or “traffic in” domain names
- With bad faith intent to profit from plaintiff’s mark
- Defendant’s domain name must be “dilutive of” famous mark or “confusingly similar to” valid mark
- Remedies include both injunction and damages
- “Statutory damages” of up to \$100,000 per infringing/dilutive name
- Forfeiture of infringing/dilutive domain names

E. State Law

- Common law infringement
- Trespass
- False advertising
- Unfair competition
- Consumer protection statutes

V. **ICANN UDRP “Arbitration”**

- Not Actually Arbitration (*Parisi v. Netlearning, Inc.*)
- Relatively inexpensive (*Dell Computer Corporation v. MTO C.A. and Diabetes Education Long Life*)
- Decision usually self executing – but may be “appealed” de novo
- Personal jurisdiction not an issue
- Law uncertain
- Limited relief
- May not be helpful if defendant has operating Web site
- Does not apply to most CCTLDs

VI. **Procedural Options**

- File suit in U.S. courts
- ICANN UDRP Proceeding
- Foreign litigation

A. U.S. Litigation

- Relatively expensive
- May be hard to serve defendant, enforce judgment
- Personal jurisdiction issues complex
- Broad relief (injunction, damages and forfeiture of domain names)
- Relatively clear and certain legal rights

B. Foreign Litigation

- Expensive
- Often uncertain result
- May be only effective way to stop foreign-based infringers

VII. Misdirection Web Sites

- Use variations on brand names
- Sell “keywords” or trademarks to third parties
- Often link or “point” to sites that offer competitive goods/services
 - <e-acme.com>
 - <acme.org>
 - <thaiacme.com>*
 - <acme.gr>*
 - <chasebanksucks.com>

*foreign language sites

A. “Typo” Squatters

- Misdirect traffic intended for genuine Web site operated by brand owner
 - <amazom.com>
 - <del.com>
 - <midrosoft.com>
 - <hometown.com>
 - <wwwlexus.com>

B. Metatag Pirates

- “Metatag” is text invisible to Internet user
- Used by search engines to identify Web sites listed in search results
- Because search technology is automated, unauthorized use of trademarks in metatags not detected by search engines

C. Unsavoury Sites

- Frequently pornographic
- Operators often unethical and difficult to find – false contact information
- Sometimes run by “true believers” in causes
 - <ballysucks.com>
 - <xxxacme.com>
 - <ihateacme.com>

Infinite variety of other domain names

D. Finding the Bad Guys

- Commercial search tools
- Customer complaints
- Sales reps and other intra-corporate sources
- Web searches
- Search engines
- <domainsurfer.com>

VIII. Search Methods

- Customer complaints
- Sales personnel and other in-house resources
- Formal Internet searches
- Search engines
- <domainsurfer.com>

IX. How to Stop Cybersquatters

- Identifying the sources and their prior activities
- Reviewing the various substantive legal rights
- Choosing the appropriate and available procedures

X. Strategic Goals for Trademark Protection

- Terminate serious infringement quickly
- Preserve strength and value of marks
- Use resources efficiently

XI. Recommended Procedures

- Establish standard search methodology
- Quick clearance of non-actionable sites
- Prompt action against high priority infringers

XII. Questionably Actionable Sites

- Fair use (*Terri Wells*)
- Gripe sites and Non-commercial use (*Marianne Bihari Bihari Interiors, Inc., v Craig Gross And Yolanda Truglio*)
- “Fan” sites (*Bruce Springsteen -v- Jeff Burgar and Bruce Springsteen Club*)
- Grey market/downstream distribution of trademarked goods
- Illegal use vs. fair use
- Public relations issues

XIII. Flagrant Misuses: Terminate With Prejudice

- Create form letters for recurring infringement/dilution paradigms
- Check lists for infringement, dilution, cybersquatting
- Obtain management guidance for cases that justify formal legal action
- Decide which merit civil litigation v. ICANN proceeding

XIV. Relevant Cases

Hasbro, Inc. v. Internet Entertainment Group, Ltd., 40 USPQ2d 1479, 1996 U.S. Dist. LEXIS 11626 (W.D. Wash. 1996) In one of the first reported cases, a court enjoined the defendant from using “candyland.com” or any similar name as a domain name to identify its “sexually explicit Internet site” which is “likely to dilute” the value of Hasbro’s CANDYLAND®.

Intermatic v. Toeppen, 947 F. Supp. 1227 (N.D. Ill. 1996); a magistrate recommended that summary judgment be granted against the use of the domain name INTERMATIC.COM based on the federal anti-dilution statute. INTERMATIC was a “strong, federally registered mark which has been exclusively used by Intermatic for over 50 years”.

Cardservice Int’l v. McGee, 950 F. Supp. 737, (E.D. Va.), *aff’d*, 129 F.3d 1258 (4th Cir. 1997). Defendants’ use of “cardservice.com” domain name and “Card Service” on Internet was found likely to cause confusion with plaintiff’s registered “Cardservice” mark. Plaintiff’s customers who wish to take advantage of its Internet services are likely to reach defendants’ “Card Service” home page instead, and wrongly assume that they have reached plaintiff’s Internet site.

Jews for Jesus v. Brodsky, 993 F. Supp. 282 (D. N.J. 1998). Plaintiff was successful in showing that defendant’s “jewsforjesus” Internet site will dilute the value of plaintiff’s “Jews for Jesus” trademark. Defendant used plaintiff organization’s mark to lure individuals to defendant’s site, and then refer, via hyperlink, to another Internet site which also contained information critical of plaintiff.

Planned Parenthood Fed'n of America v. Bucci, 1997 U.S. Dist. LEXIS 3338, 42 USPQ2d 1430 (S.D.N.Y. 1997) *aff'd*, 152 F.3d 920 (2d Cir. 1998), cert. denied, 119 S. Ct. 90 (1998). The court held that by registering Planned Parenthood.com as a domain name and then using it as a website to promote anti-abortion literature constituted trademark dilution and unfair competition.

Playboy Enters, Inc. v. Welles, 7 F. Supp. 2d 1098 (C.D. Cal 1997), *aff'd without op.*, 162 F.3d 1169 (9th Cir. 1998). Use of a third party's trademark in metatags does not always constitute trademark infringement, but see, *Playboy Enters., Inc. v. Asiafocus Int'l, Inc.*, No. Civ. A. 97-734-A, 1998 WL 724000, at *3, *6-*7 (E.D. Va. Apr. 10, 1998).

Niton Corp. v. Radiation Monitoring Devices, Inc., 27 F. Supp. 2d 102 (D. Mass. 1998), The use of metatags to divert a competitor's customers may constitute infringement.

Brookfield Communications, Inc., West Coast Entertainment Corporation, 174 F.3d 1036 (9th Cir. 1999). Defendant's use of plaintiff's "MovieBuff" mark or "moviebuf.com" in buried code or metatags on its World Wide Web site will result in initial interest confusion.

Promatek Industries, Ltd. v. Equitrac Corporation, 300 F.3d 808 (7th Cir. 2002). Defendant's use of plaintiff's trademark on its own web site and in metatags to attract customers will result in initial interest confusion.

Playboy Enterprises Inc. v. Netscape Communications Corp. 55 F. Supp. 2d 1070, 1090 (C.D. Cal. 1999). Playboy failed to obtain a preliminary injunction on the basis that defendant Internet service providers cause "initial interest confusion" with plaintiff's "Playboy" and "Playmate" trademarks by selling "banner advertisements" that respond to words "playboy" and "playmate" as search terms. Case is currently on appeal to the 9th Circuit.

Hasbro Inc. v. Clue Computing Inc. 994 F. Supp. 34, (D. Mass. 1997), *aff'd* 232 F.3d 1 (1st Cir. 2000) Plaintiff's "Clue" mark, for murder mystery board game, is a strong mark. However, Plaintiff has failed to establish that its "Clue" mark, for murder mystery board game, is "famous" within meaning of Federal Trademark Dilution Act, 15 U.S.C. Section 1125(c).

The Network Network v. CBS, Inc., 2000 WL 362016, 54 USPQ2d 1150 (C.D. Cal. 2000) Registration of TNN.com did not violate CBS' rights in its 1987 federal trademark registration of TNN. The test for dilution requires that a mark must be famous at the time the defendant adopts its mark.

Estee Lauder Inc. v. Fragrance Counter, 1999 U.S. Dist. LEXIS 14825, 52 USPQ2d 1786, No. 99-CV-382 (S.D.N.Y.). Does defendants' purchase of keywords "Clinique," "Estee Lauder" and "Origins" from the Excite and Webcrawler search engines violate trademark, dilution or unfair competition law? Case was settled.

Sporty's Farm v Sportsman's Market, 202 F.3d 489, (2d Cir. 2000). Registration of domain name "sportys.com" for primary purpose of keeping trademark owner from using that name, and defendants' creating an unrelated business violates ACPA.

Lucent Technologies Inc. v. lucentucks.com 95 F. Supp. 2d 528 (E.D. Va. 2000), Plaintiff's waiting period of eight days between sending notice of intent to proceed in rem and filing of in rem action did not satisfy jurisdictional requirements for in rem action under Anti-Cybersquatting Consumer Protection Act.

Barcelona.com Inc. v. Excelentisimo Ayuntamiento de Barcelona 63 USPQ2d 1189 (E.D. Va. 2002), Appeal from decision of UDRP panel is de novo and finding of panel is not binding on federal district court.

America Online Inc. v. Huang 106 F. Supp. 2d 848, 855-60 (E.D. Va. 2000). Domain name registration agreements between defendant and domain name registrar are not sufficient contacts with Virginia for purposes of personal jurisdiction over defendant.

Ford Motor Co. v. Ford Financial Solutions Inc., 103 F. Supp. 2d 1126 (N.D. Iowa 2000). Defendant's use of mark "Ford Financial Solutions" and domain name "fordfinancialsolutions.com" infringes plaintiff's "Ford" name and trademarks.

Bancroft & Masters Inc. v. Augusta National, Inc. 223 F.3d 1082 (9th Cir. 2000). U.S. District Court has specific personal jurisdiction over Georgia defendant in action in which plaintiff seeks declaratory judgment establishing its right to use "masters.com" domain name.

Bird v. Parsons, 62 USPQ2d 1905, 2002 FED App. 0177P (6th Cir. 2002) . Affirmed District Court holding that Washington state operator of domain name registry and domain name auction site is not subject to personal jurisdiction in Ohio or subject to ACPA for offering to sell domain names on its web-site.

Heathmount A.E. Corp. v. technodome.com, 106 F. Supp. 2d 860, 865-66 (E.D. Va. 2000). Plaintiff filing in rem complaint against domain name bears burden of demonstrating due diligence in trying to establish personal jurisdiction over potential defendant.

Shields v. Zuccarini, 89 F. Supp. 2d 634 (E.D. Pa. 2000), *aff'd* No. 00-2236 (3rd Cir. 2001). Plaintiff's "Joe Cartoon" mark is distinctive and famous, and therefore is entitled to protection under ACPA. Defendant acted with bad faith intent to profit from plaintiff's "Joe Cartoon" mark in registering domain names that are confusingly similar to plaintiff's "joecartoon.com".

Electronics Boutique Holdings Corp. v. Zuccarini, 2000 U.S. Dist. LEXIS 15719, 56 USPQ2d 1705 (E.D. Pa. 2000). Defendant's "typosquattings" are confusingly similar to plaintiff's famous "Electronics Boutique" marks, since profitability of defendant's enterprise depends on Internet users' misspellings which sends them instead to defendant's Web site where each click on advertisement results in remuneration for defendant.

OBH Inc. v. Spotlight Magazine Inc., 86 F. Supp. 2d 176, 190 (W.D.N.Y. 2000). Defendants' use of "thebuffalonews.com" domain name constitutes use of trademark "in commerce" and in connection with distribution or advertising of goods or services within meaning of Lanham Act.

Porsche Cars North America Inc. v. Spencer, 2000 U.S. Dist. LEXIS 7060, 55 USPQ2d 1026 (E.D.Cal. 2000). "Porsche" mark for automobiles is "famous" mark entitled to protection under ACPA.

BigStar Entertainment Inc. v. Next Big Star Inc., 105 F. Supp. 2d 185 (S.D.N.Y. 2000). Doctrine of "initial interest confusion" does not apply to claim that consumer searching for plaintiff's "bigstar.com" may be drawn instead to defendants' "nextbigstar.com" site, since there is no allegation that defendants have used "bigstar" or "bigstar.com" in metatags to divert customers.

Broadbridge Media v. Hypered, 106 F. Supp. 2d 505 (S.D.N.Y. 2000). Complainant does not waive right to proceed in federal district court by filing UDRP domain name dispute complaint.

Weber-Stephen Products Co. v. Armitage Hardware and Building Supply Inc., 2000 U.S. Dist. LEXIS 6335, 54 USPQ2d 1766 (N. Ill. 2000). UDRP panel decision is not binding on federal district court.

Harrods Ltd. v. Sixty Internet Domain Names, 110 F. Supp. 2d 420 (E. D. Va. 2000). Bad faith intent to profit is necessary element of in rem action under ACPA.

eBay Inc. v. Bidder's Edge Inc., 100 F. Supp. 2d 1058 (N.D. Cal. 2000). Plaintiff on-line auction site is likely to prevail on merits of its claim that defendant auction aggregator's use of automated querying programs to access plaintiff's computer systems constituted trespass.

Northern Light Technology, Inc., V. Northern Lights Club, 97 F. Supp. 2d 96 (D. Mass. 2000), aff'd 236 F.3d 57 (1st Cir. 2001). Individual non-resident defendant in trademark action is not entitled to immunity from service of process in forum state.

Lucent Technologies Inc. v. Johnson, 2000 U.S. Dist. LEXIS 16002, 56 USPQ2d 1637 (C. D. Cal. 2000). Claim that registration and use of "lucentsucks.com" domain name is entitled to First Amendment protection from cybersquatting claim, on ground that "yourcompanynamesucks" domain names, as group, merit application of First Amendment "safe harbor" defense, may not be decide on motion to dismiss.

Mattel Inc. v. Internet Dimensions Inc., 2000 U.S. Dist. LEXIS 9747, 55 USPQ2d 1620 (S.D.N.Y. 2000), "Barbie" fashion doll and logo are "distinctive" and "famous" for purposes of ACPA.

Virtual Works Inc. v. Volkswagen of America Inc., 238 F.3d 264 (CA 4 2001). Evidence shows defendant registered “vw.net” domain name with bad faith intent to profit from protected “VW” trademark, even though defendant used “vw.net” for two years as part of Internet service provider business.

Caesars World, Inc. v. Caesars-Palace.com, 112 F. Supp. 2d 502, 504 (E.D. Va. 2000) The in rem provision of the ACPA is constitutional.

Fleetboston Financial Corp. v. Fleetbostonfinancial.com, 138 F. Supp. 2d 121 (D. Mass. 2001). Court will not permit an in rem jurisdiction action to be brought in Massachusetts on the basis of the plaintiff filing suit and asking the domain name Registrar, located outside of Massachusetts, to deposit the res in that jurisdiction.

Mattel Inc. v. Barbie-Club.com, 2001 U.S. Dist. LEXIS 5262, 58 USPQ2d 1798 (S.D.N.Y. 2001) There is no basis to bring an in rem action in New York if there was no connection with the res.

Lockheed Martin v. Network Solutions Inc., 141 F. Supp. 2d. 648 (N.D. Tex. 2001), the court held that Congress did not intend to make domain name registries liable under §43(d) for infringing domain name registrations, absent a showing of bad faith registration.

Parisi v. Netlearning Inc., 59 USPQ2d 1050 (E.D. Va. 2001), the court held that the mandatory administrative proceedings conducted under UDRP are not an “arbitration” subject to the Federal Arbitration Act.

