



5-1999

Computer Law Institute

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

Charles R. Keeton

Brown, Todd & Heyburn PLLC

Jay E. Ingle

Jackson & Kelly

J. Mark Grundy

Greenebaum Doll & McDonald PLLC


Robert F. Duncan

Jackson & Kelly

See next page for additional authors

[Click here to let us know how access to this document benefits you.](#)

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

 Part of the [Commercial Law Commons](#), [Insurance 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; Keeton, Charles R.; Ingle, Jay E.; Grundy, J. Mark; Duncan, Robert F.; Tuggle, Kenneth J.; Beres, Joel T.; Webb, Bill E.; Davidson, Stephen J.; Stewart, Cynthia L.; Wilson, Judge B. II; Beyer, David J.; Metzmeier, Kurt X.; and Esposito, Shaun E., "Computer Law Institute" (1999). *Continuing Legal Education Materials*. 25.

https://uknowledge.uky.edu/uky_cle/25

Authors

Office of Continuing Legal Education at the University of Kentucky College of Law, Charles R. Keeton, Jay E. Ingle, J. Mark Grundy, Robert F. Duncan, Kenneth J. Tuggle, Joel T. Beres, Bill E. Webb, Stephen J. Davidson, Cynthia L. Stewart, Judge B. Wilson II, David J. Beyer, Kurt X. Metzmeier, and Shaun E. Esposito

**UK
CLE**

**COMPUTER
LAW
INSTITUTE**

May 1999

**UK
CLE**

**COMPUTER
LAW
INSTITUTE**

May 1999

**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 1999 by the University of Kentucky College of Law,
Office of Continuing Legal Education.
All rights reserved.

Printed in the United States of America

**UNIVERSITY OF KENTUCKY
COLLEGE OF LAW**

OFFICE OF CONTINUING LEGAL EDUCATION

Suite 260 Law Building
Lexington, Kentucky 40506-0048
(606) 257-2921 or
(606) 257-CLE1
Facsimile
(606) 323-9790

PRESIDENT, UNIVERSITY OF KENTUCKY: Charles T. Wethington, Jr.

ACTING DEAN, COLLEGE OF LAW: Robert G. Schwemm

ASSOCIATE DEAN AND DIRECTOR OF CLE: Todd B. Eberle

ASSISTANT DIRECTOR Kevin P. Bucknam

ADMINISTRATIVE/BUSINESS MANAGER: Susan C. Saunier

STUDENT ASSOCIATE Melinda E. Rawlings



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, and the Midwest.

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 Forms 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. Forms 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 Forms 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 budgeting, accounting, and financial reporting. As an "income based" program, UK/CLE's course tuitions and publications sales are budgeted to generate sufficient revenues for self support.

Commitment to Quality and Creativity

UK/CLE is a member of the Association for Continuing Legal Education (ACLE). 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 and services provided by ACLE. 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 judges, law professors, and practitioners who generously donate their time and talent to continuing legal education. Their knowledge and experience are 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.

COMPUTER LAW INSTITUTE

TABLE OF CONTENTS

UNIFORM COMPUTER INFORMATION TRANSACTIONS ACT (Formerly Proposed Uniform Commercial Code Article 2B)	SECTION A
<i>Charles R. Keeton</i>	
UPDATE ON LEGISLATION CONCERNING THE YEAR 2000.....	SECTION B
<i>Jay E. Ingle</i>	
YEAR 2000: ASSESSMENT, READINESS & REMEDIATION.....	SECTION C
<i>J. Mark Grundy</i>	
LITIGATION AND INSURANCE ISSUES IN PREPARATION FOR YEAR 2000	SECTION D
<i>Robert F. Duncan</i>	
YEAR 2000: DIRECTOR AND OFFICER LIABILITY AND THE BUSINESS JUDGMENT RULE.....	SECTION E
<i>Kenneth J. Tuggle</i>	
DOMAIN NAMES, TRADEMARKS & COPYRIGHT ISSUES IN CYBERSPACE	SECTION F
<i>Joel T. Beres</i>	
TAX ISSUES ARISING OUT OF E-COMMERCE AND OTHER RELATED ISSUES	SECTION G
<i>Bill E. Webb</i>	
RECENT DEVELOPMENTS AND EMERGING ISSUES IN ON-LINE SALES AND LICENSING.....	SECTION H
<i>Stephen J. Davidson</i>	

**NEGOTIATION OF SOFTWARE LICENSE AGREEMENTS
AND RELATED AGREEMENTSSECTION I**
Cynthia L. Stewart

JURISDICTIONAL ISSUES ARISING OUT OF E-COMMERCESECTION J
Kenneth J. Tuggle

**INTERNET / E-MAIL PRIVACY ISSUES; ENCRYPTION AND
ELECTRONIC ESPIONAGE SECTION K**

Civil Law Perspective
Judge B. Wilson II

Criminal Law Perspective
David J. Beyer

**ETHICAL AND PROFESSIONAL RESPONSIBILITY CONCERNS
ARISING FROM THE USE OF TECHNOLOGY IN THE PRACTICE
OF LAWSECTION L**
Kurt X. Metzmeier
Shaun E. Esposito

UK/CLE Is Self-Supporting

The University of Kentucky Office of Continuing Legal Education (UK/CLE) is a financially self-supporting office of the University of Kentucky College of Law. As such, UK/CLE is income-based and separately budgeted. It operates in a manner similar to not-for-profit organizations, paying all direct expenses, salaries and overhead solely from revenues. No tax dollars or public funds are used in its operations. Revenues for UK/CLE are obtained from registrant enrollment fees, and monies received from the sale of our publications. UK/CLE's sole function is to provide professional development services. Thus, in the event surplus funds become available, they are retained in our budget to improve the quality and variety of services we provide. Compliments, and criticisms concerning our programs, publications, and other services are welcomed.

UNIFORM COMPUTER INFORMATION TRANSACTIONS ACT

Formerly Proposed Uniform Commercial Code Article 2B

Charles R. Keeton
Brown, Todd & Heyburn PLLC
Louisville, Kentucky

Copyright 1999, Charles R. Keeton. All Rights Reserved.

SECTION A

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100

UNIFORM COMPUTER INFORMATION TRANSACTIONS ACT

Formerly Proposed Uniform Commercial Code Article 2B

TABLE OF CONTENTS

I. BACKGROUND A-1

II. SCOPE OF UCITA A-2

III. ELECTRONIC CONTRACTING A-2

IV. WARRANTIES IN COMPUTER INFORMATION TRANSACTIONS A-4

EXHIBIT A: PRESS RELEASE REGARDING UCITA AS FREE-STANDING ACT ... A-7

EXHIBIT B: MARCH 1, 1999 DRAFT OF UCITA (*Cited Sections Only*) A-11

COMPUTER LAW INSTITUTE

May 7, 1999

University of Kentucky College of Law, Lexington, Kentucky

UNIFORM COMPUTER INFORMATION TRANSACTIONS ACT FORMERLY PROPOSED UNIFORM COMMERCIAL CODE ARTICLE 2B

BY CHARLES R. KEETON*

- I. *Background* -- What is the Uniform Commercial Information Transactions Act (formerly Article 2B)?
 - A. The Uniform Computer Information Transactions Act ("UCITA") began its life as part of the Article 2 revision process.
 - B. The Article 2 revision project then split computer information off into a "spoke" on a proposed "hub and spoke" model.
 - C. The National Conference for Commissioners on Uniform State Laws ("NCCUSL") then jettisoned the "hub and spoke" approach and created a completely separate Article for computer information, Article 2B.
 - D. NCCUSL and the American Law Institute (the "ALI") just recently (April 7, 1999) announced that what had been considered for introduction as Article 2B of the Uniform Commercial Code would not be a part of the UCC, but rather would be split out as a free standing Uniform Computer Information Transactions Act. (A copy of the press release is attached).
 - E. According to NCCUSL, the purpose of UCITA is to respond to the immense numbers of transactions in information and their dollar value, and the fact that the Internet and information technology and commerce are major components of the future economic prosperity of the United States. NCCUSL has seen what it describes as a dramatic need for coherent and predictable legal rules to support the contracts that underlie that information and Internet economy, and that lack of uniformity and lack of clarity of these legal rules engender uncertainty, unpredictability and high transaction costs. It says that, while the codification of those rules to provide that uniformity and clarity is not possible in the Uniform Commercial Code, NCCUSL will propose uniform legislation (now known as the Uniform Computer and Information Transactions Act) to promote that uniformity and clarity. (See, again, the press release attached.)

* A.B. Summa Cum Laude Marshall University, 1971; J.D. with High Distinction University of Kentucky College of Law, 1975. Member, Brown, Todd & Heyburn PLLC, Louisville, Kentucky.

Copyright 1999 by Charles R. Keeton, reproduced in the UK/CLE Computer Law Institute with permission.

II. *Scope of UCITA.*

- A. What are "computer information transactions"?
 - 1. How does one distinguish "computer" from other "information"? See proposed Section 2B-103.
 - 2. What is a "computer information transaction"? See the definitions of "computer," "computer information," "computer information transaction," and "computer program" in proposed Section 2B-102(a)(7), (8), (9) and (10) respectively. See also the discussion of "support agreements" in proposed Section 2B-616.
 - 3. What is "information"? See the definitions of "information," "information processing system," "informational content" and "information rights," at proposed Section 2B-102(a)(26), (27), (28) and (29).
 - 4. UCITA would cover only licenses. See the definitions of "license," "licensee," "licensor," "mass-market license," and "mass-market transaction" at proposed Section 2B-102(a)(30), (31), (32), (33) and (34).
- B. Compare to the scope of proposed revised Article 2. See proposed Section 2-103.

III. *Electronic contracting.*

- A. Formation of contracts in cyberspace could require special rules in some special circumstances. For example, how are "electronic agents" to be dealt with? Is it like or unlike the traditional UCC "battle of the forms"?
 - 1. UCITA includes special rules regarding offer and acceptance for electronic agents. In general, UCITA authorizes formation of contracts by electronic agents. See proposed Section 2B-204(a).
 - 2. Special rules would exist for a contract formed between an electronic agent and a human being. To some extent, UCITA would make the outcome turn on the extent to which the human being can provide individualized responses when the electronic agent cannot. See proposed Section 2B-204(b).
- B. Many existing statutes require a "writing" of some sort. In general, UCITA would statutorily mandate that a record or authentication not be discriminated against solely because it is in electronic form. See proposed Section 2B-113. The section does not address evidentiary or proof issues, including questions about to whom the record or authentication can be attributed.