Nike, Inc. v. Crystal International, WIPO UDRP No. D2002-0352 (July 2002), a single UDRP panelist from Canada finds that there was no evidence of “bad faith”, even though the owner of nikegolf.net and 4 other variations of Nike – had been previously found liable for cyberpiracy of NIKE trademarks in a UDRP action.

XV. Laws and Regulations Governing Domain Names

A. Uniform Domain Name Dispute Resolution Policy (“UDRP”)

(As Approved by ICANN on October 24, 1999)

1. Purpose. This Uniform Domain Name Dispute Resolution Policy (the “Policy”) has been adopted by the Internet Corporation for Assigned Names and Numbers (“ICANN”), is incorporated by reference into your Registration Agreement, and sets forth the terms and conditions in connection with a dispute between you and any party other than us (the registrar) over the registration and use of an Internet domain name registered by you. Proceedings under Paragraph 4 of this Policy will be conducted according to the Rules for Uniform Domain Name Dispute Resolution Policy (the “Rules of Procedure”), which are available at www.icann.org/udrp/udrp-rules-24oct99.htm, and the selected administrative-dispute-resolution service provider’s supplemental rules.

2. Your Representations. By applying to register a domain name, or by asking us to maintain or renew a domain name registration, you hereby represent and warrant to us that (a) the statements that you made in your Registration Agreement are complete and accurate; (b) to your knowledge, the registration of the domain name will not infringe upon or otherwise violate the rights of any third party; (c) you are not registering the domain name for an unlawful purpose; and (d) you will not knowingly use the domain name in violation of any applicable laws or regulations. It is your responsibility to determine whether your domain name registration infringes or violates someone else’s rights.

3. Cancellations, Transfers, and Changes. We will cancel, transfer or otherwise make changes to domain name registrations under the following circumstances:

- a. subject to the provisions of Paragraph 8, our receipt of written or appropriate electronic instructions from you or your authorized agent to take such action;
- b. our receipt of an order from a court or arbitral tribunal, in each case of competent jurisdiction, requiring such action; and/or
- c. our receipt of a decision of an Administrative Panel requiring such action in any administrative proceeding to which you were a party and which was conducted under this Policy or a later version of this Policy adopted by ICANN. (See Paragraph 4(i) and (k) below.)

We may also cancel, transfer or otherwise make changes to a domain name registration in accordance with the terms of your Registration Agreement or other legal requirements.

4. Mandatory Administrative Proceeding.

This Paragraph sets forth the type of disputes for which you are required to submit to a mandatory administrative proceeding. These proceedings will be conducted before one of the administrative-dispute-resolution service providers listed at www.icann.org/udrp/approved-providers.htm (each, a "Provider").

a. Applicable Disputes. You are required to submit to a mandatory administrative proceeding in the event that a third party (a "complainant") asserts to the applicable Provider, in compliance with the Rules of Procedure, that

- (i) your domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights; and
- (ii) you have no rights or legitimate interests in respect of the domain name; and
- (iii) your domain name has been registered and is being used in bad faith.
- (iv) In the administrative proceeding, the complainant must prove that each of these three elements are present.

b. Evidence of Registration and Use in Bad Faith. For the purposes of Paragraph 4(a)(iii), the following circumstances, in particular but without limitation, if found by the Panel to be present, shall be evidence of the registration and use of a domain name in bad faith:

- (i) circumstances indicating that you have registered or you have acquired the domain name primarily for the purpose of selling, renting, or otherwise transferring the domain name registration to the complainant who is the owner of the trademark or service mark or to a competitor of that complainant, for valuable consideration in excess of your documented out-of-pocket costs directly related to the domain name; or
- (ii) you have registered the domain name in order to prevent the owner of the trademark or service mark from reflecting the mark in a corresponding domain name, provided that you have engaged in a pattern of such conduct; or
- (iii) you have registered the domain name primarily for the purpose of disrupting the business of a competitor; or
- (iv) by using the domain name, you have intentionally attempted to attract, for commercial gain, Internet users to your web site or other on-line location, by creating a likelihood of confusion with the complainant's mark as to the source, sponsorship, affiliation, or endorsement of your web site or location or of a product or service on your web site or location.

c. How to Demonstrate Your Rights to and Legitimate Interests in the Domain Name in Responding to a Complaint. When you receive a complaint, you should refer to Paragraph 5 of the Rules of Procedure in determining how your response should be prepared. Any of the following circumstances, in particular but without limitation, if found by the Panel to be proved based on its evaluation of all evidence presented, shall demonstrate your rights or legitimate interests to the domain name for purposes of Paragraph 4(a)(ii):

(i) before any notice to you of the dispute, your use of, or demonstrable preparations to use, the domain name or a name corresponding to the domain name in connection with a bona fide offering of goods or services; or

(ii) you (as an individual, business, or other organization) have been commonly known by the domain name, even if you have acquired no trademark or service mark rights; or

(iii) you are making a legitimate noncommercial or fair use of the domain name, without intent for commercial gain to misleadingly divert consumers or to tarnish the trademark or service mark at issue.

d. Selection of Provider. The complainant shall select the Provider from among those approved by ICANN by submitting the complaint to that Provider. The selected Provider will administer the proceeding, except in cases of consolidation as described in Paragraph 4(f).

e. Initiation of Proceeding and Process and Appointment of Administrative Panel. The Rules of Procedure state the process for initiating and conducting a proceeding and for appointing the panel that will decide the dispute (the "Administrative Panel").

f. Consolidation. In the event of multiple disputes between you and a complainant, either you or the complainant may petition to consolidate the disputes before a single Administrative Panel. This petition shall be made to the first Administrative Panel appointed to hear a pending dispute between the parties. This Administrative Panel may consolidate before it any or all such disputes in its sole discretion, provided that the disputes being consolidated are governed by this Policy or a later version of this Policy adopted by ICANN.

g. Fees. All fees charged by a Provider in connection with any dispute before an Administrative Panel pursuant to this Policy shall be paid by the complainant, except in cases where you elect to expand the Administrative Panel from one to three panelists as provided in Paragraph 5(b)(iv) of the Rules of Procedure, in which case all fees will be split evenly by you and the complainant.

h. Our Involvement in Administrative Proceedings. We do not, and will not, participate in the administration or conduct of any proceeding before an Administrative Panel. In addition, we will not be liable as a result of any decisions rendered by the Administrative Panel.

i. Remedies. The remedies available to a complainant pursuant to any proceeding before an Administrative Panel shall be limited to requiring the cancellation of your domain name or the transfer of your domain name registration to the complainant.

j. Notification and Publication. The Provider shall notify us of any decision made by an Administrative Panel with respect to a domain name you have registered with us. All decisions under this Policy will be published in full over the Internet, except when an Administrative Panel determines in an exceptional case to redact portions of its decision.

k. Availability of Court Proceedings. The mandatory administrative proceeding requirements set forth in Paragraph 4 shall not prevent either you or the complainant from submitting the dispute to a court of competent jurisdiction for independent resolution before such mandatory administrative proceeding is commenced or after such proceeding is concluded. If an Administrative Panel decides that your domain name registration should be canceled or transferred, we will wait ten (10) business days (as observed in the location of our principal office) after we are informed by the applicable Provider of the Administrative Panel's decision before implementing that decision. We will then implement the decision unless we have received from you during that ten (10) business day period official documentation (such as a copy of a complaint, file-stamped by the clerk of the court) that you have commenced a lawsuit against the complainant in a jurisdiction to which the complainant has submitted under Paragraph 3(b)(xiii) of the Rules of Procedure. (In general, that jurisdiction is either the location of our principal office or of your address as shown in our Whois database. See Paragraphs 1 and 3(b)(xiii) of the Rules of Procedure for details.) If we receive such documentation within the ten (10) business day period, we will not implement the Administrative Panel's decision, and we will take no further action, until we receive (i) evidence satisfactory to us of a resolution between the parties; (ii) evidence satisfactory to us that your lawsuit has been dismissed or withdrawn; or (iii) a copy of an order from such court dismissing your lawsuit or ordering that you do not have the right to continue to use your domain name.

5. All Other Disputes and Litigation. All other disputes between you and any party other than us regarding your domain name registration that are not brought pursuant to the mandatory administrative proceeding provisions of Paragraph 4 shall be resolved between you and such other party through any court, arbitration or other proceeding that may be available.

6. Our Involvement in Disputes. We will not participate in any way in any dispute between you and any party other than us regarding the registration and use of your domain name. You shall not name us as a party or otherwise include us in any such proceeding. In the event that we are named as a party in any such proceeding, we reserve the right to raise any and all defenses deemed appropriate, and to take any other action necessary to defend ourselves.

7. Maintaining the Status Quo. We will not cancel, transfer, activate, deactivate, or otherwise change the status of any domain name registration under this Policy except as provided in Paragraph 3 above.

8. Transfers During a Dispute.

a. Transfers of a Domain Name to a New Holder. You may not transfer your domain name registration to another holder (i) during a pending administrative proceeding brought pursuant to Paragraph 4 or for a period of fifteen (15) business days (as observed in the location of our principal place of business) after such proceeding is concluded; or (ii) during a pending court proceeding or arbitration commenced regarding your domain name unless the party to whom the domain name registration is being transferred agrees, in writing, to be bound by the decision of the court or arbitrator. We reserve the right to cancel any transfer of a domain name registration to another holder that is made in violation of this subparagraph.

b. Changing Registrars. You may not transfer your domain name registration to another registrar during a pending administrative proceeding brought pursuant to Paragraph 4 or for a period of fifteen (15) business days (as observed in the location of our principal place of business) after such proceeding is concluded. You may transfer administration of your domain name registration to another registrar during a pending court action or arbitration, provided that the domain name you have registered with us shall continue to be subject to the proceedings commenced against you in accordance with the terms of this Policy. In the event that you transfer a domain name registration to us during the pendency of a court action or arbitration, such dispute shall remain subject to the domain name dispute policy of the registrar from which the domain name registration was transferred.

9. Policy Modifications. We reserve the right to modify this Policy at any time with the permission of ICANN. We will post our revised Policy at <URL> at least thirty (30) calendar days before it becomes effective. Unless this Policy has already been invoked by the submission of a complaint to a Provider, in which event the version of the Policy in effect at the time it was invoked will apply to you until the dispute is over, all such changes will be binding upon you with respect to any domain name registration dispute, whether the dispute arose before, on or after the effective date of our change. In the event that you object to a change in this Policy, your sole remedy is to cancel your domain name registration with us, provided that you will not be entitled to a refund of any fees you paid to us. The revised Policy will apply to you until you cancel your domain name registration.

B. Anticybersquatting Consumer Protection Act (15 U.S.C. Sec. 1125(d))

TITLE III--TRADEMARK CYBERPIRACY PREVENTION

TITLE III--TRADEMARK CYBERPIRACY PREVENTION

SEC. 3001. SHORT TITLE; REFERENCES.

(a) SHORT TITLE- This title may be cited as the 'Anticybersquatting Consumer Protection Act'.

(b) REFERENCES TO THE TRADEMARK ACT OF 1946- Any reference in this title to the Trademark Act of 1946 shall be a reference to the Act entitled 'An Act to provide for the registration and protection of trademarks used in commerce, to carry out the provisions of certain international conventions, and for other purposes', approved July 5, 1946 (15 U.S.C. 1051 et seq.).

SEC. 3002. CYBERPIRACY PREVENTION.

(a) IN GENERAL- Section 43 of the Trademark Act of 1946 (15 U.S.C. 1125) is amended by inserting at the end the following:

'(d)(1)(A) A person shall be liable in a civil action by the owner of a mark, including a personal name which is protected as a mark under this section, if, without regard to the goods or services of the parties, that person--

'(i) has a bad faith intent to profit from that mark, including a personal name which is protected as a mark under this section; and

'(ii) registers, traffics in, or uses a domain name that--

'(I) in the case of a mark that is distinctive at the time of registration of the domain name, is identical or confusingly similar to that mark;

'(II) in the case of a famous mark that is famous at the time of registration of the domain name, is identical or confusingly similar to or dilutive of that mark; or

'(III) is a trademark, word, or name protected by reason of section 706 of title 18, United States Code, or section 220506 of title 36, United States Code.

'(B)(i) In determining whether a person has a bad faith intent described under subparagraph (A), a court may consider factors such as, but not limited to--

‘(I) the trademark or other intellectual property rights of the person, if any, in the domain name;

‘(II) the extent to which the domain name consists of the legal name of the person or a name that is otherwise commonly used to identify that person;

‘(III) the person’s prior use, if any, of the domain name in connection with the bona fide offering of any goods or services;

‘(IV) the person’s bona fide noncommercial or fair use of the mark in a site accessible under the domain name;

‘(V) the person’s intent to divert consumers from the mark owner’s online location to a site accessible under the domain name that could harm the goodwill represented by the mark, either for commercial gain or with the intent to tarnish or disparage the mark, by creating a likelihood of confusion as to the source, sponsorship, affiliation, or endorsement of the site;

‘(VI) the person’s offer to transfer, sell, or otherwise assign the domain name to the mark owner or any third party for financial gain without having used, or having an intent to use, the domain name in the bona fide offering of any goods or services, or the person’s prior conduct indicating a pattern of such conduct;

‘(VII) the person’s provision of material and misleading false contact information when applying for the registration of the domain name, the person’s intentional failure to maintain accurate contact information, or the person’s prior conduct indicating a pattern of such conduct;

‘(VIII) the person’s registration or acquisition of multiple domain names which the person knows are identical or confusingly similar to marks of others that are distinctive at the time of registration of such domain names, or dilutive of famous marks of others that are famous at the time of registration of such domain names, without regard to the goods or services of the parties; and

‘(IX) the extent to which the mark incorporated in the person’s domain name registration is or is not distinctive and famous within the meaning of subsection (c)(1) of section 43.

‘(ii) Bad faith intent described under subparagraph (A) shall not be found in any case in which the court determines that the person believed and had reasonable grounds to believe that the use of the domain name was a fair use or otherwise lawful.

‘(C) In any civil action involving the registration, trafficking, or use of a domain name under this paragraph, a court may order the forfeiture or cancellation of the domain name or the transfer of the domain name to the owner of the mark.

'(D) A person shall be liable for using a domain name under subparagraph (A) only if that person is the domain name registrant or that registrant's authorized licensee.

'(E) As used in this paragraph, the term 'traffics in' refers to transactions that include, but are not limited to, sales, purchases, loans, pledges, licenses, exchanges of currency, and any other transfer for consideration or receipt in exchange for consideration.

'(2)(A) The owner of a mark may file an in rem civil action against a domain name in the judicial district in which the domain name registrar, domain name registry, or other domain name authority that registered or assigned the domain name is located if--

'(i) the domain name violates any right of the owner of a mark registered in the Patent and Trademark Office, or protected under subsection (a) or (c); and

'(ii) the court finds that the owner--

(I) is not able to obtain in personam jurisdiction over a person who would have been a defendant in a civil action under paragraph (1); or

(II) through due diligence was not able to find a person who would have been a defendant in a civil action under paragraph (1) by--

(aa) sending a notice of the alleged violation and intent to proceed under this paragraph to the registrant of the domain name at the postal and e-mail address provided by the registrant to the registrar; and

(bb) publishing notice of the action as the court may direct promptly after filing the action.

(B) The actions under subparagraph (A)(ii) shall constitute service of process.

(C) In an in rem action under this paragraph, a domain name shall be deemed to have its situs in the judicial district in which--

(i) the domain name registrar, registry, or other domain name authority that registered or assigned the domain name is located; or

(ii) documents sufficient to establish control and authority regarding the disposition of the registration and use of the domain name are deposited with the court.

(D)(i) The remedies in an in rem action under this paragraph shall be limited to a court order for the forfeiture or cancellation of the domain name or the transfer of the domain name to the owner of the mark. Upon receipt of written notification of a filed, stamped copy of a complaint filed by the owner of a mark in a United States district court under this paragraph, the domain name registrar, domain name registry, or other domain name authority shall--

(I) expeditiously deposit with the court documents sufficient to establish the court's control and authority regarding the disposition of the registration and use of the domain name to the court; and

(II) not transfer, suspend, or otherwise modify the domain name during the pendency of the action, except upon order of the court.

(ii) The domain name registrar or registry or other domain name authority shall not be liable for injunctive or monetary relief under this paragraph except in the case of bad faith or reckless disregard, which includes a willful failure to comply with any such court order.

(3) The civil action established under paragraph (1) and the in rem action established under paragraph (2), and any remedy available under either such action, shall be in addition to any other civil action or remedy otherwise applicable.

(4) The in rem jurisdiction established under paragraph (2) shall be in addition to any other jurisdiction that otherwise exists, whether in rem or in personam.'.

(b) CYBERPIRACY PROTECTIONS FOR INDIVIDUALS-

(1) IN GENERAL-

(A) CIVIL LIABILITY- Any person who registers a domain name that consists of the name of another living person, or a name substantially and confusingly similar thereto, without that person's consent, with the specific intent to profit from such name by selling the domain name for financial gain to that person or any third party, shall be liable in a civil action by such person.

(B) EXCEPTION- A person who in good faith registers a domain name consisting of the name of another living person, or a name substantially and confusingly similar thereto, shall not be liable under this paragraph if such name is used in, affiliated with, or related to a work of authorship protected under title 17, United States Code, including a work made for hire as defined in section 101 of title 17, United States Code, and if the person registering the domain name is the copyright owner or licensee of the work, the person intends to sell the domain name in conjunction with the lawful exploitation of the work, and such registration is not prohibited by a contract between the registrant and the named person. The exception under this subparagraph shall apply only to a civil action brought under paragraph (1) and shall in no manner limit the protections afforded under the Trademark Act of 1946 (15 U.S.C. 1051 et seq.) or other provision of Federal or State law.

(2) REMEDIES- In any civil action brought under paragraph (1), a court may award injunctive relief, including the forfeiture or cancellation of the domain name or the transfer of the domain name to the plaintiff. The court may also, in its discretion, award costs and attorneys fees to the prevailing party.

(3) DEFINITION- In this subsection, the term 'domain name' has the meaning given that term in section 45 of the Trademark Act of 1946 (15 U.S.C. 1127).

(4) EFFECTIVE DATE- This subsection shall apply to domain names registered on or after the date of the enactment of this Act.

SEC. 3003. DAMAGES AND REMEDIES.

(a) REMEDIES IN CASES OF DOMAIN NAME PIRACY-

(1) INJUNCTIONS- Section 34(a) of the Trademark Act of 1946 (15 U.S.C. 1116(a)) is amended in the first sentence by striking '(a) or (c)' and inserting '(a), (c), or (d)'.

(2) DAMAGES- Section 35(a) of the Trademark Act of 1946 (15 U.S.C. 1117(a)) is amended in the first sentence by inserting, '(c), or (d)' after 'section 43(a)'.

(b) STATUTORY DAMAGES- Section 35 of the Trademark Act of 1946 (15 U.S.C. 1117) is amended by adding at the end the following:

'(d) In a case involving a violation of section 43(d)(1), the plaintiff may elect, at any time before final judgment is rendered by the trial court, to recover, instead of actual damages and profits, an award of statutory damages in the amount of not less than \$1,000 and not more than \$100,000 per domain name, as the court considers just.

SEC. 3004. LIMITATION ON LIABILITY.

Section 32(2) of the Trademark Act of 1946 (15 U.S.C. 1114) is amended--

(1) in the matter preceding subparagraph (A) by striking 'under section 43(a)' and inserting 'under section 43(a) or (d)'; and

(2) by redesignating subparagraph (D) as subparagraph (E) and inserting after subparagraph (C) the following:

'(D)(i)(I) A domain name registrar, a domain name registry, or other domain name registration authority that takes any action described under clause (ii) effecting a domain name shall not be liable for monetary relief or, except as provided in subclause (II), for injunctive relief, to any person for such action, regardless of whether the domain name is finally determined to infringe or dilute the mark.

'(II) A domain name registrar, domain name registry, or other domain name registration authority described in subclause (I) may be subject to injunctive relief only if such registrar, registry, or other registration authority has--

‘(aa) not expeditiously deposited with a court, in which an action has been filed regarding the disposition of the domain name, documents sufficient for the court to establish the court’s control and authority regarding the disposition of the registration and use of the domain name;

‘(bb) transferred, suspended, or otherwise modified the domain name during the pendency of the action, except upon order of the court; or

‘(cc) willfully failed to comply with any such court order.

(ii) An action referred to under clause (i)(I) is any action of refusing to register, removing from registration, transferring, temporarily disabling, or permanently canceling a domain name--

‘(I) in compliance with a court order under section 43(d); or

‘(II) in the implementation of a reasonable policy by such registrar, registry, or authority prohibiting the registration of a domain name that is identical to, confusingly similar to, or dilutive of another’s mark.

‘(iii) A domain name registrar, a domain name registry, or other domain name registration authority shall not be liable for damages under this section for the registration or maintenance of a domain name for another absent a showing of bad faith intent to profit from such registration or maintenance of the domain name.

‘(iv) If a registrar, registry, or other registration authority takes an action described under clause (ii) based on a knowing and material misrepresentation by any other person that a domain name is identical to, confusingly similar to, or dilutive of a mark, the person making the knowing and material misrepresentation shall be liable for any damages, including costs and attorney’s fees, incurred by the domain name registrant as a result of such action. The court may also grant injunctive relief to the domain name registrant, including the reactivation of the domain name or the transfer of the domain name to the domain name registrant.

‘(v) A domain name registrant whose domain name has been suspended, disabled, or transferred under a policy described under clause (ii)(II) may, upon notice to the mark owner, file a civil action to establish that the registration or use of the domain name by such registrant is not unlawful under this Act. The court may grant injunctive relief to the domain name registrant, including the reactivation of the domain name or transfer of the domain name to the domain name registrant.’

SEC. 3005. DEFINITIONS.

Section 45 of the Trademark Act of 1946 (15 U.S.C. 1127) is amended by inserting after the undesignated paragraph defining the term 'counterfeit' the following:

The term 'domain name' means any alphanumeric designation which is registered with or assigned by any domain name registrar, domain name registry, or other domain name registration authority as part of an electronic address on the Internet.

'The term 'Internet' has the meaning given that term in section 230(f)(1) of the Communications Act of 1934 (47 U.S.C. 230(f)(1)).'

SEC. 3006. STUDY ON ABUSIVE DOMAIN NAME REGISTRATIONS INVOLVING PERSONAL NAMES.

(a) IN GENERAL- Not later than 180 days after the date of the enactment of this Act, the Secretary of Commerce, in consultation with the Patent and Trademark Office and the Federal Election Commission, shall conduct a study and report to Congress with recommendations on guidelines and procedures for resolving disputes involving the registration or use by a person of a domain name that includes the personal name of another person, in whole or in part, or a name confusingly similar thereto, including consideration of and recommendations for--

(1) protecting personal names from registration by another person as a second level domain name for purposes of selling or otherwise transferring such domain name to such other person or any third party for financial gain;

(2) protecting individuals from bad faith uses of their personal names as second level domain names by others with malicious intent to harm the reputation of the individual or the goodwill associated with that individual's name;

(3) protecting consumers from the registration and use of domain names that include personal names in the second level domain in manners which are intended or are likely to confuse or deceive the public as to the affiliation, connection, or association of the domain name registrant, or a site accessible under the domain name, with such other person, or as to the origin, sponsorship, or approval of the goods, services, or commercial activities of the domain name registrant;

(4) protecting the public from registration of domain names that include the personal names of government officials, official candidates, and potential official candidates for Federal, State, or local political office in the United States, and the use of such domain names in a manner that disrupts the electoral process or the public's ability to access accurate and reliable information regarding such individuals;

(5) existing remedies, whether under State law or otherwise, and the extent to which such remedies are sufficient to address the considerations described in paragraphs (1) through (4); and

(6) the guidelines, procedures, and policies of the Internet Corporation for Assigned Names and Numbers and the extent to which they address the considerations described in paragraphs (1) through (4).

(b) GUIDELINES AND PROCEDURES- The Secretary of Commerce shall, under its Memorandum of Understanding with the Internet Corporation for Assigned Names and Numbers, collaborate to develop guidelines and procedures for resolving disputes involving the registration or use by a person of a domain name that includes the personal name of another person, in whole or in part, or a name confusingly similar thereto.

SEC. 3007. HISTORIC PRESERVATION.

Section 101(a)(1)(A) of the National Historic Preservation Act (16 U.S.C. 470a(a)(1)(A)) is amended by adding at the end the following: 'Notwithstanding section 43(c) of the Act entitled 'An Act to provide for the registration and protection of trademarks used in commerce, to carry out the provisions of certain international conventions, and for other purposes', approved July 5, 1946 (commonly known as the 'Trademark Act of 1946' (15 U.S.C. 1125(c)), buildings and structures on or eligible for inclusion on the National Register of Historic Places (either individually or as part of a historic district), or designated as an individual landmark or as a contributing building in a historic district by a unit of State or local government, may retain the name historically associated with the building or structure'.

SEC. 3008. SAVINGS CLAUSE.

Nothing in this title shall affect any defense available to a defendant under the Trademark Act of 1946 (including any defense under section 43(c)(4) of such Act or relating to fair use) or a person's right of free speech or expression under the first amendment of the United States Constitution.

SEC. 3009. TECHNICAL AND CONFORMING AMENDMENTS.

Chapter 85 of title 28, United States Code, is amended as follows:

(1) Section 1338 of title 28, United States Codes, is amended--

(A) in the section heading by striking 'trade-marks' and inserting 'trademarks';

(B) in subsection (a) by striking 'trade-marks' and inserting 'trademarks'; and

(C) in subsection (b) by striking 'trade-mark' and inserting 'trademark'.

(2) The item relating to section 1338 in the table of sections for chapter 85 of title 28, United States Code, is amended by striking 'trade-marks' and inserting 'trademarks'.

SEC. 3010. EFFECTIVE DATE.

Sections 3002(a), 3003, 3004, 3005, and 3008 of this title shall apply to all domain names registered before, on, or after the date of the enactment of this Act, except that damages under subsection (a) or (d) of section 35 of the Trademark Act of 1946 (15 U.S.C. 1117), as amended by section 3003 of this title, shall not be available with respect to the registration, trafficking, or use of a domain name that occurs before the date of the enactment of this Act.



WIPO Arbitration and Mediation Center

ADMINISTRATIVE PANEL DECISION

Nike, Inc. v. Crystal International

Case No. D2002-0352

1. The Parties

1.1 The Complainant is Nike, Inc., an Oregon Corporation with its principal place of business in Beaverton, Oregon, United States of America.

1.2 The Respondent is Crystal International located at RM609 HyoCunB/D Seo Cho Dong, 1425-10 Seo Cho Ku, Seoul, Republic of Korea.

2. The Domain Names and Registrar

2.1 The Domain Names at issue are: <nikepark.com>, <nikepark.net>, <nikemen.com>, <nikegolf.net>, <nikeshops.com>.

2.2 The Domain Names are registered with Tucows, 96 Mowat Avenue, Toronto, Ontario, Canada.

3. Procedural History

3.1 A Complaint was submitted by the Complainant to the World Intellectual Property Organization Arbitration and Mediation Center ("the Center") on April 15, 2002 in hard copy and on April 19, 2002, by email. The Center sent an Acknowledgement of Receipt of Complaint to the Complainant on April 16, 2002. The Complainant paid the required fee.

3.2 On April 18, 2002 the Center sent Request for Registrar Verification to the Registrar requesting verification of registration data. The Registrar confirmed, *inter alia*, that it is the Registrar of the Domain Names and that the Domain Names are registered in the Respondent's name.

3.3 The Center verified that the Complaint satisfies the formal requirements of the ICANN Uniform Domain Name Dispute Resolution Policy (the "Policy"), the Rules for Uniform Domain Name Dispute Resolution Policy (the "Rules"), and the WIPO Supplemental Rules for Uniform Domain Name Dispute Resolution Policy (the "Supplemental Rules").

3.4 On April 22, 2002, the Center sent a Notification of Complaint and Commencement of Administrative Proceeding to the Respondent together with copies of the Complaint, with a copy to the Complainant. This notification was sent by the methods required under Paragraph 2(a) of the Rules.

3.5 On May 17, 2002 the Center sent a Notification of Respondent default as no Response was submitted.

3.6 On June 6, 2002 the Center received a completed and signed Statement of Acceptance and Declaration of Impartiality and Independence from Cecil O.D. Branson, Q.C. (the "Sole Panelist"). The Center notified the parties of the appointment of a single-member Panel consisting of the Sole Panelist.

3.7 The Sole Panelist finds that the Panel was properly constituted and appointed in accordance with the Rules and WIPO Supplemental Rules.

4. Factual Background

4.1 Complainant, Nike Inc. is a leading sports and fitness company, designing, manufacturing and marketing a broad range of footwear, apparel and equipment. It operates a variety of retail shops throughout the world, maintains an active presence on the Internet, primarily through its <nike.com> website where it promotes and sells its goods and services and provides information about its business activities.

4.2 Complainant asserts that it owns numerous trademark registrations worldwide for its NIKE trademark, including United States Registrations nos. 978,952, 1,153,938, 1,243,248, 1,277,066 and 1,214,930 covering a broad range of goods and services. The Complainant also says it owns a French trademark registration for the mark NIKE PARK in connection with apparel, entertainment and retail services (Serial No. 98 716 571), and that it owns numerous registrations for the mark NIKE GOLF, including United States Registration No. 1944436 (Classes 18 and 25; bags, footwear and clothing); Mexican Registration Nos. 443269 (Class 18, bags), 435128 (Class 25; footwear, clothing and headwear); Canadian Registration Nos. 482728 (bags, footwear, clothing, headwear); and United Kingdom Registration No. 2039330 (clothing and footwear). Copies of the trademark registrations mentioned above were exhibited to the Complainant. While all the U.S. trademarks mentioned are registered to Nike, Inc., this does not appear to be the case with the Mexican, French, and United Kingdom marks where the trademark owner in each case is shown as Nike International Ltd., a Bermuda corporation.

5. Parties' Contentions

A. Complainant

5.1 Complainant says that the Respondent appears to have registered the Domain Names at issue on the following dates: <nikepark.com> July 4, 1999; <nikepark.net> July 4, 1999; <nikemen.com> July 17, 1999; <nikegolf.net> July 9, 1999; <nikeshops.com> February 16, 2002.

5.2 The Complainant argues the first element of paragraph 4(a) of the Policy, solely on the basis of confusing similarity. In doing so, it stresses that the Respondent's Domain Names each contain, as their central and most distinctive element, Complainant's registered and world famous NIKE trademark to which, in each instance, are added terms, each of which is readily associated with Complainant's products, services, and/or business, and which sometimes combine to form an additional trademark of Complainant.

5.3 With regard to the rights or legitimate interests of the Respondent, the Complainant asserts that there is no discernible legitimate interest in the "Nike" designation, and it does not appear that the Respondent has ever been commonly known by the "Nike", "Nike Park", "Nike Golf", "Nike Men", or "Nike Shops" designation. Further, the Complainant asserts that Respondent has never used a trademark or service mark similar thereto by which it may have come to be known and that any such use by Respondent would likely have constituted legally actionable infringement and dilution of Complainant's world famous

trademark, nor has Respondent made use of the Domain Names in connection with any business or non-commercial use of the Domain Names. The Complainant concludes that it is far more likely that Respondent is but one of many "cybersquatters" seeking to profit from Complainant's world famous trademark.

5.4 That part of the Complainant's submission in the Complaint directed specifically to the element of bad faith registration and use is set out, verbatim, below.