- C. One issue presented by contracts in cyberspace is the extent to which an electronic record has been properly authenticated and whether the authenticated record can be properly attributed to a particular person.
1. In general, UCITA does not prescribe an attribution procedure. Instead, it relies primarily on the parties to select an appropriate procedure. It does, though, provide guidelines for courts to determine the commercial reasonableness of an attribution procedure. See proposed Section 2B-114.
 2. UCITA also provides for recovery of damages for an injured party who reasonably relies upon a commercially unreasonable attribution procedure. See proposed Section 2B-115.
 3. UCITA also provides rules for determining the person to which an electronic authentication, message, record or performance is attributed. See Section 2B-116.
 4. UCITA also provides standards for proof of authentication. See proposed Section 2B-119.
 5. See also the definitions of "attribution procedure," "authenticate," and "automated transaction," at proposed Section 2B-102(a)(3), (4) and (5).
- D. Generally, a party adopts the terms of a record, including a standard form, if the party agrees to the record, by manifesting assent or otherwise. See Section 2B-207.
1. Generally, a person manifests assent if the person, acting with knowledge of, or after having an opportunity to review the record, authenticates the record or term or engages in conduct that the person has reason to know would allow the other party to infer assent to the record or term. In the case of an electronic agent, the electronic agent manifests assent if it authenticates the record or term after having an opportunity to review it. See Section 2B-111.
 2. A person has an opportunity to review a record or term only if the record or term is made available in a manner that ought to call it to the attention of a reasonable person and permit review. In the case of an electronic agent, opportunity to review occurs only if the record or term is made available in a manner that would enable a reasonably configured electronic agent to react to the record or term. See Section 2B-112(a) and (b).
 3. If the record or term is available for review only after a person becomes obligated to pay or begins its performance, opportunity to review requires the right of return. See Section 2B-112(c).

4. There are special rules for adopting terms in mass market licenses. See Section 2B-208.

IV. *Warranties in computer information transactions.*

A. Express warranties.

1. UCITA generally follows current Article 2 and requires that an affirmation of fact must become "part of the basis of the bargain" in order to create an express warranty. See proposed Section 2B-402.
2. Compare to proposed Section 2-403 of proposed revised Article 2, which continues a "basis of the bargain" test but effectively defines "basis of the bargain." See proposed Section 2-403.

B. UCITA provides an implied warranty of merchantability of a computer program. See proposed Section 2B-403. UCITA differentiates between implied warranties of merchantability to end users and to distributors. The implied warranty of merchantability does not generally apply to informational content. Compare to proposed Section 2-404 of proposed revised Article 2.

C. UCITA provides an implied warranty with respect to informational content. See proposed Section 2B-404. In general, no warranty arises with respect to published information content or with respect to a person that acts as a conduit or provides only editorial services in collecting, compiling or distributing informational content.

D. UCITA provides an implied warranty with respect to the licensee's proposed purpose and with respect to system integration. See proposed Section 2B-405.

1. Generally, if the licensor knows of the particular purpose for which information is required and that the licensee is relying upon the licensor's skill or judgment in providing that information, an implied warranty arises that the information is fit for that purpose.
2. No warranty arises with respect to aesthetics, market appeal or the like, or with respect to published informational content.
3. In general, if an agreement requires a licensor to provide or select a system, and the licensor has reason to know that the licensee is relying upon the skill or judgment of the licensor in selecting the appropriate components of that system, an implied warranty arises that the components will function together successfully as a system.

4. Compare Section 2B-405 to proposed revised Section 2-405.
- E. Implied warranties can be disclaimed in appropriate circumstances through the use of appropriate language, especially if that language is conspicuous (in the appropriate cases). See proposed Section 2B-406.
- F. Generally, a licensee that modifies a computer program does not invalidate any warranty regarding performance of an unmodified copy, but does invalidate any warranties regarding performance of the modified copy. See proposed Section 2B-407.
- G. In general, except for published informational content, a warranty to a licensee extends to all persons for whose benefit the licensor intends to supply the information or informational rights and who rightly use the information in a transaction or application of a kind in which the licensor intends information to be used. See Section 2B-409.

Copies of cited sections from the March 1, 1999 draft are attached to this outline.

EXHIBIT A

PRESS RELEASE REGARDING UCITA AS FREE-STANDING ACT

National Conference of Commissioners
on Uniform State Laws
American Law Institute
211 E. Ontario St., Suite 1300, Chicago, IL 60611
Chestnut Street
tel 312-915-0195, fax 312-915-0187
Philadelphia, PA 19104

215-243-1600, fax 215-243-1664

Contact: John M. McCabe
Elena A. Cappella
Legislative Director/Legal Counsel
tel 312-915-5976
215-243-1611
e-mail jmmccabe@nccusl.org
ecappella@ali.org

For Immediate Release

NCCUSL to Promulgate Freestanding Uniform Computer Information Transactions Act

ALI and NCCUSL Announce that Legal Rules for Computer

Information Will Not Be Part of UCC

April 7, 1999. The National Conference of Commissioners on Uniform State Laws (Conference) and the American Law Institute (Institute) have announced that legal rules for computer information transactions will not be promulgated as Article 2B of the Uniform Commercial Code, but the Conference will promulgate the rules for adoption by states as the Uniform Computer Information Transactions Act.

The Conference, a 107-year-old organization whose purpose is to prepare statutes for enactment uniformly among the states, and the Institute, a 76-year-old organization whose purpose is "to promote the clarification and simplification of the law and its better adaptation to social needs," have long been partners in drafting the various articles of the Uniform Commercial Code (Code or UCC). For the past several years the two organizations have worked cooperatively on a UCC project to prepare a statute that would codify evolving legal rules for computer information transactions.

The information industry has grown exponentially in the last decade and already exceeds most

manufacturing sectors in size. The numbers of transactions in information and their dollar value are immense. The Internet and information technology and commerce are major components of the future economic prosperity of the United States. As the nation moves from an economy centered around transactions in goods and services to an information economy, the need has grown dramatically for coherent and predictable legal rules to support the contracts that underlie that economy. Lack of uniformity and lack of clarity of the legal rules governing these transactions engender uncertainty, unpredictability, and high transaction costs. Nonetheless, it has become apparent that this area does not presently allow the sort of codification that is represented by the Uniform Commercial Code.

Institute members will have an opportunity to discuss the Uniform Computer Information Transactions Act (UCITA) at the Institute's annual meeting in San Francisco in May, but will not have votes on it. The proposed statute is then scheduled to be completed and promulgated at the annual meeting of the Conference in Denver this summer. It will be targeted by the Conference for immediate introduction and enactment beginning this fall in the 50 states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands. The Conference believes that UCITA can provide a framework in which sound business practices may further evolve in the marketplace bounded by standards of appropriate public policy.

###

EXHIBIT B

MARCH 1, 1999 DRAFT OF UCITA
(Cited Sections Only)

1 PART 1

2 GENERAL PROVISIONS

3 [A. Short Title and Definitions]

4 SECTION 2B-101. SHORT TITLE. This article may be cited as Uniform Commercial
5 Code - Software Contracts and Licenses of Information. [Computer Information Transactions]

6 Reporter's Note: The bracketed language indicates a change in title that might be considered in light of the new
7 scope. It has not been considered or approved by the relevant groups.
8

9 SECTION 2B-102. DEFINITIONS.

10 (a) In this article:

11 (1) "Access contract" means a contract electronically to obtain access to, or
12 information ~~in electronic form from~~, an information processing system of another person not
13 ~~owned or controlled by the licensee~~, or the equivalent of such access.

14 (2) "Access material" means any information or material, such as a document,
15 ~~authorization, address, or access code, acknowledgment, or other material necessary for a party~~
16 to obtain authorized access to information, or control or possession of a copy.

17 (3) "Attribution procedure" means a procedure established by law, regulation, or
18 agreement, or a procedure otherwise adopted by the parties, to for the purpose of verifying that
19 an electronic message, authentication, record, or performance is that of a specific person, or to for
20 the purpose of detecting changes or errors in the information content. The term includes a
21 procedure that requires the use of algorithms or other codes, identifying words or numbers,
22 encryption, callback or other acknowledgment procedures, or any other p rocedures that are
23 reasonable under the circumstances.

24 (4) "Authenticate" means to sign, or otherwise to execute or adopt a symbol or
25 sound, or to use encryption or another process with respect to a record, with intent of the

1 authenticating person to:

2 (A) identify that person;

3 (B) adopt or accept the terms or a particular term of a record that includes
4 or is logically associated with, or linked to, the authentication, or to which ~~referenced in a record~~
5 containing the authentication refers; or

6 (C) confirm the content ~~establish the integrity of the information in a record~~
7 that includes or is logically associated with, or linked to, the authentication, or to which
8 ~~referenced in a record~~ containing the authentication refers.

9 (5) "Automated transaction" means a contract formed or performed in whole or in
10 part by electronic means or by electronic messages in which the electronic actions or messages of
11 one or both parties that establish the contract are not intended to be reviewed in the ordinary
12 course by an individual.

13 (6) "Cancellation" means the ending of a contract by a party because of a breach
14 by the other party. "Cancel" has a corresponding meaning.

15 (7) "Computer" means an electronic device that can perform substantial
16 computations, including numerous arithmetic operations or logic operations, without human
17 intervention during the computation or operation.

18 (8) "Computer information" means electronic information, ~~including software~~,
19 that is in a form directly capable of being processed ~~or used by~~, or obtained from or through, a
20 computer, but does not include information referred to in Section 2B-104(2).

21 (9) "Computer information transaction" means a license or other contract whose
22 subject matter is (i) the creation or development of, ~~including the transformation of information~~
23 ~~into~~, computer information or (ii) to provide access to, acquire, transfer, use, license, modify, or
24 distribute computer information. The term does not include a contract ~~for to~~ distribution or

1 ~~create for purposes of distribution. of information in print form, such as in a book, newspaper or~~
2 ~~magazine, or to create information for the purpose of distribution in print form even if the~~
3 ~~information provided for distribution pursuant to the contract is delivered in electronic form.~~

4 (10) "Computer program" means a set of statements or instructions to be used
5 directly or indirectly in a computer to bring about a certain result. The term does not include
6 ~~separately identifiable informational content such as a separately identifiable motion picture or~~
7 ~~sound recording or the like.~~

8 (11) "Consequential damages" include compensation for losses resulting from a
9 party's general or particular requirements and needs of which the other party at the time of
10 contracting had reason to know and which losses could not reasonably be prevented by the
11 aggrieved party, and compensation for losses from injury to person or property proximately
12 resulting from any breach of warranty. The term does not include direct or incidental damages.

13 (12) "Conspicuous", with reference to a term, means so written, displayed, or
14 otherwise presented that a reasonable person against which it is to operate ought to have noticed
15 it. A term in an electronic record intended to evoke a response by an electronic agent is
16 conspicuous if it is presented in a form that would enable a reasonably configured electronic agent
17 to take it into account or react without review of the record by an individual. Conspicuous terms
18 include, but are not limited to, the following:

19 (A) with respect to a person:

20 (i) a heading in capitals in a size equal or greater than, or in
21 contrasting type, font or color to, the surrounding text;

22 (ii) language in the body of a record or display ~~that is in larger or~~
23 ~~other contrasting type, font, or color or is set off from the surrounding text by symbols or other~~
24 ~~marks that call attention to the language; and~~

1 (iv) otherwise incident to the breach; and

2 (B) do not include consequential or direct damages.

3 (265) "Information" means data, text, images, sounds, mask works, or works of
4 authorship. The term includes software.

5 (276) "Information processing system" means an electronic system ~~or facility~~ for
6 creating, generating, sending, receiving, storing, displaying, or processing ~~electronic~~ information.

7 (287) "Informational content" means information that is intended to be
8 communicated to or perceived by an individual in the ordinary use of the information, or the
9 equivalent of such information. The term does not include computer instructions that control the
10 interaction of a computer program with other computer programs or with a machine or device.

11 (298) "Informational rights" include all rights in information created under laws
12 governing patents, copyrights, mask works, trade secrets, trademarks, publicity rights, or any
13 other law that gives ~~permits~~ a person, independently of contract, a right to control or preclude
14 another person's use of or access to the information on the basis of the rights holder's interest in
15 that information.

16 (3029) "License" means a contract within this article that authorizes access to or
17 use of information or of informational rights ~~that exist or are to be created~~ and expressly limits the
18 contractual rights, permissions, or uses granted, expressly prohibits some uses, or expressly grants
19 less than all rights in the information. A contract may be a license whether or not the transferee
20 has ~~obtains~~ title to a licensed ~~a~~ copy. "License" includes an access contract and, for purposes of
21 [the Uniform Commercial Code], a consignment of a copy. The term does not include a
22 reservation or creation of a security interest.

23 (310) "Licensee" means a transferee in a license or other ~~an~~ agreement under this
24 article, ~~whether or not the agreement is a license~~. A licensor is not a licensee with respect to rights

1 reserved to it under the agreement.

2 (321) "Licensor" means a transferor in a license or other an agreement under this
3 article, ~~whether or not the agreement is a license~~. ~~As b~~Between a provider of access in an access
4 contract and its customer, the provider of access is the licensor. ~~As b~~Between the provider of
5 access ~~and a provider of the informational content to be accessed~~, the provider of content is the
6 licensor. ~~In If performance consists of an exchange of information or informational rights~~, each
7 party is a licensor with respect to the information, informational rights, or access it provides.

8 (332) "Mass-market license" means a standard form that is prepared for and used
9 in a mass-market transaction.

10 (343) "Mass-market transaction" means a transaction ~~within~~under this article
11 that is:

12 _____ (A) a consumer transaction; ~~or~~

13 _____ (B) ~~any other that is a transaction with an end-user licensee if: which~~

14 _____ (i) ~~the -transaction is for involves~~ information or informational
15 rights directed to the general public as a whole including consumers under substantially the same
16 terms for the same information;

17 _____ (ii) ~~A transaction other than a consumer transaction is a mass-~~
18 ~~market transaction only if the licensee acquires the information or rights in a retail transaction~~
19 ~~under terms and in a quantity consistent with an ordinary transaction in the a retail market; and~~

20 _____ (iii) ~~the -A transaction other than a consumer transaction is not a~~
21 ~~mass market transaction if it is:~~

22 _____ (IA) a contract for redistribution; ~~or (B) a contract for~~
23 public performance or public display of a copyrighted work;

24 _____ (IIG) a transaction in which the information is customized

1 or otherwise specially prepared by the licensor for the licensee other than minor customization
2 using a capability of the information intended for that purpose;

3 _____(III~~D~~) a site license; or

4 _____(IV~~E~~) an access contract.

5 (354) "Merchant" means a person that deals in information or informational rights
6 of the kind or that otherwise by the person's occupation holds itself out as having knowledge or
7 skill peculiar to the practices or information involved in the transaction, ~~whether of not the person~~
8 ~~previously engaged in such transactions,~~ or a person to which such knowledge or skill may be
9 attributed by the person's employment of an agent or broker or other intermediary that by its
10 occupation holds itself out as having such knowledge or skill.

11 (365) "Nonexclusive license" means a license that does not preclude the licensor
12 from transferring to other licensees the same information, informational rights, or contractual
13 rights within the same scope. For purposes of the [Uniform Commercial Code], the term includes
14 a consignment of a copy.

15 (376) "Present value" means the value, as of a date certain, of one or more sums
16 payable in the future or one or more performances due in the future, discounted to a date certain.
17 The discount is determined by the interest rate specified by the parties in their agreement unless
18 that rate was manifestly unreasonable when the transaction was entered into. Otherwise, the
19 discount is determined by a commercially reasonable rate that takes into account the
20 circumstances of each case when the transaction was entered into.

21 (387) "Published informational content" means informational content prepared for
22 or made available to recipients generally, or to a class of recipients, in substantially the same form .
23 The term does not include informational content that is:

24 _____(A) ~~and not~~ customized for a particular recipient, by an individual ~~that is a~~

1 enable the display and performance of the motion picture or sound recording. Such transactions are, in any event,
2 exclude from the scope of this article by virtue of the combined effects of Section 2B-104(1) and Section 2B-
3 104(6). The motion picture is excluded under subsection (6), while the program is excluded under subsection (1) as
4 a mere incident of the transfer of the motion picture product. The language in the definition here merely
5 corresponds to and confirms that result.

6 41. "Standard form." The definition refers to forms, not standard terms. A form consists of record
7 containing a group of terms prepared for frequent use as a group. Standard forms in modern commerce are
8 ubiquitous. The definition does not cover a tailored contract comprised of "terms" selected from prior agreements.
9 The record must itself have been prepared for repeated use and actually have been used without negotiation other
10 than of the ordinarily tailored terms noted in the definition. If a standard form is offered but then negotiated or
11 changed other than with respect to the ordinarily tailored terms noted in the definition, the resulting record is not a
12 standard form contract.

13 42. "Terminate." This definition conforms to original Section 2-106.
14

15 [B. General Scope and Terms]

16 SECTION 2B-103: SCOPE

17 (a) This article applies to computer information transactions.

18 (b) If a transaction involves computer information and goods, the following rules apply:

19 (1) This article applies to the computer information and to copies of computer
20 information, its packaging and documentation, but does not apply to a copy of software contained
21 in and transferred as part of other goods unless:

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

23 (B) giving the purchaser of the goods access to or use of the software is a
24 material purpose of the transaction.

25 (2) Except as provided in paragraph (1), Article 2 or 2A applies to goods in the
26 transaction.

27 (c) Except as provided in subsection (b), if another article of the [Uniform Commercial
28 Code] applies to a transaction, this article does not apply to the subject matter of the other article.

29 (d) The parties may by agreement provide that all or part of this article, including contract
30 formation rules, governs a transaction in whole or in part or that other law governs the transaction
31 in whole or in part. An agreement that this article does or does not apply to some but not all of a
32 transaction cannot alter a rule that otherwise applies and cannot be varied by agreement. In all
33

1 other cases, following rules apply to the agreement:

2 (1) An agreement to opt out of Article 2B cannot alter standards of good faith,
3 unconscionability, or public policy invalidation, or the defense in Section 2B-118 and the
4 limitations in Section 2B-716. An agreement to opt into Article 2B is subject to any similar
5 restrictions in otherwise applicable law. Neither agreement can alter an otherwise applicable
6 consumer protection law referenced in Section 2B-105.

7 (2) In a mass market transaction, the following rules apply:

8 (A) An agreement to opt into or opt out of Article 2B is enforceable only
9 if the transaction involves subject matter governed by Article 2B and subject matter governed by
10 other contract law, or if there is good faith uncertainty about whether Article 2B or other contract
11 law governs.

12 (B) The agreement cannot alter law applicable to distribution of
13 information in non-electronic form.

14 (3) Except for mass market transactions, the following rules apply:

15 (A) An agreement to opt out of Article 2B is not enforceable unless the
16 transaction involves subject matter not governed by Article 2B or there is good faith uncertainty
17 about whether Article 2B or other contract law governs.

18 (B) An agreement to opt into Article 2B is not enforceable unless the
19 subject matter of the transaction includes information or informational rights or there is good faith
20 uncertainty about whether Article 2B or other contract law governs.

21 **Definitional Cross Reference:**

22 "Agreement": Section 1-201. "Computer": Section 2B-102. "Computer information": Section 2B-102. "Computer
23 information transaction": Section 2B-102. "Consumer": Section 2B-102. "Copy": Section 2B-102. "Goods":
24 Section 2-1-. "Electronic": Section 2B-102. "Information": Section 2B-102. "Party": Section 1-201. "Purchaser":
25 Section 1-201. "Software": Section 2B-102.