"1. Respondent registered the domain names in bad faith, since he knew at the time of the fame and Complainant's ownership of its NIKE trademark [sic]. Respondent could readily foresee that people would assume the domain names to be connected with Complainant, that the public would seek out this sites [sic] in the hope of finding Complainant's site, and that Complainant would therefore wish to own and use it.

2. Moreover, Respondent's use and registration of these domain names has prevented Complainant from using its own world-famous trademark in these domain names. This conduct constitutes bad faith registration and use of the domain names under controlling law and precedent.

3. Lastly, Complainant has previously taken action against Respondent to recover domain names Respondent has appropriated. See Nike, Inc. v. Crystal International, ([WIPO Case No. D2001-0102](#)) (returning domain names [nikewomen.com](#), [nikeshop.net](#), [nikeshop.org](#), [nike-shop.com](#), [nike-shop.net](#), and [inike.net](#) to Complainant.) Respondent has demonstrated a pattern of behavior in incorporating Complainant's trademarks in its domain names in bad faith."

B. Respondent

5.5 Respondent has failed to respond to Complainant's contentions as found in the Complaint.

C. No Other Submissions

5.6 The Panel has not received any other requests from Complainant or Respondent regarding further submissions, waivers or extensions of deadlines, and the Panel has not found it necessary to request any further information from the Parties (taking note of the Respondent's default in responding to the Complaint).

6. Procedural Order

6.1 The form and content of the Complaint prompted this Panel to issue a Procedural Order, a copy of which is annexed to this decision. Complainant's Response to the Procedural Order filled in some of the gaps which had been identified in the Complaint, including the relationship between the named Complainant and NIKE International Ltd., the discrepancy in the different contact information given for the Respondent in the Complaint, and the reason for the Complainant not seeking the transfer of the Domain Names in this case at the same time as those in [WIPO Case No. D2001-0102](#) between the same parties – the Complainant says that it was not then aware of them.

6.2 Other aspects of the Complainant's Response to the Procedural Order are set out later in this decision.

7. Discussion and Findings

7.1 The Complaint was submitted on the basis of the provisions of the Registration Agreement in effect between the Respondent and NSI, which incorporates, by reference, the Policy by way of NSI's domain name dispute policy in effect at the time of the dispute. The Policy requires that domain name registrants such as Respondent submit to a mandatory administrative proceeding regarding third-party allegations of

abuse of domain name registration (Policy, paragraph 4(a)).

7.2 The Panel is satisfied that WIPO took all steps reasonably necessary to notify the Respondent of the filing of the Complaint and initiation of these proceedings, and that the failure of the Respondent to furnish a reply or participate in any other fashion is not due to any omission by WIPO (see Procedural History, above).

7.3 Under Rule 5(e) of the Rules, if a Respondent does not submit a Response, in the absence of exceptional circumstances, the Panel shall decide the dispute based upon the Complaint.

Paragraph 15(a) of the Rules addresses the principles to be used in rendering a decision:

"A Panel shall decide a complaint on the basis of the statements and documents submitted and in accordance with the Policy, these Rules and any rules and principles of law that it deems applicable."

It has been said that inferences ought not to be drawn from the default of a Respondent in filing a Response other than those that have been established or can be inferred from the facts presented by the Complainant and that, as a result of the default, have not been rebutted by any contrary assertions of evidence. See: *Terabeam Corp. v. Colin Goldman*, WIPO Case No. D2001-0697. Evidence, not mere assertions, must be presented even in the case of a Response not being filed. This is in accord with those Rules material to this issue. Rule 5(e), in requiring that the decision be "based upon the Complaint" in the absence of a Response, must mean a Complaint which complies with Rule 3(b)(ix) which requires that a Complaint shall "[d]escribe, in accordance with the Policy, the grounds on which the complaint is made including, in particular, . . . (3) why the domain name(s) should be considered as having been registered and being used in bad faith". The provision in question goes on to advise the Complainant that the description should, for the bad faith elements, "discuss any aspects of Paragraphs 4(b) and 4(c) of the Policy that are applicable." This I take to mean, as the circumstances set out in 4(b) are not exclusive, that any aspects of the particular circumstances being relied on to prove these elements in the subject case should be discussed. No such meaningful discussion can take place in a proceeding such as this without consideration of the admissible evidence led in support of the elements which are being advanced. That evidence is required is clear from the general power given to Panels in para. 10(d) which mandates us to "determine the admissibility, relevance, materiality and weight of the evidence." Complaints are determined on the basis of the evidence the parties themselves choose to put before the Panelist. It is not an inquisitorial system and therefore not for the Panel to undertake such a role. See: *Randgold Resources Limited and Randgold & Exploration Co.Ltd. v. Pico Capital Corp.*, WIPO Case No. D2001-1108; *Ascendes Corporation dba MarketTouch v. Market Touch Limited*, WIPO Case No. D2001-1186. I have, therefore, not conducted a search of the web-sites to which the Domain Names in question resolve. To require Panels to conduct extensive searches of their own will likely result in a breach of Rule 10(b) which mandates that "the Panel shall ensure that the Parties are treated with equality and that each Party is given a fair opportunity to present its case." Also, the material time for identifying whether anything is posted on the web-site in question is not after the proceedings have been commenced.

In order to obtain the relief requested under the Policy, Complainant must prove in the Administrative Proceeding that each of the three elements of paragraph 4(a) are present:

(i) that the Domain Name registered by the Respondent is identical or confusingly similar to a trademark or service mark in which the Complainant has rights; and

7.4 The Panel finds that this element has been proved.

(ii) that the Respondent has no rights or legitimate interests in respect of the Domain Name; and

7.5 Due to my findings about the third element, the Panel need not address this.

(iii) that the Domain Name has been registered and is being used in bad faith

7.6 I will focus on bad faith use in dealing with this element and will assume that bad faith registration has

been proved. Here, there is no evidence that Respondent has attempted to sell the Domain Names for profit, has engaged in a pattern of conduct depriving others of the ability to obtain Domain Names corresponding to their trademarks, is a competitor of Complainant seeking to disrupt its business, or is using the Domain Name to divert Internet users for commercial gain. Nor is there such conduct as cyberflying, failing to provide correct or any contact information, not responding to communications which might reasonably be thought to compel a Response, being disingenuous in his or her assertions, or failing to make any preparations to use the Domain Names over an extended period of time. Lack of *bona fide* use on its own is insufficient to establish bad faith, where there is no evidence that Respondent has participated in such conduct as mentioned above. See: *Société des Produits Nestlé S.A. v. Pro Fiducia Treuhand AG*, WIPO Case No. D2001-0916.

In the Complainant's submission number 2 as set out in para. 5.4 above it asserts that "Respondent's use and registration of these domain names has prevented Complainant from using its own world-famous trademark in these domain names. This conduct constitutes bad faith registration and use of the domain names under controlling law and precedent." But, what was this use? There must be something beyond mere registration and it should be a use at the time of the commencement of the UDRP proceedings. It is the opinion of this Panel that mere continuous ownership is not sufficient. There are a number of cases involving what could be characterized as well-known or famous names where Complainants failed to recover a confusingly similar Domain Name for one reason or another, including *Koninklijke Philips Electronics N.V. v. Manageware*, WIPO Case No. D2001-0796, *Mattel Inc. v. Kim Dong Jin*, NAF Case No. 114462, *Koninklijke Philips Electronics N.V. v. Relson Limited*, WIPO Case No. D2001-0003; and *PRL USA Holdings, Inc. v. Polo*, WIPO Case No. D2002-0148. Although a distinguished Panelist has said that whether a trademark is "well known" or "famous" is outside the mandate of UDRP Panels. (See: *Ingersoll-Rand Co. v. Frank Gully*, WIPO Case No. D2000-0021). The name "Nike" is not fanciful. She was the ancient Greek goddess of victory.

In paragraphs 8 and 9 of the Procedural Order this Panel touched upon some of the legal concepts seen as applicable in proving a UDRP case. I now think it helpful to elaborate upon them as they concern the bad faith element.

An Administrative Panel must not deal with propositions not asserted. (See *The Estate of Gary Jennings and Joyce O. Service v. Submarine and J. Ross*, WIPO Case No. D2001-1042.) It is for the Complainant to plead the issues and to support them with some arguments and evidence. (*Jones Apparel Group, Inc. v. jonesapparelgroup.com*, WIPO Case No. D2001-0719; *Chambre de Commerce et d'Industrie de Rouen v. Marcel Stenzel*, WIPO Case No. D2001-0348; *Club Monaco Corporation v. Charles Gindi*, WIPO Case No. D2000-0936; *Tyco International Services AG and Tyco International (U.S.) Inc. v. Paul Quinn*, WIPO Case No. D2000-1740; and *Arturo Salice S.p.A. v. Paul Izzo & Company*, WIPO Case No. D2000-0537; Simply stating the reasons will not normally be sufficient to meet the Complainant's burden of proof. (*Ferrari S.p.A. v. Pierangelo Ferrari*, WIPO Case No. D2001-1004; *Pomellato S.p.A. v. Richard Tonetti*, WIPO Case No. D2000-0493; *Corneliani F. Ili Claudio e Carlalberto Corneliani S.p.A. v. Corantos s.r.l.*, WIPO Case No. D2000-0759). Assertions that any use of the Domain Name by another party would likely mislead or deceive the Complainant's customers, without evidence, is not of much use. (*Capt'n Snooze Management Pty. Ltd. v. Domains 4 Sale*, WIPO Case No. D2000-0488).

7.7 The use of the conjunctive "and" in para. 4(a)(iii) of the Policy means that both bad faith registration and bad faith use must be proven by the Complainant. See: *World Wrestling Federation Entertainment Inc. v. Michael Bosman*, WIPO Case No. D99-0001; *Dow Jones & Company, Inc. v. The Hephzibah Intro-Net Project Limited*, WIPO Case No. D2000-0704; *The Chancellor, Masters and Scholars of the University of Oxford v. D.R. Seagle*, WIPO Case No. D2000-0308; *Baby Creysi Of America, Inc., et al v. Aseoria en Computo Integral, et al* WIPO Case No. D2000-0237; *British Sky Broadcasting Limited v. Domain Reservations*, WIPO Case No. D2000-0507; *Global Media Resources SA v. Sexplanets aka SexPlanets FreeHosting*, WIPO Case No. D2001-1391 (<sexplanets.com>). The complementary provision under the STOP Policy reads "has been registered or has been used in bad faith". If "and" meant "or" under the UDRP, why was "or" used for STOP?

7.8 In *Telstra Corporation Ltd v. Nuclear Marshmallows*, WIPO Case No. D2002-0003 a distinguished Panelist held that the concept of a domain name "being used in bad faith" is not limited to positive action; "inaction is within the concept." He continued as follows:

"... what circumstances of inaction (passive holding) other than those identified in paragraphs 4(b)(i), (ii) and (iii) can constitute a domain name being used in bad faith? This question cannot be answered in the abstract; the question can only be answered in respect of the particular facts of a specific case. That is to say, in considering whether the passive holding of a domain name, following a bad faith registration of it, satisfies the requirements of paragraph 4(a)(iii), the Administrative Panel must give close attention to all the circumstances of the Respondent's behaviour. A remedy can be obtained under the Uniform Policy only if those circumstances show that the Respondent's passive holding amounts to acting in bad faith."

7.9 Evidence which proves bad faith use comes primarily from three sources. Communications between the parties, particularly statements made by a Respondent, demonstrate bad faith use. Cease and desist letters relating to the alleged offending use have been effective in drawing out the Respondent. What is posted on a web-site, often but not always the site to which the Domain Name resolves, performs the same function, e.g. where the web-site advertises a competing product, displays pornographic material, or links to such web-sites. On the other hand, if there was a possible fair use or a disclaimer on the web-site, the result may be otherwise. Another way of proving bad faith use through evidence is to obtain particulars about the Respondent and its enterprises, past history, reputation and ownership of other Domain Names, not the subject of the case at hand. There are other evidentiary indicia such as false contact information, making untruthful statements in a Response, and the like. In this case, although it had two opportunities to do so, the Complainant failed to produce any such evidence. In this regard it should be noted that my Procedural Order included the following specific question:

"7. When was the site entered, and what were the contents thereof, including disclaimers if any?"

The Complainant did not address this question.

7.10 The Complainant, in its Complaint in this case, says:

"On August 7, 2000, Complainant sent a letter to Respondent placing Respondent on notice of his ongoing trademark infringement and dilution of Complainant's trademarks, and seeking transfer of Respondent's domain name. Complainant's letter also offered to reimburse Respondent for his out-of-pocket costs in registering the domain name. (see Annex F). Respondent never responded."

The Complainant says that it relies on that letter to prove the instant case. In the letter it is asserted that "your registration and ownership of these domain names constitutes trademark infringement, and violates the newly enacted United States Cyber Piracy Prevention Act of 1999. NIKE hereby requests that you transfer this name to NIKE immediately." For this purpose the sender of the letter encloses transfer documents for signature. The only name, <nikewoman.com>, covered by that letter, was one of those dealt with in WIPO Case No. D2001-0102, decided March 19, 2001, but that letter was not mentioned in the decision in that case between these same parties. Under the circumstances, it is difficult for this Panel to conclude that the Respondent in the instant case should have a finding of bad faith use made against it for not having responded to a much earlier letter about names dealt with in another case.

7.11 The Complainant asserts that its victory in the earlier case, *Nike, Inc. v. Crystal International*, WIPO Case No. D2001-0102 should be used against the same Respondent in this case. It has been held that previous decisions which decide an element favourable to Complainant in the instant case are not particularly helpful as they will have undoubtedly turned upon the evidence before the deciding Panel. See: *Harrods Limited v. Virtual World Internet*, WIPO Case No. D2002-0396. The earlier decision between the parties to the instant case does not identify the evidence provided by the Complainant in support of bad faith use sufficiently to be of help here.

7.12 In its Response to the Procedural Order the Complainant says that it did not attempt to contact Respondent before initiating the UDRP action and provides no evidence that it attempted to view the web-sites to which the Domain Names in issue resolve but rather merely asserts that:

"Under the current UDRP Rules, Complainant is under no duty to contact Respondent before filing a UDRP action. Moreover, Complainant believes that its previous letter and the decision in WIPO D2001-0102 provide Respondent sufficient notice that its registration of domain names incorporating

Complainant's NIKE trademark violates the U.S. Anti-Cyberpiracy Prevention Act ("ACPA"), and infringes Complainant's rights under numerous international laws."

". . . Complainant notes that the ACPA would apply to Respondent regardless of Respondent's nationality. The ACPA provides an in rem cause of action against the property of the domain name itself. Thus, the nationality of the domain name's owner is irrelevant."

Other than noting that the letter, in addition to the *in rem* aspect of ACPA, threatens "significant financial penalties", and that the Registrar is Canadian, this Panel takes no issue with the Complainant's belief as expressed above. However, it is not my remit to apply the ACPA nor "numerous international laws". The jurisdiction of this Panel is to be found wholly within the UDRP with the only remedy being a transfer or cancellation of the Domain Names in respect of which this matter is submitted. In sum, Complainant appears not to place any meaningful reliance on active use of the Domain Names in question subsequent to their registration, nor upon passive use as this Panel understands it to be necessary as laid down in *Telstra Corp. Ltd. v. Nuclear Marshmallows* WIPO Case No. D2000-0003, and other cases which have followed it.

7.13 Para. 4(a)(iii) requires proof that "your domain name ... is being used in bad faith". Without appropriate evidence of use, either active or passive, this Panel cannot find this element to have been proved by the Complainant. Speculation based on assertions does not amount to proof, the onus of which is on the Complainant.

8. Decision

For the foregoing reasons, the Panel decides that the Complainant fails in its request that the Domain Names <nikepark.com>, <nikepark.net>, <nikemen.com>, <nikegolf.net>, and <nikeshops.com> be transferred to the Complainant from the Respondent.