26 **Reporter's Notes:**

27 1. *General Structure.* Section 2B-103(a) states the affirmative scope of Article 2B. Unless a
28 transaction is a "computer information transaction," this article does not apply. See Section 2B-102 (defining

1 "computer information transaction"). Subsections (b) and (c) deal with mixed transactions. Subsection (d) allows
2 the parties to opt into or out of the article by agreement. An "agreement" does not require a signed writing, but
3 refers to the bargain of the parties in fact, including applicable usage of trade and course of dealing. Section 2B-
4 104 states several exclusions from the scope of the article. As a contract statute, Article 2B does not alter or even
5 deal with intellectual property rights law.

6 2. *Scope of the Article.* This article applies to "computer information transactions" as defined in
7 Section 2B-102. The article focuses on transactions involving creation or distribution of computer software,
8 multimedia or interactive products, computer data, Internet, and online distribution of information. This leaves
9 unaffected the many transactions in the core businesses of other information industries (e.g., print, motion picture,
10 broadcast, sound recordings) whose business practices in their core businesses differ from those of the computer
11 software, online, and data industries. This article does not apply to print books, newspapers, or magazines.
12 Whether a magazine publisher can place contractual limitations on purchasers of copies of its magazines or books
13 is not addressed in Article 2B.

14 The scope of Article 2B is limited by the affirmative scope statement in subsection (a) which does
15 not include:

- 16 • Sales or leases of goods, except as indicated in Section 2B-103(b).
- 17 • Services contracts, except as in the definition of "computer information transaction".
- 18 • Creation or distribution of print materials (books, magazines, newspapers).
- 19 • Still photography.
- 20 • Casual, non-contractual exchanges of information.
- 21 • Creation or distribution of motion pictures, sound recordings, broadcast or cable programming.
- 22 • The subject matter of other articles of the Uniform Commercial Code.

23 3. *Transactions in Computer Information.* Transactions in computer information are contracts
24 whose subject matter entails the acquisition, development or distribution of computer information. "Computer
25 information" is information in a form directly capable of being processed or used by, or obtained from or through,
26 a computer, but does not include information of a type or used in a manner referred to in Section 2B-104(2). See
27 Section 2B-102.

28 Transactions in computer information differ from sales or leases of goods because the focus of the
29 transaction is on the information, its content or capability, rather than on the tangible items that contain the
30 information is delivered. In a sale of goods, the buyer obtains ownership of the subject matter of the contract (e.g.,
31 the specific toaster or television). That ownership creates exclusive rights in the subject matter (e.g., the toaster). In
32 contrast, a person in a transaction whose subject matter involves obtaining the computer information and that
33 acquires a copy of computer information may obtain ownership of the copy but does not, and cannot reasonably
34 expect to, own the information or the rights associated with it. Unlike a buyer of goods, the purchaser of a copy
35 often has little interest in retaining possession or control of the original disk that contained the information unless
36 the information remains on that disk and nowhere else. Often, a purchaser copies the information into a computer,
37 rendering the original diskette largely immaterial.

38 Transactions in computer information differ from transactions in other information because of
39 the nature of the information involved. Information capable of being processed in a computer is more readily
40 susceptible to modification and to perfect reproduction than information in other form such as printed books or
41 magazines. Indeed, to use computer information, one must copy it into a machine. See *Stenograph v. Bossard*, 46
42 U.S.P.Q.2d 1936 (D.C. Cir. 1998); *MAI Systems Corp. v. Peak Computer, Inc.*, 991 F.2d 511 (9th Cir. 1993). In
43 order to access and view computer information from a remote computer, one must copy it into the local computer.
44 This creates copyright law issues with which this article does not deal. It also creates contract law issues addressed
45 in this act.

46 4. *Computer.* The term "computer" is defined in Section 2B-102. The definition comes from a
47 leading dictionary of terms related to the computer industry and conforms to ordinary definitions. It does not
48 include traditional televisions, VCR or similar systems whose automated functions are primarily intended to
49 receive or transmit broadcasts, or to perform or display motion pictures or sound recordings. In any event, this
50 article does not apply to all information received or processed by a computer and does not apply to computers per
51 se. Whether or not received by a computer, motion pictures, broadcast and similar programming are excluded
52 from this article under Section 2B-104.

53 5. *Included Transactions.* The scope of this article turns on the definition of "computer information
54 transaction." "Computer information transactions" include transactions involving the creation, distribution, or

1 license of computer information, including software. Section 2B-102. Transactions for information not in a form
2 directly capable of computer processing are excluded unless the parties agree to be governed by its provisions.

3 For a transaction to be included, acquiring the computer information, access to it, or its use must
4 be the subject matter of the transaction and not a mere incident of another type of transaction. The mere fact that
5 information is sent or recorded in digital form is not sufficient. Thus, for example, a contract for airplane
6 transportation does not become an Article 2B transaction simply because the ticket is in electronic form. The
7 subject matter of the transaction is not the computer information, but the service – air transportation from one
8 location to another. Similarly, an insurance policy prepared for a client and recorded in digital form is not a
9 computer information transaction, but simply a contract for insurance whose result or terms is evidenced in digital
10 form. A contract for a digital signature certificate is a contract for digital certification or identification services, not
11 a contract whose subject matter is the computer information. This article does not apply to the many cases in which
12 a person provides information to another person for purposes of another transaction such as making an
13 employment or loan application.

14 Typically, a contract included in this article is for commercial use or distribution of the computer
15 information. The article thus includes, for example, a license allowing a company to transform photographs into
16 digital form for re-licensing in that form to others. It also includes a contract to compile in digital form a database
17 of names for use by a client as a product furnished to others for use as a mailing list.

18 *a. Creation, Development and Support.* The article applies to contracts for the
19 development or creation of computer information, such as software development contracts and contracts for the
20 creation of computer databases. Contracts of this type have been subject to inconsistent court rulings, applying the
21 U.C.C. or common law contract theories based on fine and not clear distinctions. Article 2B applies to all such
22 transactions. The article does not, however, cover contracts for development or creation of motion pictures, sound
23 recordings, or broadcast programs. These are excluded from the definition of “software” and the definition of
24 “computer information.” In any event, transactions of this type are excluded under Section 2B-104. This article
25 also does not cover contracts for the creation or development of print books or articles which do not involve
26 computer information.

27 *b. Computer information Transaction.* The article covers transactions for access to,
28 acquisition, transfer, use, or distribution of computer information. This includes all transactions involving the
29 distribution or use of computer programs. Such transactions are covered whether they involve a license or an
30 unrestricted sale of a copy of the program.

31 This article also covers transactions involving access to or information from a computer system.
32 This encompasses Internet and similar systems that allow access to information databases. This form of
33 information distribution does not include broadcast of digital information involving motions pictures, sound
34 recordings or the like.

35 *6. Mixed Transactions.* Inevitably, as with Article 2 transactions in goods, some transactions in
36 computer information present questions about to what extent the transaction is governed by Article 2B and to what
37 extent it is governed by common law or law in another statute. Transactions that are governed by several sources of
38 contract law in a single transaction (i.e., “mixed transactions”) are so common under current law as to be
39 unexceptional and, indeed, virtually universal. They routinely exist in all consumer transactions (e.g., videos, CDs,
40 and software) and all transactions involving copyrighted works. For consumer goods, transactions are governed by
41 common law, Article 2 (or 2A), and state or federal consumer law. For copyrighted works, transactions are
42 variously (and non-uniformly) governed by common law, copyright law, Article 2 (or 2A), and various state
43 statutes. While Article 2B provides more uniformity and clarity on the issues it addresses, it is supplemented by
44 common law (Section 1-103), copyright law, and consumer or other state law (Section 2B-105).

45 Here, the relevant issue is not whether a single or multiple sources of contract-related law apply
46 (because multiple sources always apply), but whether Article 2B, rather than another source, is involved in the
47 mix. On this issue, courts use two distinct approaches under other U.C.C. provisions and under common law.

- 48 • A “gravamen of the action” standard: applies rules tailored to a subject matter only to that particular
49 subject, asking in effect to which subject matter does the particular dispute pertain.
- 50 • A “predominant purpose” standard: makes a determination about the overall transaction and applies the
51 law applicable to the predominant subject matter to the “entire” transaction.

52 Article 2B adopts a modified gravamen of the action approach in subsection (b) with respect to goods and in
53 subsection (c) with respect to the subject matter of other articles of the U.C.C., but as discussed in a following note,
54 courts may use a predominant purpose test with respect to non-U.C.C. subject matter.

55 *7. Computer Information and Goods.* In a transaction in which computer information and goods

1 are involved, Article 2B applies to the computer information, while Article 2 (or Article 2A) applies to the goods.
2 This recognizes the differences in the two types of subject matter and the transactional differences that result from
3 the different subject matter.

4 There are two exceptions. The first, in Section 2B-103(b), is that Article 2B applies to goods that
5 are merely a copy, documentation, or packaging of the computer information covered by this article. In effect,
6 these "goods" are mere incidents of the computer information and, as such, should be incorporated into this article
7 to prevent unintended results through the interface of the U.C.C. transactional articles. Article 2B covers both the
8 computer software and the media on which the software is copied or documented.

9 The second exception in subsection (b) concerns copies of software contained in and sold or
10 leased as part of goods. Section 2B-103(b)(1) provides that, if software is embedded in goods, Article 2B applies to
11 the copy of the software only if it is part of a computer or a computer peripheral or if giving the purchaser access
12 to the functional attributes of the software is a "material purpose" of the transaction. In fact, however, in most mass
13 market transactions where the issues are most significant, which law applies often does not alter the outcome.

14 Article 2B governs contract issues for software embedded in goods other than a computer or a
15 computer peripheral only if a material purpose of the transaction is to provide the functional attributes of the
16 program. Thus, while a television may be operated by software, the material purpose of the sale of an ordinary
17 television set is to acquire the set and television reception. This is not an Article 2B transaction, but that result
18 may change if television sets evolve into computing systems in which a material purpose for the user is to obtain
19 software processing. Similarly, while an automobile may have some functions operated by a computer program,
20 the program that operates the brakes or other functions is not a primary purpose of the transaction for the
21 purchaser. The transaction is within Article 2 or 2A. On the other hand, the development or supply contract for
22 the program that enables the manufacturer to use the program in its system, however, is in Article 2B. Similarly,
23 separately licensed software in a digital camera that enables the camera to be linked to a computer so that images
24 can be transferred back and forth and manipulated is within Article 2B. Factors suggesting that the program's
25 processing capacity is a material focus of the transaction include the extent to which the processing capabilities of
26 the software is a dominant focus of the product's appeal, the extent to which discussions of the parties focused on
27 that processing capacity in contrast to other attributes of the product, and the extent to which the agreement makes
28 those processing capabilities a separate focus for agreed terms.

29 **8. Computer Information and other UCC Articles.** The articles of the U.C.C. control with
30 reference to their subject matter. For example, Article 8, and not this article, deals with investment securities and
31 rights or remedies with respect to that subject matter, even though in modern practice securities may be dealt with
32 through a computer. The same applies with respect to the subject matter of Article 4 and Article 4A: payment
33 systems, checks, and funds transfers. This follows the same rule that applies under original Article 2 and 2A.
34 Similarly, if a provision of Article 9 conflicts with a provision of Article 2B, Article 9 controls. However, if a
35 computer information transaction is involved, such as a license of computer information, Article 2B applies to the
36 terms and enforcement of that license.

37 **9. Computer Information and Other Contract Law.** Where the issue does not involve goods or the
38 subject matter of other articles of the U.C.C., courts should follow general interpretation principles to determine
39 the applicability of Article 2B. In most cases involving computer information and other subject matter, this will
40 entail application of a form of the "predominant purpose" test as used in most states with respect to original Article
41 2, but modified here to reflect the issues presented in reference to Article 2B. The predominant purpose is judged
42 as of the time of the contracting.

43 If computer information is the predominant purpose of the transaction, Article 2B rules apply
44 instead of other contract law (e.g., common law). The predominant purpose test has been applied by courts dealing
45 with the scope of Article 2 where goods and other subject matter (e.g., services) are involved in a transaction. The
46 basic test asks whether Article 2B or other subject matter constitutes the main intended focus of the contract. Thus,
47 in a contract between an author and a publisher, if the author agrees to allow the publisher to distribute the work in
48 "book, motion picture or digital form", the agreement is outside Article 2B if the predominant purpose is to give
49 the publisher the right of first publication in book (printed) form or the right to motion picture uses. This is true if,
50 for example, the intended primary exploitation of the contracted-for work is in print or motion picture form, both
51 of which are outside Article 2B. The fact that "electronic rights" are also covered in the agreement does not result
52 in Article 2B coverage since the focus is on other rights. Similarly, a contract with a producer whose predominant
53 purpose is to develop a motion picture for distribution as such does not come within Article 2B simply because the
54 grant includes secondary rights to use parts of the film in interactive contexts. The predominant purpose is
55 creation of a motion picture. On the other hand, a contract giving a software publisher the right to reproduce a

1 photographic image in "software and other works" is governed by Article 2B if the predominant purpose is to allow
2 use in computer information even though use in print form is also permitted. Similarly, a license to acquire rights
3 to use software by a motion picture studio which may use the software as a tool in creating motion pictures is an
4 Article 2B transaction, while a license to use digital scenes or images in a motion picture is excluded.

5 In applying the predominant purpose test to information transactions, the standard should be
6 refined to include consideration of the type of transaction envisioned in the parties' agreement. For example, in a
7 loan transaction a loan officer might deliver a diskette containing interest rate calculations for use by the borrower.
8 Under the predominant purpose test, no part of the transaction is covered by Article 2B because the predominant
9 purpose of the agreement between the lender and borrower is the common law loan. Further, the transactional type
10 mirrors a common law loan transaction and the mere presence of the software does not alter this fact. This type of
11 an approach is more appropriate than that of some courts which, under prior law, applied sale of goods rules to
12 software development transactions because, even though the bulk of the contract concerned development services,
13 the program was to be delivered on a diskette or tape. The proper analysis should have been whether the principles
14 of Article 2 (e.g., damage calculation rules, conforming tender rule, rules on timing of ownership transfer, rules on
15 duration of license, effect of negligence, contract modification, etc.) fit the nature of the transaction in fact better
16 than would the rules available under other law (e.g., common law regarding services contracts). This more
17 nuanced analysis is more appropriate for new technology areas in order to avoid elevating form over substance

18 While the cases under Article 2 thus provide some guidance, it is appropriate to consider
19 additional factors. Thus courts should consider the extent to which the transaction as a whole corresponds to the
20 transactional framework involved in computer information transactions. If it does, Article 2B should apply to the
21 entire transaction, but if not, it is possible that Article 2B should not apply at all. Among the transactional factors
22 that courts should consider are: 1) the nature of the underlying intellectual property rights involved, including,
23 with respect to copyrighted works, differences in the rights provided under the Copyright Act for different types of
24 works, 2) the extent to which regulatory regimes apply to the subject matter and were considered in the transaction,
25 3) the extent to which allocation of liability risk for inaccurate or improperly functioning information is a concern,
26 and 4) the extent to which the parties involved are performing services rather than information-related
27 transactions.

28 The test applies at various levels of use or distribution, but the result may differ at each level. For
29 example, a courier company that licenses communications software from a software publisher is engaged in an
30 Article 2B transaction. The subject matter of the agreement is a license in the software itself. If the courier company
31 provides the software to customers merely to access data on the current location of packages, however, the
32 predominant purpose may be the services. If the software publisher enters into a license with the end user, that
33 license is in Article 2B.

34 The predominant purpose test can apply only if the parties have not otherwise agreed as to
35 coverage by Article 2B or other law. In the foregoing illustrations, for example, if the parties elect coverage under
36 Article 2B, that agreement governs as would an agreement that Article 2B should not apply at all. In any event,
37 Article 2B coverage or non-coverage does not create "mixed contracts." The only issue is whether Article 2B
38 supplants common law or other rules otherwise applicable to a transaction. Agreement here, as elsewhere in the
39 U.C.C., can be found in the express terms of the contract as well as in the usage of trade or course of dealing
40 between the parties, or as inferred from the circumstances of the contracting.

41 10. *Contract Choice.* Subsection 2B-103(d) follows the basic rule that contract choices control and
42 applies this principle to determining what law governs. The subsection distinguishes between decisions to opt
43 entirely into or out of Article 2B subsection (d)(1-3), and decisions to do so only in part (subsection (d)).

44 The parties can agree to have Article 2B apply to the entire transaction, part of the transaction, or
45 none of the transaction. These choices, of course, deal with applicability of Article 2B and not with whether other
46 law continues to apply to issues not dealt with in Article 2B. Also, a contract choice here is effective irrespective of
47 any "predominant purpose" of the transaction. An enforceable decision to opt into or out of Article 2B may render
48 the "predominant purpose" test moot.

49 In determining whether the agreement to opt-into or opt-out of Article 2B was formed and is
50 enforceable, a court will ordinarily apply the contract formation rules of this article and the general concept of
51 agreement in the U.C.C. This is especially true where the transaction involves some subject matter governed by
52 Article 2B. Here, as elsewhere, an agreement can be found as easily in the express terms of the contract of the
53 parties as in course of dealing, usage of trade, or as inferred from the circumstances.

54 For commercial parties, the ability to choose Article 2B or another body of state contract law
55 gives an important opportunity to avoid uncertainty and the effects of potentially conflicting rules potentially

1 applicable under multiple bodies of state contract law (e.g., Article 2B, Article 2, Article 2A, and common law).
2 This power of contract choice is especially important in that Article 2B does not apply to all transactions in
3 information. On the other hand, especially in contracts with no bargaining, there is an interest on the part of the
4 party who receives non-negotiable terms that the choice not unfairly deprive it of protections mandated under the
5 other law that may not be varied by agreement. This interest, of course, does not validly apply to contract rules
6 that can be varied by agreement. The provisions of subsection (d) balance the interests in other contexts.

7 *a. General Limits: Opting Entirely Out.* Contract terms on this issue are subject to rules
8 on unconscionability and fundamental public policy concerns. In addition, subsection (d) contains several
9 restrictions on enforcing the choice of the parties on whether Article 2B governs or not.

10 (1). *Subject Matter Limitations.* The ability to *opt out* of Article 2B exists only in
11 certain cases. In essence, in both a mass market and any other transaction, the parties by agreement can opt out of
12 Article 2B only if the transaction includes subject matter that would not otherwise be governed by Article 2B (a
13 "mixed transaction"), or if there is good faith uncertainty about whether Article 2B applies. Thus, in the latter
14 case, the parties may agree to opt out (or opt into) Article 2B to avoid the uncertainty of whether Article 2 or
15 Article 2B applies. The opt out is presumably into the law that governs the other subject matter or the one whose
16 application was uncertain.

17 A contract choice here is effective irrespective of any "predominant purpose" of the transaction,
18 but may render the "predominant purpose" test moot. The "predominant purpose" test is applicable only if in fact
19 the transaction does involve Article 2B subject matter *and* other subject matter, at least in part, or if a contract
20 choice to opt out is ineffective in whole or in part under this section. In the latter event, a court could conclude
21 that under a predominant purpose test, particular law governs.

22 (2). *Rules Affected.* Subsection (d)(1) states the general rule that a decision to *opt*
23 *out* of Article 2B cannot alter certain fundamental rules that would be applicable to the contract if Article 2B
24 applied to part of the transaction. These include standards of good faith, unconscionability and the public policy
25 rule in Section 2B-105(b). For other than the listed Article 2B provisions, opt out is not substantively restricted,
26 but it is limited with respect to the transactions in which it can be used.

27 In reference to substantive rules, in most cases, Article 2B allows their variation by agreement
28 and, thus, these rules can be varied by a general opt-out. For those few Article 2B rules that cannot be varied by
29 agreement, except as listed in the subsection, the interest in allowing certainty prevails. An opt-out places the
30 entire contract under a different legal regime with its own applicable rules that deal with these topics. This is true,
31 for example, for limits on liquidated damage terms. Common law, Article 2 and Article 2A all contain provisions
32 dealing with this topic and, while somewhat similar, these rules make a balance attuned to those other legal
33 regimes. A rule which makes ineffective a general contract choice to the extent it affects this rule would create a
34 situation in which an agreement would be required to comply with Article 2B (for its subject matter), Article 2 (for
35 goods) and common law (for other subject matter) in the same transaction. The alternative concept, adopted here,
36 is that the opt-out brings with it both the positive and the restrictive parts of the other body of law in full, and
37 results in the loss of both the positive and restrictive parts of Article 2B. This is also true, for example, in a
38 decision to opt out of Article 2B where Article 2 is the other law and governs as to the creation and disclaimer of
39 warranties. It is also the case of the effect of an opt-out on the provisions of Section 2B-208 on both the
40 enforceability of a mass market form and the return right. If there is an opt-out, other law applies to both issues.