Cecil O.D. Branson, QC
Sole Panelist

Dated: August 2, 2002

Addendum

PROCEDURAL ORDER

pursuant to Rule 12 of the WIPO Supplemental Rules

Nike, Inc. v. Crystal International

Case No. D2002-0352

1. Upon reviewing the Complaint in this case the Panel's initial view was that it ought to be disallowed as being deficient in its content. A good number of Panels, including this one, have said that an Administrative Panel must not deal with propositions not asserted. It is for the Complainant to plead the issues and to support them with some arguments and evidence. Simply stating reasons will not normally be sufficient to meet the Complainant's burden of proof. More particularly, it has been held by a Panel that the mere assertion that any use of the Domain Name by another party would likely mislead or deceive the Complainant's customers, without evidence, is not of much use. With these general admonitions in mind, this Panel is concerned about the failure of the Complaint to address a number of material facts which ought to be within its knowledge.

2. It is noted that the sole Complainant in this case is Nike Inc. However, the Complaint and Annexes thereto shows that the Mexican, French and United Kingdom trademarks mentioned are owned by Nike International Ltd., a Bermuda corporation. The Complaint does not disclose any relationship between Nike International Ltd. and Nike Inc., either generally or specifically regarding any licensing agreements for trademarks. Generally, in the Complaint, the Complainant whenever it refers to its name states it as being simply "Nike". Nowhere is there any explanation of the place of Nike International Ltd. within the corporate structure, nor is there any mention of licence agreements concerning the use of any trademarks. Nike International Inc. is not mentioned at all. If the Mexican, French and United Kingdom marks are considered material by the Complainant, the aforesaid information should have been provided.

3. The Complainant, in its Complaint says as follows:

On August 7, 2000, Complainant sent a letter to Respondent placing Respondent on notice of his ongoing trademark infringement and dilution of Complainant's trademarks, and seeking transfer of Respondent's domain name. Complainant's letter also offered to reimburse Respondent for his out-of-pocket costs in registering the domain name. (see Annex F). Respondent never responded.

Here, it should be noted that the Complaint says:

7. All information known to the Complainant regarding how to contact the Respondent is as follows:

*Joowan Lee
Crystal International
RM609 HyoChunB/D SeoChoDong
1425-10 SeoChoKu
Seoul, 137-070 KR
Tel: 822-555-1554*

Despite this, in an earlier paragraph, relying on Network Solutions, Inc.'s Whois database, in addition to the above contact information it is shown that the Respondent can be contacted through an e-mail address "maxion@maxion.co.kr". The August 7, 2000, letter directed to Joowan Lee has an altogether different address in Seoul, Korea. This discrepancy is not explained.

4. The August 7, 2000, letter refers to a single Domain Name, <nikewoman.com>. In the letter a belief is expressed that "your registration and ownership of these domain names [sic] constitutes trademark infringement, and violates the newly enacted United States Cyber Piracy Prevention Act of 1999. NIKE hereby requests that you transfer this name to NIKE immediately." Is it the Complainant's contention that the United States Cyber Piracy Prevention Act of 1999 applies to a Korean national? If so, why? The August 7th letter encloses transfer documents for signature. Do those documents include any of the names under consideration in the case before this Panel, i.e., WIPO Case No. D2002-0352, or does it relate only to the name <nikewoman.com> despite the reference to "these domain names" above?

5. The name <nikewoman.com> was one of those dealt with in WIPO Case No. D2001-0102, the decision for which was given on March 19, 2001. Is it Complainant's submission that the Respondent in this case No. D2002-0352 should have a finding of bad faith use made against it for not having responded to the August 7, 2000, letter about another name, particularly given the length of time intervening, and WIPO Case No. D2001-0102 in which a decision was rendered on March 19, 2001, well before the

commencement of the case before this Panel?

6. In light of the above, there are further material facts which should be within the knowledge of the Complainant which have not yet been disclosed. These include the following:

1. Why were no proceedings taken against the Respondent in 2001 for the four names registered in July 1999, when as the Complainant states that it "has been careful to prevent conflicting uses from emerging" in regard to its trademark and similar second-level Domains. The Registrar of most of the names involved in the 2001 case was the same and at least one of the names before that earlier Panel was registered on the same day as <nikemen.com> in this case – July 17, 1999.

2. There is no evidence of the attempts "to contact Respondent at all available addresses", other than the August 7, 2000, letter? Were they by telephone, email, in-person or by registered mail?

3. Was the Respondent's contact information correct?

4. What were the contents of such communications? Did they require an answer?

5. Why was nothing done between August 7, 2000, and April 9, 2002, the date of filing of the Complaint in this case?

6. Have any of the names in question been used? If so, when, and for what purpose?

7. When was the site entered, and what were the contents thereof, including disclaimers if any?

8. What attempts were made to ascertain whether Respondent owns other names than those involved in this case and WIPO Case No. D2001-0102?

9. If so, how many does it own and what are they?

10. It is not clear from Complainant's submission concerning bad faith whether it is relying on any one or more of the four stated circumstances of evidence of registration and use in bad faith set out in paragraph 4b of the UDRP, or whether it is relying on other bases on which this Panel is expected to find bad faith registration *and* use.

11. The third, and last, paragraph under the Complainant's submission in regard to Respondent's bad faith reads as follows:

Lastly, Complainant has previously taken action against Respondent to recover domain names Respondent has appropriated. See Nike, Inc. v. Crystal International, (WIPO Case No. D2001-0102) (returning domain names nikewomen.com, nikeshop.net, nikeshop.org, nike-shop.com, nike-shop.net, and inike.net to Complainant.) Respondent has demonstrated a pattern of behavior in incorporating Complainant's trademarks in its domain names in bad faith.

Is this argument directed to paragraph 4b(ii) of the UDRP? If so, is the Complainant taking the position that, despite the requirement in paragraph 4a(iii) of proof that the Domain Name has been registered *and* is being used in bad faith, that this language should be read disjunctively? What, for instance, if the Respondent registered the names in question in bad faith but did nothing more?

1. Is the Complainant relying on WIPO Case No. D2001-0102 as a precedent which this Panel ought to follow, as the parties were the same and the names bore some similarity to those in issue our case? If so, what was submitted in the Complaint in the earlier case, as the decision in that case does not spell out the bases on which bad faith registration and use was argued.

7. As stated above, the preliminary decision of this Panel was to disallow the claim on the basis of numerous deficiencies in the pleadings. These Complaints are determined on the basis of the evidence the parties themselves choose to put before the Panel. It is not an inquisitorial system and therefore not for the

Panel to undertake such a role. See *Rengold Resources Limited and Rengold & Exploration Co. Ltd. v. Pico Capital Corp.*, WIPO Case No. D2001-1108 and *Ascendes Corporation dba MarketTouch v. Market Touch Limited*, WIPO Case No. D2001-1186. In a similar vein, it must be recognized that Complainants, having the onus of proof upon them, ought to give considered thought to the drafting of the Complaint, taking into account that there is no right of reply if a Response is filed and, further, that a Response may not be filed. In the latter case, the Panel must decide on the basis of the record as presented. Yet, in a case such as this, not to order transfer of the Domain Names in question, has been thought by some to be too draconian a penalty for bad pleading. I would dissent from this as a general proposition as a Respondent is entitled to review the Complaint and make a decision based thereon that it need not file a Response where the case has not been adequately proved. Previous Panels have dealt with these situations in a number of ways such as a strong criticism of the way in which the case was presented, but ordering a transfer of the name in any event, or ruling against the Complainant without prejudice to the Complainant refileing its Complaint with better pleadings and evidence, or as this Panel is inclined to do, seek better particulars. To go ahead and order transfer of the names in the face of deficient pleadings and evidence could tarnish the integrity of the process, and encourage others to do so. Nor do I think that dismissing the case outright, with or without comment with regard to whether a refiled Complaint can be made would be appropriate. This could delay unnecessarily a final resolution of the matter with the extra expense of starting afresh without knowing whether the refiled Complaint would be accepted.

8. Paragraph 15(a) of the Rules instruct Panels to "decide a Complaint on the basis of the statements and documents submitted in accordance with the Policy, these Rules and any rules and principles of law that it deems applicable". This, in my view, is exemplified by article 18 of the UNCITRAL Model Arbitration Law, sometimes referred to as the "Magna Carta of Arbitration Procedure" which says "The parties shall be treated with equality and each party shall be given a full opportunity of presenting his case." An equivalent statement is to be found in virtually all national arbitration laws and the rules of all major international arbitration institutions including WIPO in article 38(b) of its Arbitration Rules.

9. This Panel therefore orders that the Complainant be given an opportunity to respond both specifically and generally to the concerns and questions above in writing delivered to the WIPO Center no later than Tuesday, July 16, 2002. The Respondent will be served with a copy of this document at the same time, and shall then have until 12 noon GMT on Wednesday, July 24 to file a Response both to the Complaint as originally filed by the Complainant and to any further supplemental material filed in response to this Procedural Order. Both filings shall include any exhibits or other documentation necessary to support the submissions made. The time for the filing of the Panel's decision in this matter will have to be adjusted accordingly. Exhibits not available in electronic form shall be faxed to the Center, with hard copies to follow by courier. The Panel will disregard in their entirety any late filed submissions.

10. This Panel will enter into its final consideration of this matter after the time period above has expired and, barring extenuating circumstances, propose to render a final decision by August 5, 2002.

Cecil O.D. Branson, QC
Sole Panelist

Dated: July 4, 2002



WIPO Arbitration and Mediation Center

ADMINISTRATIVE PANEL DECISION

Dell Computer Corporation .v. MTO C.A. and Diabetes Education Long Life

Case No. D2002-0363

1. The Parties

The Complainant is Dell Computer Corporation of One Dell Way, Round Rock, Texas 78682, United States of America.

The Respondents are MTO C.A. of Mariedy #2, P. Fijo, Falcon Estade Falcon, Venezuela and Diabetes Education Long Life™ - Dell™, a division of Master Tec Occidente C.A. (MTO C.A.) of Edificio Mariedy No. 2, Prolongacion Calle Progreso, Esquina Pumarrosa, Punto Fijo, Estado Falcon, Venezuela.

2. The Domain Name and Registrar

The domain names at issue are:

| | | |
|---------------------|--------------------------|----------------------|
| <bancondell.com> | <dellaboutus.com> | <dellafrica.com> |
| <dellamerica.com> | <dellamericas.com> | <dellargentina.com> |
| <dellaruba.com> | <dellaaustralia.com> | <dellaustria.com> |
| <dellbahamas.com> | <dellbelgium.com> | <dellbelize.com> |
| <dellbermuda.com> | <dellbolivia.com> | <dellbrasil.com> |
| <dellbrazil.com> | <dellca.com> | <dellcaribbean.com> |
| <dellcaribe.com> | <dellcentralamerica.com> | <dellchile.com> |
| <dellcolombia.com> | <dellcontact.com> | <dellcostarica.com> |
| <dellcuba.com> | <dellcustomer.com> | <delldenmark.com> |
| <dellearth.com> | <dellecuador.com> | <dellelsalvador.com> |
| <dellengland.com> | <dellequator.com> | <delleuro.com> |
| <dellfinland.com> | <dellgermany.com> | <dellgreece.com> |
| <dellguatemala.com> | <dellhawaii.com> | <dellhongkong.com> |
| <dellindonesia.com> | <dellinvestors.com> | <dellisrael.com> |
| <dellitaly.com> | <delljapan.com> | <dellkuwait.com> |
| <dellmex.com> | <dellmexico.com> | <dellmiddleeast.com> |
| <dellna.com> | <dellnetherlands.com> | <dellnewzealand.com> |
| <dellnicaragua.com> | <dellnorthamerica.com> | <dellnorway.com> |
| <delloffers.com> | <dellpakistan.com> | <dellpanama.com> |

| | | |
|-----------------------|------------------------|-------------------------|
| <dellportugal.com> | <dellpuertorico.com> | <dellrussia.com> |
| <dellsa.com> | <dellscotland.com> | <dellsingapore.com> |
| <dellsouthafrica.com> | <dellsouthamerica.com> | <dellspain.com> |
| <dellsweden.com> | <dellswitzerland.com> | <delltaiwan.com> |
| <delluae.com> | <delluk.com> | <dellunitedkingdom.com> |
| <delluruguay.com> | <dellvenezuela.com> | <dellwww.com> |
| <usadell.com> | <usdell.com> | <dellchina.com> |
| <delleurope.com> | <dellfrance.com> | |

The Registrar is Tucows.com, Inc., Toronto, Canada.

3. Procedural History

The WIPO Arbitration and Mediation Center [the Center] received the Original Complaint on April 17, 2002 [electronic version] and on April 22, 2002 [hard copy]. On April 23, 2002, the Center transmitted via email notification of Complaint deficiency. The Center received Amendment (1) to the Complaint on April 23, 2002 [electronic version] and on April 26, 2002 [hard copy]. The Center received Amendment (2) to the Complaint on May 14, 2002 [electronic version] and on May 16, 2002 [hard copy]. By Amendment (2) to the Complaint the Complainant added three further domain names, which were registered by the Respondent after the date [April 17, 2002] when the Original Complaint was transmitted to the Center. The Original Complaint, Amendment (1) to the Complaint and Amendment (2) to the Complaint are hereinafter collectively referred to as "the Complaint".

The Center verified that the Complaint satisfies the formal requirements of the ICANN Uniform Domain Name Dispute Resolution Policy [the Policy], the Rules for Uniform Domain Name Dispute Resolution Policy [the Rules], and the WIPO Supplemental Rules for Uniform Domain Name Dispute Resolution Policy [the Supplemental Rules]. The Complainant made the required payment to the Center.

The formal date of the commencement of this administrative proceeding is April 24, 2002.

On April 22, 2002 the Center transmitted via email to Tucows.com, Inc. a request for registrar verification in connection with the eighty domain names at issue in the Complaint and on the same day Tucows.com, Inc. transmitted by email to the Center Tucows' verification response confirming that the registrant is Diabetes Education Long Life - Dell (trademark) and that the contact for administrative, billing and technical purposes is Dell™ <diabetes@dellwww.com> all of the same address at Estado Falcon, Venezuela.

On May 23, 2002 the Center transmitted via email to Tucows.com, Inc a request for registrar verification in connection with the additional three domain names at issue in Amendment (2) to the Complaint and on the same day Tucows.com, Inc transmitted by email to the Center Tucows' verification response confirming that the registrant is Diabetes Education Long Life - DELL and that the contact for administrative billing and technical purposes is DELL™ <diabetes@dellwww.com> all of the same address at Estado Falcon, Venezuela.

the Rules, the Center transmitted by on April 24, 2002 to Respondent the Notification of Complaint and Commencement of the Administrative Proceeding. The Center advised that the Response was due by May 14, 2002. On the same day the Center transmitted by fax and by mail copies of the foregoing documents to Respondent at the addresses provided by the Complaint and Tucows.com, Inc.

The Center received the Respondent's Response on May 9, 2002 [electronic version] and on May 15, 2002 [hard copy]. On May 10, 2002 the Center transmitted Acknowledgement of Receipt of Response to the Respondent and to the Complainant.

Having received on May 15, 2002 Mr. David Perkins' Declaration of Impartiality and Independence and his Statement of Acceptance, the Center transmitted to the parties a Notification of Appointment of Administrative Panel and Projected Decision Date, in which Mr. David Perkins was formally appointed as the Sole Panelist. The Projected Decision Date was June 11, 2002. The Sole Panelist finds that the Administrative Panel was properly constituted and appointed in accordance with the Rules and the Supplemental Rules.

On May 23, 2002 the Panel issued a Procedural Order admitting Amendment (2) to the Complaint and providing the Respondent with an opportunity to submit a supplemental Response by May 27, 2002, such Response to be limited to the issues raised in Amendment (2) to the Complaint. On May 28, 2002 the Respondent duly filed a Supplemental Response.