41 The basic theme is that a contract choice to opt out of Article 2B as a whole (see subsection (d)(4)
42 on partial opt out) should ordinarily be enforced and that the interests of the parties are properly safeguarded under
43 the other law (U.C.C. or common law) as a whole. The issues listed in subsection (d)(1) represent exceptions
44 under current law or policies that are so fundamental that their variance should not be permitted.

45 *b. General Limits: Opting In.* Contract terms on this issue are subject to standards of
46 unconscionability and public policy concerns. In addition, subsection (d) contains several restrictions on enforcing
47 the choice of the parties on whether Article 2B governs or not.

48 (1). *Subject Matter Limitations.* The ability to opt into Article 2B exists only in
49 certain cases. In a mass market transaction, the parties can opt in only if the transaction involves Article 2B
50 subject matter (along with other subject matter) or if there is good faith uncertainty about whether Article 2B
51 applies. In addition to simply recognizing the role of contract choice, the goal of allowing this option to take effect
52 is to allow parties to reduce conflicting rules and uncertainty, some of which are caused by Article 2B itself
53 (because of the decision to focus on a narrow group of transactions). If there is no Article 2B coverage and no
54 good faith uncertainty, the transaction in the mass market should be governed under otherwise applicable law. In
55 this respect, subsection (d)(3)(B) further indicates that a decision to opt into Article 2B cannot alter the law

1 regarding distribution of non-electronic copies, such as books and magazines, which are outside the scope of this
2 article.

3 Outside the mass market, interests in allowing parties to make and enforce contractual
4 choices is even greater. Yet, even here, it seems inappropriate to allow a decision to opt into Article 2B where the
5 transaction involves subject matter entirely unrelated to the general nature of this article – transactions in
6 information. Subsection (d)(3) allows a decision to opt into Article 2B, but only if the transaction subject matter
7 includes information or informational rights. Thus, a decision by parties to a commercial trademark license to be
8 governed by Article 2B is enforceable, while the decision by parties to a real estate lease is not enforceable.

9 The overall effect of the subsection is as follows: Assume that three commercial parties
10 enter an agreement to create a product involving cable services (common law), software or multimedia (Article 2B)
11 and hardware (Article 2). The parties to the commercial agreement may agree that any of the three laws governs
12 and, thus, avoid inconsistent and overlapping rules. As to Article 2B subject matter, the agreement does not alter
13 good faith, unconscionability, public policy or self-help rules. If the resulting product is distributed in a mass
14 market transaction, if it involves Article 2B subject matter, the agreement may elect Article 2B or other law as
15 covering the deal, with the limits as stated above, but if there is no Article 2B subject matter in the product, Article
16 2B cannot be made to apply.

17 (2). *Rules Affected.* Subsection (d)(1) states the general rule that a decision to *opt*
18 *in* cannot alter any rule of otherwise applicable law similar to the listed rules: good faith, unconscionability, the
19 public policy rule in Section 2B-105(b), the self-help limitation, and the electronic consumer defense. In addition,
20 neither an opt-out, nor an opt-in can vary consumer protection laws described in Section 2B-105.

21 The discussion in the notes dealing with limits on the right to opt out are relevant here. In
22 reference to substantive rules, in most cases, contract law allows variation by agreement and these rules can be
23 varied by a general opt-in. For those few other rules, the interest in allowing contract choices that enhance
24 certainty prevails, especially where the rule does not involve a consumer protection that cannot be varied by
25 contract. Opting into Article 2B places the entire contract under this legal regime. The basic theme is that a
26 contract choice to opt into Article 2B as a whole (see subsection (d)(4) on partial opt-in) should ordinarily be
27 enforced.

28
29 **SECTION 2B-104. EXCLUSIONS FROM THIS ARTICLE.** This article does not

30 apply to:

31 (1) a contract or a transaction that provides access to, use, transfer,
32 clearance, settlement, or processing of:

33 (A) deposits, loans, funds, or monetary value represented in electronic
34 form and stored or capable of storage electronically and retrievable and transferable electronically,
35 or other right to payment to or from a person;

36 (B) an instrument or other item;

37 (C) a payment order, credit card transaction, debit card transaction, or a
38 funds transfer, automated clearing house transfer, or similar wholesale or retail transfer of funds;

39 (D) a letter of credit, document of title, financial asset, investment
40 property, or similar asset held in a fiduciary or agency capacity; or

TAB 8
Nimmer/ Ring proposal
SCOPE OF THE ARTICLE

Note:

This proposal builds on and refines the scope concept approved by the Committee at its last meeting. Most importantly, the proposal clarifies definitions central to the scope of the article. It also clarifies the right of the parties to opt into or out of Article 2B coverage.

(8) "Computer information" means information in an electronic form that is obtained from or through the use of a computer, or that is in digital or equivalent form capable of being processed by a computer, but does not include information referred to in Section 2B-104(2).

(9) "Computer information transaction" means an agreement a purpose of which is to create or modify, transfer, license, or provide access to computer information or informational rights in computer information. The term includes support agreements to the extent covered in Section 2B-616.

(25) "Information" means data, text, images, sounds, mask works, software, or collections or compilations thereof.

Notes:

1. The comments to "computer information" will indicate that the reference to "equivalent form" refers to analog and any future computational technologies, eliminating the possibility that the reference to "digital" technology would otherwise lock the scope of the article into a particular, current technology. They will also explain that the term does not cover information merely because it could be scanned or otherwise entered into a computer, but is limited to electronic information form or capable directly of being processed in a computer.

2. The comments to "computer information transaction" will indicate that the concept obviously does not cover transactions involving books, magazines or other print material. This is true even though the information provided under a contract for the distribution of information in a print publication is performed by the delivery of the text on a computer diskette. The purpose of such transactions is to engage in print publication and distribution, not in a computer transaction.

SECTION 2B-103: SCOPE

(a) This article applies to computer information transactions.

(b) If a transaction involves computer information and goods, the following rules apply:

(1) This article applies to the computer information and to copies of it, its packaging and documentation. However, if a copy is contained in and sold or leased as part of goods, this article applies to that copy only if:

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

(B) giving the purchaser of the goods access to or use of the computer information is a material purpose of the transaction.

(2) Except as provided in paragraph (1), Article 2 or 2A applies to the goods in the transaction.

(c) If this article and another article of the U.C.C. other than Article 2 or 2A, apply to a transaction, the following rules apply:

(1) If there is a conflict between this article and Article 9, Article 9 governs.

(2) In all other cases, this article does not apply to the subject matter of the other article.

[(d) If a transaction involves computer information and other subject matter, but not within subsection (b) or (c) and is not excluded under Section 2B-104, this article governs if the computer information is the primary purpose of the transaction.]

(e) Except as provided in subsection (c)(1), the parties may agree that this article, including contract formation rules, governs a transaction ("opt in") or that other law governs the transaction and this article does not apply ("opt out"). The agreement is subject to the following rules:

- (1) An agreement to opt into this article in a mass-market transaction:
 - (i) does not alter the applicability or effect of a consumer law referred to in Section 2B-105(d); and
 - (ii) is unenforceable with respect to a purchase of a tangible copy of information in print form.
- (2) An agreement to opt out of this article in a mass-market transaction:
 - (i) does not alter the applicability or effect of standards of good faith, unconscionability, or public policy invalidation under this article, or the defense in Section 2B-118; and
 - (ii) cannot alter the limitations in Section 2B-716.

Notes:

1. Subsections (b) and (c) adopt approaches to over-lapping coverage among articles of the U.C.C. The rules allow each article to apply to its own subject matter. The exception in subsection (b) retains the approach to allocating coverage between Article 2 (or 2A) and Article 2B which gives coverage of computer information embedded in goods to Article 2 (or 2A) except with respect to the circumstances described in subsection (b), and gives coverage of copies and documentation relating to computer information to Article 2B.

2. Subsection (d) adopts the principle discussed in notes to the prior draft, applying a predominant purpose to "mixed transactions" where the non-Article 2B subject matter is not within another article of the code. This would apply, for example, to a transaction involving computer information and services, or involving computer information and print information.

3. Subsection (e) simplifies and clarifies the prior draft with respect to the ability of parties to opt into or out of Article 2B. It follows a principle of contract choice, subject to relatively limited exceptions intended to protect specific interests. Among the limitations is the rule that the agreement cannot alter the rule relating to conflicts with Article 9 as stated in subsection (c)(1).

Subsection (e)(1) deals with opt in agreements and clarifies that this agreement cannot alter the effect of otherwise applicable consumer protection rules. Subsection (e)(1) provides in effect that the parties cannot opt into Article 2B in a mass market transaction involving a purchase of information in print form. Within the U.C.C., the term "purchase" includes all forms of voluntary transfers. The limitation applies only with respect to mass-market transactions and, thus, would not preclude parties to a commercial agreement that does not occur in a retail market from electing to be governed by Article 2B.

Subsection (e)(2) deals with agreements to opt out of Article 2B. Here, in agreeing to opt out of Article 2B, the parties in effect agree to place themselves under a body of law developed in common law or another U.C.C. article, each of which provides its own integrated set of rules applicable to particular transactions. That being true, the provisions of that other law supplant Article 2B rules with their own approach to fairness and other issues. There are two primary exceptions. The first concerns mass-market transactions where it seems appropriate to preclude alteration of fundamental protections in light of the nature of the agreement that is likely in a retail market. The second concerns the limitations on electronic self-help.

1 (b) When it is claimed or appears to the court that the contract or any term thereof may be
2 unconscionable the parties shall be afforded a reasonable opportunity to present evidence as to its
3 commercial setting, purpose and effect to aid the court in making the determination.

4 **Uniform Law Source:** Section 2-302.

5 **Definitional Cross References:**

6 "Contract": Section 1-201. "Court": Section 2B-102. "Term": Section 1-201.

7 **Reporter's Note:**

8 1. *Scope of the Section.* This section adopts the Article 2 doctrine that allows courts to invalidate
9 unconscionable contracts or terms. The use of the word "term," rather than "clause," is stylistic only with no
10 substantive change intended.

11 2. *Basic Policy and Effect.* This section allows courts to rule directly on the unconscionability of
12 the contract or a particular term therein and to make a conclusion of law as to its unconscionability. The basic test
13 is whether, in light of the general commercial background and the commercial needs of the particular trade or case,
14 the terms involved are so one-sided as to be unconscionable under the circumstances existing at the time of the
15 making of the contract. Subsection (b) makes it clear that it is proper for the court to hear evidence on these
16 questions. The principle is one of the prevention of oppression and unfair surprise and not of disturbance of
17 allocation of risks because of superior bargaining power.

18 3. *Electronic commerce.* While this article confirms the enforceability of automated contracting
19 practices involving "electronic agents," in some cases automation may produce unexpected results because of errors
20 in programs, problems in communication, or other unforeseen circumstances. When this occurs, common law
21 concepts of mistake may apply, as may the provisions of Section 2B-118 and Section 2B-204. In addition,
22 unconscionability doctrine may apply to invalidate a term caused by breakdowns in the automated contracting
23 processes.

24 4. *Remedy.* The court, in its discretion, may refuse to enforce the contract as a whole if it is
25 permeated by the unconscionability, or it may strike any single term or group of terms which are so tainted or
26 which are contrary to the essential purpose of the agreement, or it may simply limit unconscionable clauses so as to
27 avoid unconscionable results.

28 5. *Decision of the court.* Unconscionability is a decision to be made by the court. The commercial
29 evidence allowed under subsection (b) is for the court's consideration, not the jury's. Only the terms of the
30 agreement which result from the court's action on these matters are to be submitted to the general triers of fact for
31 resolution of a matter in dispute.

32

33 **SECTION 2B-111. MANIFESTING ASSENT.**

34 (a) A person or electronic agent manifests assent to a record or term in a record if the
35 person, acting with knowledge of, or after having an opportunity to review the record, term or a
36 copy of it, or if the electronic agent, after having had an opportunity to review:

37 (1) authenticates the record or term;

38 (2) in the case of the conduct or statements of a person, the person intends to
39 engage in the conduct or make the statement and has reason to know that the other party may
40 infer from the conduct or statement that the person assents to the record or term; or

1 (3) in the case of operations of an electronic agent, the electronic agent engages in
2 operations that the circumstances clearly indicate constitute acceptance.

3 (b) If this article or other law requires assent to a specific term, a ~~person or electronic~~
4 ~~agent does not manifest assent to that term unless it had an opportunity to review the term and the~~
5 manifestation of assent must relates specifically to the term.

6 (c) Conduct or operations manifesting assent may be proved in any manner, including a
7 showing that a procedure existed by which a person or an electronic agent must have engaged in
8 the conduct or operations in order to obtain, or to proceed with use of the information or
9 informational rights. Proof of assent depends on the circumstances. Proof of compliance with
10 subsection (a)(2) is sufficient if there is conduct that assents and subsequent conduct that
11 electronically reaffirms assent.

12 **Uniform Law Source:** Restatement (Second) of Contracts § 19.

13 **Definitional Cross References.**

14 "Authenticate". Section 2B-102. "Electronic agent". Section 2B-102. "Information". Section 2B-102.

15 "Informational Rights": Section 2B-102. "Record". Section 2B-102. "Term". Section 1-201.

16 **Reporter's Notes:**

17 1. *Scope and Purpose.* This section defines "manifestation of assent." "Manifesting assent" has
18 several roles in contract law. The two primary roles treat manifested assent as 1) a way by which a party indicates
19 agreement to a binding contract, and 2) a standard to determine when a party adopts the terms of a record as the
20 terms of the contract. Often, the same conduct both adopts the terms of a record and constitutes agreement to the
21 relationship. In addition to these two primary roles, in some cases, this article requires agreement or assent to a
22 term to establish the enforceability of the term.

23 2. *Source and General Theme.* "Manifesting assent" as a term comes from the *Restatement*
24 *(Second) of Contracts* § 19. This section corresponds substantively to the *Restatement*. While the concepts that
25 underlie the *Restatement* on this point are present throughout U.S. law, the concept is more fully explicated here
26 than in case law and codification lends itself to uniformity in terminology and application.

27 Manifesting assent does not require a signature, any specific type of language or conduct. It can
28 be shown by an appropriate authentication, by conduct including use or other performance with respect to the
29 subject matter, or by words. In electronic commerce, it especially important to clarify the conditions under which
30 conduct may establish contractual relationships and to expressly recognize the diverse alternatives that exist.

31 3. *Three analyses.* Determining whether a person manifested *assent to a record* under this article
32 entails analysis of three issues:

33 • First, the person must have had knowledge of the record or term or an opportunity to review it.
34 Opportunity to review requires that the record be available in a manner that ought to call it to the
35 attention of an ordinary reasonable person. Section 2B-112.

36 • Second, assuming an opportunity to review, the person must authenticate the record or term, orally
37 express assent, or engage in conduct with reason to know that in the circumstances the conduct
38 indicates assent. *Restatement (Second) of Contracts* § 19. Authenticating a record requires executing
39 or adopting a symbol or processing the record with intent to authenticate. Section 2B-102. Conduct
40 manifests assent if the party acted with knowledge or reason to know that this would infer assent.

- 1 • Third, the conduct or authentication must be attributable to the person to be bound. General agency
2 law and Section 2B-116 provide standards for attribution.

3 4. *Assent by Authentication.* Under current law, a person indicates assent to a record or term by
4 signing the record or term. In this article, "authentication" replaces "signature", but the concept remains the same.
5 Signing a record containing contract terms in a setting that entails the formation of an agreement ordinarily
6 indicates the intent of the signing party to show assent to the terms or, at least, that a reason to know the act of
7 signing or authenticating can be inferred as an expression of assent to the contract and terms. In most cases, as
8 under current law on signatures, no question exist about the meaning of a signature or authentication or the context
9 will clearly indicate the appropriate inference. In the few cases in which doubt exists, the authentication must be
10 made with intent to adopt or agree to the record. Section 2B-119 states a presumption generally true under prior
11 law on signatures: unless the circumstances indicate to the contrary, an authentication encompasses an intent to
12 identify the party, accept or adopt the record and its terms, and establish the integrity of the record's contents. The
13 intent pertains to the person to be bound, not to the person receiving the authenticated record and confirming that
14 the authentication is that of the other party. See notes to Section 2B-102(4).

15 5. *Assent by Conduct or Words.* Assent also occurs if a party acts (or fails to act), or makes a
16 statement, having reason to know these will be inferred as assent by the other party. Determining when this occurs
17 entails reference to the circumstances. The issue does not involve proof of subjective intent, knowledge, or
18 purpose, but objective characteristics of assent, including whether there was an act or a failure to act voluntarily
19 engaged in with reason to know the inference of assent that would be drawn. Assent does not require that the party
20 have an ability to negotiate or alter terms. However, the person's conduct or failure to act must be voluntary. This
21 is satisfied if the alternative of refusing the contract existed even if refusal would leave no alternative source for the
22 refused deal.

23 Of course, actual knowledge that the inference will be drawn from particular conduct suffices.
24 More generally, "reason to know" can be indicated by one or more of the following: the nature of the conduct;
25 whether the context, including any language on a package, a container or in a record, indicates what actions
26 indicate assent; whether the actor could decline to engage in the conduct and return the information; what
27 information was communicated to the actor before the conduct occurred; whether the conduct resulted in access to
28 and use of information that was offered subject to contract terms; what are the ordinary expectations of other
29 persons in similar contexts; what are the standards and practices of the business, trade or industry; or other
30 relevant factors. As in the *Restatement*, failure to act constitutes assent if the party that fails to act has reason to
31 know this will create an inference of assent.

32 No particular type of conduct or formality is required. The section recognizes the wide range of
33 behavior and interactions that in modern commerce establish a contractual relationship between parties and the
34 terms of that relationship. However, subsection (c) makes clear that if the assenting party has an opportunity to
35 confirm or deny assent before proceeding to obtain or use the information, the confirmation establishes assent. This
36 sets out one method of meeting the criteria of subsection (a)(2). In many cases, of course, a single indication of
37 assent by an electronic or other act, such as by opening a container or commencing to use information, suffices if it
38 occurs under circumstances giving the actor reason to know that this signifies assent. On the other hand, an act
39 that does not bear a relationship to a contract or a record would fail under the general standard. Similarly, acts
40 that occur in context of a mutual express reservation of the right to defer agreement do not assent to a contract that
41 neither party intended.

42 *Illustration 1:* The registration screen for NY Online prominently states: "Please read the
43 license. It contains important terms about your use and our obligations with respect to the
44 information. Click here to review the License. If you agree to the license, indicate this by
45 clicking the "I agree" button. If you do not agree to the license, click the "I decline" button." The
46 on-screen buttons are clearly identified. The underlined text is a hypertext link which, if selected,
47 promptly displays the license. *A party that indicates "I agree" manifests assent to the license
48 and adopts the terms of the license*

49 *Illustration 2:* The first screen of an on-line stock-quote service requires that the potential
50 licensee enter a name, address and credit card number. After entering the information and
51 striking the "enter" key, the licensee has access to the data and receives a monthly bill. In the
52 center of the screen amid other language in small print, is the statement: "Terms and conditions
53 of service; disclaimers" indicating a hyperlink to the terms. The customer's attention is not called
54 to this sentence nor is the customer asked to react to it. *Even though entering name and
55 identification, coupled with using the service, assents to a contract, there is no assent to the*

1 "terms of service" and disclaimer since there is no act indicating assent to the record containing
2 the terms. A court would determine the contract terms on other grounds, including the default
3 rules of this article and usage of trade.