Having verified the communication records in the case file, the Administrative Panel finds that the Center has discharged its responsibility under para. 2(a) of the Rules "to employ reasonably available means calculated to achieve actual notice to Respondents". Therefore, the Administrative Panel shall issue its Decision based upon the Complaint, Amendment (1) to the Complaint, Amendment (2) to the Complaint, the Response, the Supplemental Response, the Policy, the Rules and the and the Supplemental Rules.

4. Factual background

4.1 *The Complainant's Business*

The Complainant was founded in 1984. It is the world's largest direct seller of computer systems. In its fiscal year [February 1, 2001 to January 31, 2002] it had revenues of approximately US\$31.2 billion.

4.2 *The Complainant's DELL trademark*

4.2.1 The Complainant began using the name and mark DELL as a tradename, trademark and service mark in 1987. The Complainant is the proprietor of more than 30 US trademark registrations and applications containing the mark DELL. Copies of the following are annexed to the Complaint:

| Country | Registration No. | Mark | Class(es) | Application/ Registration Dates |
|---------|------------------|------|-----------|--|
| USA | 1,498,470 | DELL | 9 | Filed: December 9, 1987 Registered: August 2, 1986 |

| | | | | |
|-----|-----------|--------------------|----|---|
| | | | | Registered: October 9, 1990 |
| USA | 1,860,272 | DELL (Stylised) | 9 | Filed: February 27, 1992 Registered: October 25, 1994 |
| USA | 2,236,785 | DELL | 40 | Filed: March 19, 1998 Registered: April 6, 1999 |
| USA | 2,390,851 | WWW.DELL L.COM* | 9 | Filed: August 26, 1998 Registered: October 3, 2000 |

*The WWW.DELL.COM mark was first used in commerce in December 1997.

4.2.2 In addition, the Complainant uses a family of marks combining DELL with another component. These include but are not limited to:

| Country | Registration No. | Mark | Class(es) | Application/ Registration Dates |
|---------|------------------|-------------------------------|-----------|--|
| USA | 2,030,084 | DELL DIMENSIO N | 9 | Filed: January 11, 1996 Registered: January 14, 1997 |
| USA | 2,284,782 | DELL PRECISION | 9 | Filed: March 5, 1998 Registered October 12, 1999 |
| USA | 2,333,902 | DELL FINANCIAL SERVICES | 42 | Filed: August 13, 1997 Registered: March 21, 2000 |

4.2.3 The DELL mark and variations of it are also registered by the Complainant in more than 130 countries around the world.

4.2.4 In the Respondent's country, Venezuela, the Complainant sells products and owns a number of trademark registrations for DELL for use in relation to computer products and services. These include:

| Registration Number | Mark |
|---------------------|-----------------|
| P-208279 | DELL |
| P-208280 | DELL |
| P-208281 | DELL |
| P-208284 | DELL |
| P-175192 | DELL (stylised) |
| P-217855 | WWW.DELL.COM |
| S-13926 | WWW.DELL.COM |
| N-41282 | WWW.DELL.COM |

4.2.5 The Complainant extensively advertises and promotes its trademarks, products, services and image. During the 2001 fiscal year alone, the Complainant spent over US\$431 million in advertising and promotion. The Complainant states that as a result of these activities and of its business, the DELL mark has become an asset of incalculable value to the Corporation.

4.3 *The Complainant's Internet Business*

The Complainant conducts business on the Internet through numerous DELL domain names. The earliest of these, <dell.com>, was registered on November 22, 1988. By the end of the fiscal year 2000 [February 1, 2000 to January 1, 2001] online internet sales by the Complainant accounted for almost 50% of its revenue and averaged US\$40 million per day. The domain names used by the Complainant include:

| | | |
|----------------------|----------------------|----------------------|
| <dell.com> | <e-dell.com> | <dellcomputers.com> |
| <delldirect.com> | <dellnet.com> | <dellfoundation.org> |
| <dell rowser.com> | <dellfactory.com> | |
| <dell webpc.com > | <dellhost.com> | |
| <dell auction.com> | <dell auctions.com> | |
| <dellplus.com> | <dell4me.com> | |
| <dellexchange.com> | <dellpoweredge.com> | |
| <dell precision.com> | <dell attitude.com> | |
| <delldimension.com> | <dellselectcare.com> | |

4.4 *Complainant's Patronage of diabetes*

The Complainant believes that medical education about diseases, including diabetes, is an important and worthy cause. The Complainant is a supporter of the Juvenile Diabetes Research Foundation's annual walk to cure diabetes. Over 1500 of the Complainant's employees, including the corporation's founder [Michael Dell] and its President [Kevin Rollins], participated in the 2001 Austin Walk for the cure, raising over US\$130K in that one event.

4.5 *The Respondents*

- 4.5.1 The Respondents are represented by Glen McShand of Naples, Florida. He is the President and founder of Master Tec Corporation - also of Naples, Florida - which is described in the Response as;

"... a very well known engineering firm that serves the petroleum and mining industry worldwide."

Master Tec Occidente C.A. [MTO C.A.] of Venezuela is described as a sister company of Master Tec Corporation. The Response states:

"Master Tec Corporation and Master Tec Occidente C.A. have hundreds of trademarks well known by the Petroleum, Mining, Aerospace, Government, Health, Medical and general industry".

- 4.5.2 In February 1999 "Dell™ Diabetes Education Long Life™" was founded as a Division of MTO C.A. The parties involved were America Tec Corporation: Tec Corporation: Master Tec Corporation [all of the USA]; MTO C.A. [of Venezuela] and Mr. McShand. The Response explains that in August 1995 Mr. McShand's infant son, Ian (21 months old), was diagnosed with Type I diabetes. Mr. McShand and his wife started to help other families struck with that disease through education, support and counselling. It appears that the concept behind the Respondent organization is to provide assistance worldwide to diabetes suffers and/or their families.

The original registrant of the domain name in issue, BANCONDELL.COM, was AZTEC of Naples, Florida. The Original Complaint was filed on April 17, 2002. The next day [April 18, 2002] all 80 domain names were transferred from MTO C.A. to Diabetes Education Long Life - DELL (Trademark), which is now the effective Respondent in this administrative action. The additional 3 domain names in issue - identified in Amendment (2) to the Complaint - were registered by the Diabetes Education Long Life - DELL.

5. The Parties' Contentions

5.1 *The Complainant's Case*

5.1.1 The Complainant's case is that the domain names in issue are identical or confusingly similar to its DELL and DELL family of trademarks and service marks, that the Respondent has no rights or legitimate interest in respect of those domain names, and that such domain names were registered and are being used in bad faith.

5.1.2 The Complainant states that it first became aware of the domain names in issue through a domain name Watch Report, the first in January 2002 which identified 62 of the domain names and the second in March 2002 which identified the remaining 18 domain names. After filing the Original Complaint [on April 8, 2002], the Complainant became aware of 3 additional registrations, namely:

<dellfrance.com>; and <dellchina.com> registered April 20, 2001 and <delleurope.com>

registered May 1, 2002 and these were added in Amendment (2) to the Complaint.

5.1.3 The Complaint exhibits the following inter partes correspondence with the Respondents:

February 12, 2002: The Complainant's attorneys addressed a *cease and desist* letter to Mr. McShand in relation to 62 domain names [identified in their January 2002 domain names Watch Report] and 4 of the 5 US registered trademarks [referred to in paragraphs 4.2.1 above].

February 19, 2002: The Complaint exhibits an affidavit from Jennifer Brockmeyer relating to two conversations with Mr. McShand on that date. Ms Brockmeyer is a project assistant with the Complainant's attorneys [Jones Day Reavis & Pogue of Columbus, Ohio]. Her testimony is as follows:

- Mr. McShand stated that his active website, <www.dellwww.com>, was used for diabetes education.
- Mr. McShand stated, that although the domain names were not for sale, the Complainant could make an offer and he would discuss any such offer with his partners.
- Mr. McShand said that if the Complainant persisted with threats or legal action, he would post on his websites the fact that Dell Computer Corporation was trying to shut down a children's diabetes website.

Mr. Dreitler [of the Jones Day Firm] and Mr. McShand when the latter stated that his intention was to make money from the 62 sites complained of in the *cease and desist* letter.

- The Complaint also exhibits an affidavit from Mr. Dreitler, which refers to a follow-up conversation which he had later the same day with Mr. McShand. His testimony is as follows:
- Mr. McShand stated that he would not transfer the 62 domain names in issue to the Complainant.
- Mr. McShand said he was entitled to use DELL as his worldwide domain name. There was, therefore, no need for him to use a domain name incorporating the word *diabetes*.
- When asked if he was putting so much work into the domain names with no expectation of making money, Mr. McShand replied:

"Of course I intend to use them to make money"

Mr. McShand volunteered that he now had more than 80 DELL domain names.

February 20, 2002: email to Jones Day from Mr. McShand in response to the *cease and desist* letter of February 12. The salient points of that letter are:

"Dell" is a generic word. It's dictionary definition means "A small, secluded, wooded valley."

- Many hundreds of companies are doing business under names which include the word "dell". For example, dell purse book, dell crossword puzzles etc.
- The Complainant has no entitlement to claim exclusive ownership of the word "dell".
- The Respondent is not in the business of manufacturing computers.
- DELL is an acronym for "Diabetes Education Long Life".
- The Respondent's web pages are directed to US citizens suffering from or concerned with diabetes. As his audience expanded to other countries, he would register DELL with the TLD for each country.

The domain names were not for sale.

The letter then reads in the final paragraph:

"If your client is interested in my domains, he or his representatives should approach me in a better way. I am always open to help."

5.1.4 The Respondent's <dellwww.com> website

The front page of this website is exhibited to the Complaint. It is captioned:

"Children with Diabetes Type I
The Dell or wooded valley is fragile like our children. Education is key for long life."

The web page then gives a synopsis of Mr. McShand's story of his son's illness [see, paragraph 4.5.2 above] under the caption.

"Ian's Story"

Then under another caption

"Our DELL Sites"

the web page lists over 60 of the DELL prefixed domain names in issue in the Complaint.

- 5.1.5 Of these, the only active domain name is <dell.www.com>. This, the Complaint says, should be compared to the Complainant's own <www.dell.com> website registered on November 22, 1988 [see, paragraph 4.3 above]. First, addition of the suffix *www* does not distinguish that domain name in issue from the Complainant's DELL trademark. Second, it is clearly intended to trap those wishing to visit the Complainant's website but who mistakenly type the *www* after DELL instead of before it. This is characterized as *typo-piracy*, the Complaint referring to the following decisions under the Policy.

NIKE, Inc .v. Alex Nike, WIPO Case No. D2001-1115. In that case the domain name in issue was <wwwnike.com>. No response was filed. The Panel stated that it had:

"... no hesitation in accepting the Complainant's submission that the only distinctive element of the Domain Name is the very well known mark NIKE, the Complainant's trade mark. The addition of the letters "www" as a prefix in the context of a domain name is wholly non-distinctive... . The Domain Name is undoubtedly confusingly similar to the trademark NIKE."

World Wrestling Federation Entertainment Inc .v. Matthew Bessette, WIPO Case No. D2000-0256. The domain names in issue were <www.wwf.com> and <www.stonecold.com>. No Response was filed. Finding for the Complainant, the Panel stated:

"Respondent's Domain Names each differs from Complainant's domain names by a single character, a period between the common third level domain, "www", and the second level domain name. The Panel agrees with the Complainant's assertion that Respondent is a "typo-pirate" who attempts to mislead Internet users who mistakenly omit the period between "www" and the second level domain name. Cybersquatters commonly register domain names such as the ones at issue, in order to take advantage of and profit from the unavoidable fact that typographical errors occur."

- 5.1.6 Further, the Complainant states that none of the domain names in issue relate, *ex facie*, to diabetes or education. The Complaint exhibits, for example, an available domain name which is appropriately descriptive of the Respondent's asserted aims, namely:

<diabeteseducation.net>.

Where circumstances such as this prevail, it is an indication of bad faith intent in registering the confusingly similar trademark. Here, the Complaint cites:

Cir. 2001). This is a decision of the US Court of Appeals for the Fourth Circuit. The domain name in issue was *vw.net*, which Volkswagen said constituted a bad faith intent to profit from the famous VW trademark. At the time Virtual Works Inc registered the domain name in issue, available alternative domain names more closely describing its business were available, these included:

<vwi.net>; <vwi.org>; <virtualworks.net>; and <virtualworks.org>.

The Appeal Court upheld the District Court's decision granting summary judgment to Volkswagen, the Court citing as an indicia of bad faith intent under the 1999 Anticybersquatting Consumer Protection Act [ACPA] the availability of <vwi.net> and .org at the time Virtual Worlds Inc registered <vw.net>.

5.1.7 **February 21, 2002:** following receipt of Mr. McShand's email dated February 20, 2002 [paragraph 5.1.3 above], Mr. Dreitler replied by email advising him that, although the Complainant had hoped to resolve the dispute informally, his cybersquatting activities would result in the matter being dealt with at "... a more formal forum".

5.1.8 **February 21, 2002:** later that day Mr. McShand replied by email reiterating his position that the Complainant could not:

"... claim exclusive ownership in the entire planet, all services and/or goods with the generic word dell."

The Complaint states that, adopting Mr. McShand's theory, it would not be possible to obtain registered trademarks in dictionary words such as "coke"; "delta"; "sprite"; "ivory" etc. *En passant*, the Panel would observe that Mr. McShand did not in his email of February 20, 2002 appear to deny the Complainant's rights in the DELL trademark for computers and computer related goods and services but was saying that the Complainant could not assert rights in that trademark over other non-computer related services, such as the Respondent's educative website for diabetes sufferers and those involved with diabetes sufferers. That said, the Complainant points to the fact that the Policy does not require a Complainant to demonstrate exclusive rights to a trademark for each and every good and service.

5.1.9. **April 12, 2002:** Mr. McShand implemented the threat made in his conversation on February 19, 2002 with Ms Brockmeyer [see, paragraph 5.1.3 above] that he would draw the dispute to the attention of computer magazines. There is exhibited to the Complaint an article entitled "Dispute over Dell Domains".

April 18, 2002: the Respondent sent an email to the Complainant in, inter alia, the following terms:

"Your company Dell Computer Corporation must stop harassing our business. Your actions are going to oblige us to take further actions. We will communicate this issue to all news and editors around the globe."

5.1.10 **Identical or Confusingly Similar**

confused with the Complainant's family of DELL trademarks and domain names. All those domain names contain the DELL trademark combined with generic terms or the name of a country where the Complainant carries on business under or by reference to the DELL name and mark. Of the 54 separate country names - only counting duplicates like <dellmex.com> and <dellmexico.com> once and not counting non-country specific domain names like <dellsouthamerica.com> - the Complainant carries on business or directly sells its products in 49 of those 54 countries.

- 5.1.11 As to the Respondent's <dellwww.com> domain name, the Complainant's case is that it is to all intents and purposes identical [see, paragraph 5.1.5 above].
- 5.1.12 In support of its case that domain names comprising a trademark with a generic term have been held to be confusingly similar with the Complainant's trademark, the Complainant refers to the following cases under the Policy.

Brown & Bigelow Inc .v. Site Ads. Inc. NAF Case No. FA0011000096127, where the domain name in issue, <hoylecasino.com>, was found to be confusingly similar to the Complainant's HOYLE trademark. The Panel referring to *The Body Shop International PLC .v. CPIC Net and Syed Hussain*, WIPO Case No. D2000-1214 and *Space Imaging*, AF0298 cases [separately summarized below], the latter as authority for the proposition that a combination of the Complainant's mark with a generic term that has an obvious relationship to the Complainant's business gives rise to confusing similarity.

The Body Shop International PLC .v. CPIC Net and Syed Hussain, WIPO Case No. D2000-1214, where the domain name in issue, <bodyshopdigital.com> was found to be confusingly similar to the Complainant's well-known THE BODY SHOP name and mark.

- 5.1.13 In support of its case that a domain name comprised of the Complainant's trademark followed by country designations has been held to be confusingly similar, the Complainant refers to the following cases.

America Online, Inc .v. Asia On-Line This Domain for Sale, NAF Case No. FA0004000094636, where the domain names in issue included <ao-laustralia.com>; <ao-lchina.com>; <ao-leurope.com>; <ao-lhonkong.com> etc were found to be confusingly similar with the Complainant's well-known AOL name and trademark.

Bloomberg L.P. .v. Sein M.D., NAF Case No. FA0101000096487, where the domain names in issue, <bloombergchina.com> and <bloombergjapan.com> were held to be confusingly similar with the Complaint's BLOOMBERG name and trademark, the Panel stating:

"The mere addition of a geographic identifier does not render the distinctive trademark BLOOMBERG diminished, nor does an addition of the words CHINA and JAPAN controvert the ownership of trademark or service mark rights in the Complainant."

5.1.14 *Rights or Legitimate Interests*

Respondent registered the 83 DELL domain names in issue without any legitimate right or interest in respect of them. Specifically, there is no evidence of the Respondent's use, or demonstrable preparations to use 82 of the 83 domain names in issue. As to the only domain name in issue in use, namely <dellwww.com>, it purports to be a "strained acronym" for "Diabetes Education Long Life". There is no rational connection between the DELL trademark and a site devoted to diabetes education. This is the more so when other domain names that contain the word "diabetes" are available for registration [see, paragraph 5.1.6 above]. Further, neither Mr. McShand nor MTO C.A. are commonly known as DELL. Put shortly, the domain names in issue are not being used in connection with a *bona fide* offering of goods or services. They were registered by the Respondent long after DELL had become a famous trademark of the Complainant and with full knowledge of the Complainant's superior and prior rights in the DELL trademark.

5.1.15 *Registered and Used in Bad Faith*

Here, the Complainant points, as evidence of bad faith, to transfer of 80 of the domain names from MTO C.A. to the Respondent shortly after [April 18, 2002] first being contacted by the Complainant's attorneys [the *cease and desist* letter dated February 12, 2002] - see, paragraphs 4.5.3 and 5.1.3 above respectively]. The Complainant asserts that Mr. McShand took this step to transfer the domain names away from the United State to Venezuela being

"... apparently insecure in his stated beliefs that he had an absolute right to own the domains"

5.1.16 The Complainant points as further evidence of bad faith to the April 2002 Press Release by Mr. McShand [see, paragraph 5.1.9 above] in which he;

- identifies himself as the owner of the disputed domain names, making no mention of MTO C.A.; and
- tried to muddy the Complainant's name in connection with this dispute.

5.1.17 As other bad faith evidence, the Complainant states that the address provided by MTO C.A. was incomplete and the telephone number provided in Wisconsin is not a working telephone number, which it characterizes as "willful omissions ... to keep from being located by legitimate trademark owners."

5.1.18 Finally, the Respondent's attempt to hide behind a worthy cause so as to be paid by the Complainant for the domain names in issue is nothing less than extortion, the Respondent clearly banking on the Complainant not wanting to risk adverse publicity.

April 18, 2002: the Respondent sent an email to the Complainant in, inter alia, the following terms:

"Your company Dell Computer Corporation must stop harassing our business. Your actions are going to oblige us to take further actions. We will communicate this issue to all news and editors around the globe."

5.2 The Respondents Case

5.2.1 Identical or Confusingly Similar

As foreshadowed in Mr. McShand's email dated February 20, 2002 [paragraph 5.1.3 above], the crux of the Respondents' case is as follows:

- The word "Dell" is a generic word meaning "a small, secluded, wooded valley". As such it is available for any one to use provided that such use does not conflict with prior use by a business for the same goods and services.
- There are many other registered trademarks in the United State and in other countries also for the word DELL and for marks including the word DELL which do not belong to the Complainant.
- Because the Complainant and the Respondents are engaged in very different activities, use by the Respondents of the domain names in issue for its diabetes education project cannot give rise to any misrepresentation or confusion in relation to the Complainant's goods or activities.

5.2.2 The Response then lists the following US and EC Community registered trademarks and trademark applications for DELL and for marks in which DELL is a component, none of which belong to the Complainant. [Where the Class(es) and registration dates are not shown in the table, it is because such information is not provided in the Response.]

| Country | Registration No. | Mark and Class(es) | Proprietor | Registration Date |
|---------------|-------------------|-------------------------------------|--|-------------------|
| United States | 681,510 | DELL ... | Random House Inc | July 7, 1959 |
| United States | 532,275 | DELL CROSSWORD PUZZLES 16 | Dell Publishing Company Inc | October 24, 1947 |
| United States | 676,728 | DELL CROSSWORD ANNUAL 31 | Dell Publishing Company Inc | April 7, 1959 |
| United States | 779,077 | DELL PURSE BOOK ... | Dell Publishing Company Inc | October 27, 1964 |
| United States | 792,637 | THE FARMER IN THE DELL ... | Farmer in the Dell [of Neenah, Wisconsin] | July 13, 1965 |
| United States | App. No. 76376273 | FARM IN THE DELL 43 | Farm in the Dell International Inc [of Mountain] | ... |
| United States | 1,111,026 | Mr DELL 29 | Mr Dell Foods Inc | January 9, 19?? |
| United States | 1,224,455 | SUNNY DELL 32 | Southland Corporation | January 18, 1982 |
| United States | 2,357,754 | DELL LAND ... | Jacob Joseph Dell | ... |
| United | App. No. | DELL LAND | Jacob Joseph | ... |

| | No. | Class(es) | | Date |
|---------------|----------------------|--|---|-------------------|
| States | 78107555 | 41 | Dell [of Seguin Texas] | |
| United States | App.No. 76283960 | SUSAN DELL 25 | Susan Dell Inc [of Austin, Texas] | ... |
| United States | App. No. 76284277 | SUSAN DELL 25 | Susan Dell Inc | ... |
| United States | 1,762,728 | VAN DELL 14 | Park Lane Associates Inc | April 6, 1993 |
| United States | 1,818,586 | ALP AND DELL 42 | Roth Kase USA Ltd | January 25, 1994 |
| United States | 1,773,774 | ALP and DELL 29 | Roth Kase USA Ltd | May 25, 1993 |
| United States | 1,827,104 | DELL's SECRET GARDEN 1 | Dell's Secret Garden Inc [of Albany, Georgia] | March 23, 1994 |
| United States | 1,862,895 | DELL RHEA's CHICKEN BASKET 42 | Dellco Inc [of Illinois] | November 15, 1994 |
| United States | 2,482,604 | DELL- COMM 9 | Dell-Comm Inc [of Minnesota] | August 28, 2001 |
| United States | App. No. 75186301 | DELL COMM 37 & 42 | Dell- Comm Inc | ... |
| United States | 2,089,203 | BLUE DELL 29 | Northwest Packing Co [of Vancouver] | August 19, 1997 |
| United States | 2,288,289 | ROCCA DELL'ULIVE TO ... | ... | ... |
| United States | 2,158,291 | SIGILLO DELL'ARTE ... | ... | ... |
| United States | 2,206,921 | MOUNTAIN DELL ... | Mountain Craft Inc | ... |
| United States | 2,457,353 | THE DELL ... | Dell Enterprises Inc [of Nebraska] | ... |
| United States | 2,461,824 | DUNDEE DELL ... | Dell Enterprises Inc | ... |
| United States | App. No. 76234415 | FARMER IN THE DELL 28 | Hasbro Inc | ... |
| United States | App. No. 76240735 | THE DELL GROUP 35 | The Skill Bureau Inc [of Boston] | ... |
| United States | 1,932,995 | GUERNSEY DELL 11 | Guernsey Dell Inc [of Chicago] | November 7, 1995 |
| United States | 2,017,988 | DELLWOOD ... | Dellwood Financial | November 19, 1996 |

| | No. | Class(es) | | Date |
|---------------|------------------|------------------------------|-----------------------------------|--------------------|
| | | | Services Company [of Minneapolis] | |
| United States | 2,079,798 | THE O'DELL GROUP ... | O'Dell | July 15, 1997 |
| United States | App.No. 76374207 | DELL'ARTE CHOCOLATE CAFÉ ... | Arthur Newman | ... |
| United States | 2,474,604 | DELLS RIVER DISTRICT ... | City of Wisconsin Dells | ... |
| United States | 2,503,474 | DELLS RIVER DISTRICT ... | City of Wisconsin Dells | ... |
| United States | 1,929,736 | DELLS BOAT TRIP ... | Dells Boat Co Inc | ... |
| EC Community | 166,058 | DELL 16 | Random House Inc | April 1, 1996 |
| EC Community | 1,411,801 | DELL 16 | Random House Inc | September 19, 1997 |
| EC Community | 1,475,929 | DELL d. 30 | Kerry Group plc | ... |
| EC Community | 1,390,157 | DELL'OLMO 24 | Ratti S.p.A. | ... |
| EC Community | 1,552,477 | 'DELLS 29 | Largo Food Exports Ltd | August 4, 1995 |
| EC Community | 2,045,500 | DELL UGO 29 & 30 | Dellugo Ltd | September 20, 1994 |
| EC Community | 1,163,781 | DELLORTO 12 | Dell'Orto S.p.A. | ... |
| EC Community | 1,163,780 | DELLORTO 7 | Dell'Orto S.p.A | ... |

5.2.3 The Response also lists companies which have the name / mark DELL or include it as a component in their business names.

| Corporation / Business | Activities | Date of First Use |
|---|---|-------------------|
| Dell Corporation [of Rockville, MD] | Speciality contracting firm | 1972 |
| O'Dell Engineering Inc [of Modesto, CA] | Land Development Projects | 1983 |
| Dell Services Inc [of Michigan] | Service Centre for home electronics and computers | pre 1977 |
| Dell Quay Sailing Club | Sailing Club | ... |

5.2.4 The Response lists domain names that use or incorporate the mark DELL.

| Domain Name | Registrant | Business [where stated] |
|----------------|-------------------------------------|-----------------------------|
| <dellcorp.com> | Dell Corporation [of Rockville, MD] | Speciality Contracting firm |

| | | |
|-------------------------|---|---|
| <dellspace.com> | Rackspace Ltd [of San Antonio, Texas] | |
| <delltech.com> | Dell Tech Laboratories Ltd [of Ontario, Canada] | |
| <delllab.com> | Michael Richardson [of Chesapeake, VA] | |
| <dellsex.com> | Unused Domain [of New Orleans] | |
| <dellfamily.com> | Nick Dell [of Los Angeles] | |
| <mzdells.com> | Mr. Dell Foods Inc | Processed potatoes |
| <dellpharmacy.com> | Dell Pharmacy [of Ontario, Canada] | |
| <odellengineering.com> | O'Dell Engineering Inc | Land development projects |
| <highlanddell.com> | Dell Schaefer P.A. [of Hollywood, FL] | Attorneys |
| <dellscentral.com> | Wisconsin Dells Central | |
| <dellman.com> | Larry Mile [of Wisconsin] | |
| <dellservice.com> | Dell Service Inc | Service center for home electronics and computers |
| <dellsbank.com> | Bank of Wisconsin Dells | |
| <dellstar.com> | Dell Star Technologies Inc [of Tulsa] | Video and surveillance systems |
| <wisconsindells.com> | Family Fun in the Wisconsin Dells | |
| <dellboy.com> | Jason Conway [of Middlesex, United Kingdom] | |
| <dellsleatherworks.com> | Dells Leather Works | |
| <dellink.com> | Mun Young Gu [of Seoul, Korea] | |
| <riodell.com> | City of Rio Dell, California | |
| <thendell.com> | Dells on Anderson Island Vacation Rental | |
| <seversondells.org> | Severson Dells | Non profit Nature Reserve & Environmental Education & Research Facility |
| <dellscoupons.com> | Wisconsin Dells | |
| <dellalpe.com> | Dell Alpe | Italian Foods |
| <dellschamber.com> | Wisconsin Dells Chamber of Commerce | |
| <jeuniferodell.org> | Jennifer O'Dell | Actress |
| <design-dell.com> | Dell Point Technologies Inc | Manufacturers of gas and fire wood pellet stoves |
| <delliran.com> | Delliran Company [of Tehran] | |

| | | |
|-----------------------------|---|--------------------------------------|
| <dellmedia.com> | DigitaLive.com [of Los Angeles] | |
| <dellonline.com> | Andrew Dell [of Westminster, CA] | |
| <wisdells.com> | Wisconsin Dell Visitors & Convention Bureau | |
| <dellarteoperaensemble.org> | Dell'Arte Opera Ensemble | |
| <wdell.com> | Walton Dell's Website | |
| <dellbrothers.com> | Dell Brothers | Formal Clothing |
| <westfallodell.com> | Westfall O'Dell Motors | |
| <dellgames.com> | Talkshop Ltd [of Dublin, Ireland] | |
| <delldigital.com> | Superfly Inc [of Stockton, CA] | |
| <dellphoto.com> | Dell Photography Incorporation [of Atlanta, GA] | |
| <dellsonline.com> | Wisconsin Dells Hotel | |
| <delltrack.com> | Eric Simpson [of Walnut Creek, CA] | |
| <dells-inn.com> | Rodeway Inn | |
| <dellus.com> | Laurent Dellus [of Illinois] | |
| <dellme.com> | Mercabe Continental SA de CV [of Monterrey, Mexico] | |
| <dellcustomerservice.com> | Interwise Inc, doing business as Itsyourdomain.com | |
| <dellbank.com> | DigitaLive.com [of Los Angeles] | |
| <dellengineering.com> | Dell Engineering P.A. [of Bayville, NJ] | |
| <dellglonbal.com> | S Hadi [of Los Angeles] | |
| <dellhome.com> | Internet Hosting [of Montreal, Canada] | |
| <dellbusiness.com> | Internet Hosting [of Montreal, Canada] | |
| <dellenglish.com> | Dell International English [of Beijing, PRC] | International Information Technology |
| <dellnetwork.com> | Jong-Hyun Lee [of Korea] | |
| <dellwireless.com> | Centrade Corp | |
| <dellcom.com> | Shin-Webxist Hyun [of Korea] | |
| <dellcompany.com> | Boukhaili Hamdaoui [of Paris, France] | |
| <delldisk.com> | Kyu Lee | |
| <doctordell.com> | BulkRegister.com | |
| <dell1.com> | Raphael Afilalo [of St. Laurent, Canada] | |

| | | |
|----------------|--------------------------------------|--|
| <eurodell.com> | Meta Domains.com [of Birmingham, AL] | |
|----------------|--------------------------------------|--|

5.2.5 The Response cites the following uses of the generic word "Dell":

- Several companies in the United Kingdom.
- Several companies in Switzerland.
- 12 registered trademarks in Austria.

WIPO's Madrid Express database contains "30 records with the generic word DELL".

Various businesses and individuals in addition to those listed in paragraphs 5.2.2 to 5.2.4 above, including:

Dell Tech Laboratories Ltd:
Dell Road Gospel Church:
Dell'Osso Farms:
Various departments of Rio Dell City:
Law Office of Susan Dell:
Casa Dell Angolo:
<Salon dell area.com>;
<widells.com>;
<dellarte.com>;
<dellwilliams.com>;
>olivedellranch.com>;
Bruce Dell Law Firm:
Compagnia Dell Olio, United States of America:
Dell & Schaefer [Attorneys];
<dellhouse.co.uk>;
John Odell Emergency Operation Centers; and
Judith Chaffee's Commedia Page [<commedia-dell-arte.com>]

5.2.6 The Response asserts that the above examples comprise only a sample of the very many uses of the word DELL by individuals, companies and organizations other than the Complainant. For example,

- there are many more companies and individuals using the word DELL as their trademark or service mark in other countries;
- in the United States alone there are over 100 attorneys with the surname DELL;
- DEL [Spanish] and DELL [Italian] mean "from". So, in Italy there are very many businesses whose names incorporate DELL. In Spanish, using the prefix DEL with a word beginning with the letter L will produce a phonetic "dell"; for example Del Lago [from the lake].

5.2.7 In the light of the forgoing, the Respondent's case is that the Complainant cannot assert its DELL trademarks - which are registered in relation to computer goods and services - to prevent use of the word / mark DELL in respect of quite disparate activities such as diabetes education or diabetes supplies. It follows, the Respondent says, that the domain names in issue cannot be confusingly similar to the Complainant's DELL trademark.

5.2.8 *Rights or Legitimate Interests*

Here the Respondent's case is as follows. First, before being put on notice of this dispute [by the cease & desist letter dated February 12, 2002 - see, paragraph 5.1.3 above] the Respondent had been using the DELL acronym for its diabetes education etc activities [i.e. February 1999 - see, paragraph 4.5.2 above]. This use was *bona fide* since it bore no relation to the Complainant's use of the DELL mark for its wholly disparate business and because, as demonstrated in paragraphs 5.2.1 to 5.2.7 above, DELL is generally used in business by very many other individuals and companies and DELL and/or marks incorporating DELL are registered by proprietors other than the Complainants for different goods and services.

- 5.2.9 Even though the Respondent has no registered trademark rights in DELL, it is known by the domain name <dell.www.com> [see, paragraphs 5.1.3 and 5.1.4 above]. The Response states:

"The Respondent's Business Operations, Communications, Customer Support, Customer Services, Sales, Purchasing, Accounting etc are done mainly by use of the Internet. The Respondent's Business rely on the Internet. The Respondent created the business with the purpose to run it exclusively from the Internet."

5.2.10 *Registered and Used in bad Faith*

The Respondent's case is as follows. The other domain names in issue, which are not as yet used, were registered so as to secure all the domains needed for the Respondent's *business plan and strategies*. The Respondent describes its strategy as being to build:

"... several web pages and interconnect them with hyperlinks. Also to point all the remaining domain's URL to the main URL that is <http://www.dellwww.com>. By this way the search engines will direct our customers to our main page or to any other direction decided by our Strategy Department."

The Respondent describes its Business Plan as being:

"... to secure all countries, cities and states or words needed for their global expansion."

The Response explains that it is necessary to have the TLD *.com* for each country, so that residents of each country can readily reach the main website. For example, a person in France searching for the Respondent website need only type DELLFRANCE and with a *.com* suffix the search engine will direct that person to that main website.

- 5.2.11 This, the Response says, is precisely how the Complainant uses its domain names. For example, <dellcomputers.com>; <delldirect.com>; <dellbrowser.com>; <dellfactory.com>; <dellplus.com>; <dellwebpc.com>; <dell4me.com>; <dellexchange.com>; <dellpoweredge.com>; <dellprecision.com>; <delldimension.com> and <dellselectcare.com> [see,

<dell.com>.

5.2.12 Further, the fact that prior to notice of this dispute [in February 2002] the Respondent's domain names in issue - other than <dellwww.com> - were neither active nor linked to <dellwww.com> is not an indication of bad faith registration and use. The Complainant too has domain names, for example <delllaptop.com>; <dellnews.com>; <dellhelp.com>; <dell dvd.com>; <delltips.com>; <dellhostings.com>; <delltv.com>; <dellorders.com>; <dellfinance.com>; and <dellparts.com> which are neither active nor linked to another of the Complainant's websites.

5.2.13 The Respondent did not register or acquire the domain names in issue primarily for the purpose of selling them to the Complainant for consideration in excess of its costs directly related to those domain names. Mr. McShand made it clear in his telephone conversations on February 19, 2002 [see, paragraph 5.1.3 above] that the domain names were not for sale. Mr. McShand goes on to say in the Response that, in reply to questions from Ms Brockmeyer / Mr. Dreitler asking if he was willing to sell or accept an offer for those domains, he stated

"If you want to make us an offer, that is up to you. I already told you that our business has no intention of selling its trademarks or domains. Do whatever you wish. Any communication will be discussed by our directors."

5.2.14 The Response concludes in the following terms:

"The Respondent registered the domains and is using them in the best faith, best values and best belief. The Respondent's mission is not only to make a profit. The Respondent's mission is to give the best service, the best product, and the best education in diabetes. And as a consequence of all this, there is a profit left. A profit that will be used to serve even better the Respondent's customers or anyone in the need."

5.3 *Other cases under the Policy involving the Complainant's DELL trademark*

5.3.1 These are not cited in the Complaint or the Response. In WIPO Case No. D2001-0285, Parmi Phull of Valencia, Spain had registered <dellonline.net> and <dellonline.org>. No Response was filed. From the Decision it seems clear that the Respondent had engaged in a pattern of conduct of registering domain names incorporating the famous trade marks of third parties. The Complaint was upheld [Decision dated April 11, 2001].

5.3.2 In WIPO Case No. D2001-0361 Logo Excellence of Houston, Texas [the *alter ego* of Mr. Bryron Hoffmann] had registered 10 domain names incorporating the DELL mark. For example, <dellpower.com> and <dellconnect.com>. That Complaint was also upheld [Decision dated May 7, 2001].

5.3.3 WIPO Case No. D2000-0659 involved 9 domain names incorporating the DELL mark registered by Got Domain Names for Sale. These included <dellpalm.com>, .net and .org; <dellwireless.net> etc. As in WIPO Case No. D2001-0285, the Respondent here had registered numerous other domain names incorporating the trademarks of various entities, such as CNN, Bell

August 15, 2000].

- 5.3.4 The most notorious of these cases, WIPO Case No. D2000-1087, was decided on November 17, 2000. It concerned 122 DELL domain names including <dellcomputersystem.com>; <dellinsurance.com>; <dell-mobile.com>; <dellservices.com> etc registered by Alex and Birgitta Ewaldsson of Sweden. No Response was filed. Again the Respondents were found to have registered numerous other domain names incorporating the trademarks of other parties, including the Swedish Company, TELIA and others including PHILIPS: SIEMENS: IKEA: BENTLEY and JAGUAR. The Complaint was upheld.
- 5.3.5 The Panel has cited these cases under the Policy, since all of the domain names in issue in this administrative proceeding were registered subsequent to the Decisions in those cases. The registration by AZTEC was on December 29, 2001, the registrations by MTO CA were variously made on December 3, 5, 6, 7, 12, 14, 16 and 31, 2001 and on February 20, 2002, and the registrations by Diabetes Education Long Life - DELL - on April 20 and May 1, 2002. It is to be noted that the Respondent's only active website <dellwww.com> was registered by MTO CA on December 14, 2001, the Respondent Diabetes Education Long Life - DELL having been formed in February 1999.

6. Discussion and Findings

- 6.1 The Policy paragraph 4(a) provides that the Complainant must prove each of the following:
- (i) that the Respondent's domain name is identical or confusingly similar to a trademark or service mark in which the Complainant has rights; and
 - (ii) the Respondent has no rights or legitimate interests in respect of the domain name; and
 - (iii) the domain name has been registered and is being used in bad faith.
- 6.2 Paragraph 4(c) of the Policy identifies circumstances which, in particular, but without limitation, if found by the Panel to be proved based on its evaluation of all the evidence presented, shall demonstrate the Respondent's rights or legitimate interests for the purpose of paragraph 4(a)(ii) of the Policy.
- 6.3 Paragraph 4(b) of the Policy sets out circumstances which, if found by the Panel to be present, shall be evidence of the registration and use of a domain name in bad faith.

6.4 Identical or Confusingly Similar

- 6.4.1 The Panel finds the domain name <dellwww.com> to all intents and purposes identical to the Complainant's DELL trademark.
- 6.4.2 The remaining 82 domain names fall into two categories. The majority comprises the prefix DELL with the suffix being the name of a country (for example, <dellbrazil.com>), the name of a geographical area [for example,

[for example, <dellmex.com> and <dellcaribe.com>]. These total 74 domain names. To them should be added 2 further domain names where the country abbreviation precedes the DELL mark, namely <usadell.com> and <usdell.com>. They are what will be termed DELL country / geographical domain names in issue and total 76 domain names in all.

- 6.4.3 There are then 6 domain names where the DELL mark is used with a generic word or words. These are <dellaboutus.com>; <dellcontact.com>; <dellcustomer.com>; <delloffers.com>; <dellinvestors.com> and <bancondell.com>. They will be termed the DELL generic domain names.
- 6.4.4 As to the 76 DELL country / geographical domain names in issue, the Panel considers that the *America Online, Inc. v. Asia On-Line This Domain for Sale*, NAF Case No. FA0004000094636 and the *Bloomberg L.P. v. Sein M.D.*, NAF Case No. FA0101000096487 cases [see, paragraph 5.1.13 above] were correctly decided.
- 6.4.5 As to the 6 DELL generic domain names in issue, the Panel also regards them as confusingly similar to the DELL trademark and family of trademarks. The Panel refers in this respect not only to the cases under the Policy cited by the Complainant [see, paragraph 5.1.12 above] but also to the Decisions under the Policy involving the Complainant's DELL trademarks [see, paragraph 5.3 above].
- 6.5 Rights or Legitimate Interests**
- 6.5.1 The nub of the Respondent's case, boiled down to its essentials, is that the Complainant's DELL trademark and family of trademarks are relevant only to its computer goods and services. It is abundantly clear that there are DELL registered trademarks for other goods and services, that many individuals and companies do business under the DELL name or a name incorporating DELL, so why in relation to a diabetes education website should the Respondent not be free to use the acronym DELL [Diabetes Education Long Life] for its DELL country / geographic domain names? The rationale for registering those domain names is explained in paragraph 5.2.10 above.
- 6.5.2. The Policy is, however, concerned with whether on the facts of a particular dispute the Respondent can demonstrate rights to or legitimate interests in the domain name in issue. In this case, the DELL trademark is well known internationally in the context of the Complainant and its products. Searches of national trademark databases, such as the TESS US Patent and Trademark Office database referred to in the Response, will reveal the extent of the Complainant's registered rights in the DELL trademark and family of trademarks. In addition, cases decided under the Policy - such as the earlier DELL cases noted in paragraph 5.3 above - are readily accessible from the Center's website and were so accessible in December 2001 when the earliest of the domain names in issue were registered. There is, therefore, no question of the Respondent being *taken by surprise* in relation to the existence of the Complainant and its DELL trademarks and the way in which those trademarks have been used in earlier cases under the Policy.
- 6.5.3 The Respondent Diabetes Education Long Life - DELL was formed in February 1999 [see, paragraph 4.5.2 above]. Its business is "done mainly by

<dellwww.com> [see, paragraph 5.1.5 above] and that domain name was not registered until December 14, 2001 [see, paragraph 5.3.5 above]. So the actual use made of that domain name in issue pre dates by less than 2 months the Complainant's *cease and desist* letter of February 12, 2002 [see, paragraphs 5.1.2 and 5.1.3 above]. As to the Respondent's preparations to use that domain name and the other 82 domain names in issue the Response is silent, except to explain its strategy to direct them to the main website at <dellwww.com> [see, paragraph 5.2.10 above].

6.5.4 The question is whether such use or intended use can be said to be in connection with a *bona fide* offering of goods or services. In that connection, there is - as the Complaint says - no rational connection between the DELL trademark and a site devoted to diabetes education. The natural domain name for such a site would be to include the word "diabetes", not a strained acronym. The Panel is persuaded by the Complainant's case in this respect and by the Decision of the US Court of Appeals for the Fourth Circuit under the ACPA [see, paragraph 5.1.6 above].

6.5.5 Further, the Respondent's description of its existing business and future business is not, in the Panel's view, convincing. The Response refers to the Respondent's "Business Operations, Communications, Customer Support, Customer Services, Sales, Purchasing, Account etc" but no examples of any of these activities are given [see, paragraph 5.2.9 above]. If the Respondent is, as the Response claims, using the domain names in issue

"... in the best faith, best values and best belief"

it is strange that no concrete examples of such use are provided.

6.5.6 In short, the Panel concludes that - on the evidence before it - the Respondent has not demonstrated circumstances within paragraph 4(c)(i) of the Policy. As to paragraph 4(c)(ii), there is no evidence either that the Respondent business has been commonly known by any of the domain names in issue. Of the 83 domain names, only one has been used in relation to an active website and then only since mid December 2001 at the earliest [see, paragraph 6.5.3 above].

6.5.7 The Panel does not read the Response as advancing a case under paragraph 4(c)(iii) of the Policy but, in any event, the evidence does not - in the Panel's view - support such a case.

6.5.8 As to the 6 DELL generic domain names [see, paragraph 6.4.3 above] none have, in the Panel's view, the remotest connection with the stated aims of Mr. McShand, with the possible exception of <dellabout.us>. The others are suited to a commercial enterprise - for example, <dellinvestors.com> - not a website dedicated to the education and help of diabetes sufferers and their carers. As to <dellaboutus.com>, in the context of the domain names as a whole and in the light of the Respondent's strategy [see, paragraph 5.2.10 above] the Panel concludes that the Respondent cannot demonstrate rights or legitimate interests in that domain name or in the other 82 domain names in issue. The Complaint, therefore, succeeds in satisfying paragraph 4(a)(ii) of the Policy.

- 6.6.1 Having been put on notice of the Complainant's rights [the cease and desist letter of February 12, 2002 - paragraph 5.1.3 above], the Respondent continued to register more DELL country / geographical names subsequently. On February 20, 2002 some 13 such domain names [including, for example, <dellportugal.com> etc] were registered, followed by 2 in April 2002 and 1 in May 2002 [see, paragraph 5.1.2 above].
- 6.6.2 Did the Respondent register the domain names in issue [between December 2001 and May 2002] primarily for the purpose of selling them to the Complainant for valuable consideration in excess of the costs directly related to those names? The Respondent denies that he did and that the domain names are for sale. However, the Respondent is prepared to consider an offer from the Complainant to purchase those domain names [see, paragraph 5.2.13], which is hardly consistent with the philanthropic aims of the Respondent to educate and support diabetes sufferers. Further, the Respondent could not have been unaware of the Complainant and its well known DELL trademark. Trademark searches would quickly have given the Respondent an idea of the extent of the Complainant's DELL and DELL family trademark registrations. A WHOIS search would, similarly, have revealed the extent of the Complainant's DELL domain name registrations. Further, in the context of the Respondent's warranties and representations in its Registration Agreements with the Registrar, it would have been prudent to check the Center's website and that of the National Arbitration Federation [NAF] for any existing cases under the Policy relating to the Complainant's DELL trademark. Finally, there is the Respondent's conduct after being put on notice of the Complainant's case in February 2002 [see, paragraph 6.6.1 above].
- 6.6.3 Although there is no evidence of any pattern of conduct by the Respondent of registering as domain names trademarks of either parties, in the Panel's view the weight of evidence points to conduct falling within paragraph 4(b)(i) of the Policy. But, even if that is incorrect, the Panel is not bound by the circumstances set out in paragraph 4(b) of the Policy [see, paragraph 6.3 above] and is entitled to look at all the circumstances presented in the Complaint and the Response. While the aims of Mr. McShand and his wife to assist diabetes sufferers and their carers are acknowledged, the acronym DELL is just too strained to be believable and it is just not credible that using the corporate and brand name of the world's largest direct seller of computer systems is appropriate to bring such sufferers to a diabetes help site.
- 6.6.4 In all the circumstances, the Panel finds that the Complainant has made out its case under paragraph 4(a)(iii) of the Policy.

7. Decision

For all the foregoing reasons, the Panel decides that the 83 domain names in issue [listed in paragraph 2 above] are identical or confusingly similar to the Complainant's DELL trademark and family of trademarks, that the Respondent has no rights or legitimate interests in respect of those domain names and that they have been registered and are being used by the Respondent in bad faith. Accordingly, the Panel directs that registration of the 83 domain names in issue be transferred to the Complainant.

David Perkins
Sole Panelist

Dated: July 5, 2002