4 6. *Objective standard.* Manifesting assent requires that, from all the facts known to it, a
5 reasonable person has reason to know that particular conduct will indicate that the actor assents to the record.
6 Actions objectively indicating assent are effective even though the actor may subjectively intend otherwise. This
7 follows traditional contract law doctrine of "objective" assent. This concept is especially important in electronic
8 commerce where many transactions do not involve direct contact between individuals. Information providers and
9 licensees must rely on actions confirming the existence of a contract, and the acceptance of contract terms.
10 Doctrines of mistake, supplemented by Section 2B-118, as well as doctrines invalidating the effects of fraud and
11 duress apply in appropriate cases.

12 7. *Electronic Agents.* Assent may occur through automated systems. In electronic commerce, there
13 is rapidly increasing use of computer programs (described as "bots" or "intelligent agents") programmed to search
14 for (on behalf of a potential purchaser) or make available (on behalf of a potential licensor) particular types of
15 information under set contractual terms or alternatives. Either or both parties may use electronic agents. The
16 reduced transaction costs are significant and the benefits that come from a technology that enables broad
17 comparative shopping and electronic shopping on terms set by the consumer are immense for consumers and for
18 providers of information. For an electronic agent, assent cannot be based on knowledge or reason to know. The
19 issue is whether the circumstances clearly indicate that the operations of the automated system indicate assent.
20 Safeguards exist under Article 2B through unconscionability doctrine and Section 2B-204.

21 8. *Third Party Service Providers.* Assent requires an act by the party to be bound or by its agents.
22 In many Internet situations, a party is able to reach a particular system because of services provided by a third party
23 communications or other service provider. In such cases, the services provider typically does not intend to engage
24 in a contractual relationship with the provider of the information. While the "customer" activity may constitute
25 assent to terms, they do not bind the service provider since the service provider's actions are in the nature of
26 transmissions and making information access available by the user of the service, not assent to a contractual
27 relationship.

28 This article is clear that service providers – providers of online services, network access, or the
29 operation of facilities thereof – do not manifest assent to a contractual relationship from their provision of such
30 services, including but not limited to transmission, routing, providing connections, linking or storage of material at
31 the request or initiation of a person other than the service provider. If, for example, a telecommunications
32 company provided the routing for a user to reach a particular online location, the user of the service would
33 potentially manifest assent to an agreement or record at that location. The service provider who provided the
34 routing to such online location would not.

35 Of course, in some on-line systems, the service party provider has direct contractual relationships
36 with the content providers or may desire access to and use of the information on its own behalf and therefor assent
37 to terms in order to obtain access. In the absence of these circumstances, however, the mere fact that the third-
38 party service provider enables the customer to reach the information site does not constitute assent to the terms at
39 that site.

40 9. *Other Means of Assent.* Manifestation of assent to a record is not the only way in which parties
41 define their bargain. This article does not alter recognition of other methods of agreement. For example, a product
42 description can become part of an agreement without manifestation of assent to a record repeating the description;
43 the product description can define the bargain itself. Thus, a party that markets a database of names of consumer
44 attorneys can rely on the fact that the product need only contain consumer attorneys because this is the basic
45 bargain it is proposing; the provider is not required to seek manifest assent to a record stating that element of the
46 deal. Similarly, the licensee may rely on the fact that the database must pertain to consumer lawyers, not other
47 lawyers. The nature of the product defines the bargain if the party makes the purchase on that basis. If a product
48 is clearly identified on the package or in representations to the licensee as being for consumer use only, the terms
49 are effective without requiring language in a record restating the description or conduct assenting to that record. Of
50 course, if the nature of the product is not obvious and there is no assent to a record defining that nature or other
51 agreement to it, the conditions may not become part of the agreement.

52 In many cases, copyright or other intellectual property notices or restrictions restrict use of a
53 product, regardless of whether there is assent under this section. For example, common practice in video rentals
54 places a notice on screen of the limitations imposed on the customer's use of the video under applicable copyright
55 and criminal law, such as by precluding commercial public performances. The enforceability of such notices does

1 not depend on compliance with this section.

2 10. *Authority to Act.* The person manifesting assent must be one that can bind the party seeking the
3 benefits or being charged with the obligations or restrictions of the agreement. If a party proposing a record desires
4 to bind the other party, it must establish that the person that acted had authority to do so or, at least, that the entity
5 allegedly represented by that person accepted the benefits of the contract or otherwise ratified the individual's
6 actions. Concepts of apparent authority may apply. If the person who manifested assent did not have authority and
7 the conduct was not ratified or otherwise adopted, there may be no license. If this is the case, use of the information
8 may infringe a copyright.

9 There must be a connection between the individual who had the opportunity to review and the
10 one whose acts constitute assent. Of course, a party with authority can delegate that authority to another. Thus, a
11 CEO may implicitly authorize her secretary to agree to a license when the CEO instructs the secretary to sign up
12 for legal materials online or to install a newly acquired program that is subject to a screen license.

13 Questions of this sort arise under agency law as augmented in this article. In appropriate cases,
14 Article 2B rules regarding attribution play a role in resolving whether the ultimate party is bound to the contract
15 terms. Section 2B-116 deals with when, in an electronic environment, a party is bound to records purporting to
16 have come from that party. This article leaves to other law questions of agency law. Section 1-103.

17 11. *Assent to particular terms.* The section distinguishes assent to a record and, if required by other
18 provisions of this article, assent to particular terms. Assent to a record involves conduct, expressions or an
19 authentication with respect to a record as a whole, while assent to a particular term, if required, encompasses acts
20 that relate to that particular term. One act, however, may assent to both the record and the term only if the
21 circumstances, including the language of the record, clearly indicate to the party that doing the act is assent also to
22 the particular term.

23 12. *Proof of Terms.* A party that relies on the terms of linked text or other electronic records must
24 prove the content of the text at the time of the licensee's assent. One way of doing so is to retain records of content
25 at all periods of time or maintain a record of changes and their timing. Issues of proof are matters of evidence law.
26

27 SECTION 2B-112. OPPORTUNITY TO REVIEW; RETURN.

28 (a) A person ~~or electronic agent~~ has an opportunity to review a record or term only if the
29 record or term is made available in a manner that ~~-(1) in the case of a person, -~~ought to call it to
30 the attention of a reasonable person and permit review .

31 ~~_____ (b) ; or (2) in the case of a~~ An electronic agent has an opportunity to review a record or
32 term only if the record or term is made available in manner that ,would enable a reasonably
33 configured electronic agent to react to the record or term.

34 ~~(cb) Except as otherwise provided in subsection (e),~~ if a record or term is available for
35 review only after a person becomes obligated to pay or begins its performance, the person has an
36 opportunity to review only if the person has a right to a return if upon its rejection of the terms
37 of the record. The right to a return may arise by law under Section 2B-208 or 2B-617, by
38 agreement or otherwise. However, (e) ~~A~~ right to a return is not required for an opportunity to
39 review ~~if the record or term:~~

- 1 (1) the record is a proposal for a modification of a contract;
2 (2) the record provides the particulars of performance pursuant to agreement
3 under Section 2B-305; or
4 (3) in a case that does not involve is not a mass-market license, but is governed
5 by Section 2B-207, and the parties at the time of contracting had reason to know that a the record
6 or terms would not be presented at or prior to the initial use or access to the information. -

7 **Definitional Cross References:**

8 "Contract". Section 2B-102. "Electronic agent". Section 2B-102. "License": Section 2B-102. "Record". Section
9 2B-102. "Return": Section 2B-102. "Term". Section 1-201.

10 **Reporter's Notes:**

11 1. *Scope of Section.* This section gives content to the concept of "opportunity to review." An
12 "opportunity to review" is a precondition to manifesting assent to a record. Consistent with general contract law,
13 the concept requires an opportunity to review the record, not that the record actually be read.

14 2. *General Concept.* An opportunity to review in the case of a person requires that the record be
15 made available in a manner that ought to call it to the attention of a reasonable person and permit review. This is
16 met if the person actually knows or has reason to know that the record or term exists and the circumstances permit
17 review. Of course, an opportunity to review a copy of the record or term suffices if the actual record or term is the
18 same as that made available for review.

19 a. *Declining to Use the Opportunity to Review.* An opportunity to review may exist even
20 though the person foregoes or ignores the opportunity. Contract terms presented in an over the counter transaction
21 or made available in a binder as required for some transactions under federal law create an opportunity to review
22 even if the party does not use that opportunity. This is not changed because the party desires to complete the
23 transaction rapidly, or is under external pressure to do so, or because the party has other demands on its attention,
24 unless one party intentionally manipulates the circumstances to induce the other party not to review the record.

25 b. *Permits Review.* How a record is made available for review differs for electronic and
26 paper records. In both settings, however, a record is not available for review if access to it is so time-consuming or
27 cumbersome as to effectively preclude review. It must be presented in such a way as to reasonably permit review.
28 In an electronic system, a record that is promptly accessible through an electronic link ordinarily qualifies. Actions
29 that comply with federal or other applicable consumer laws that require making contract terms available or provide
30 standards for doing so, satisfy this section.

31 3. *Return.* In modern commerce, there are circumstances in which the terms of a record are not
32 available until after there is a commitment to the transaction. This is often true in mail order transactions,
33 software contracts, insurance contracts, airline ticket purchases, and other common transactions. If the record is
34 available only after that commitment, there is no opportunity to review unless the party can return the product (or
35 in the case of a vendor that refuses the other party's terms, recover the product) and receive reimbursement of any
36 payments if it declines the terms of the record. This return right, which does not exist in current law absent
37 agreement, creates important protection for the party asked to assent to terms in these circumstances. In cases
38 governed by Section 2B-208, there is a statutory right to a return.

39 This right is also intended to provide a strong incentive for a provider of information to make the
40 terms of the license available up-front if commercially practicable. Doing so avoids the obligations regarding
41 return stated in this article, both in this section and in Section 2B-208. In addition to that incentive, deferring
42 when license terms are presented may have implications on the application of other doctrines where the choice to
43 do so is not grounded in commercial judgment. For example, the doctrine of unconscionability has a procedural
44 fairness aspect which might be affected by the method of presenting terms where the terms are oppressive.

45 The return right exists only for the first user. Subsequent parties are bound by the first contract.

46 Failure to provide an opportunity or a right to a return in cases of records presented after the
47 initial commitment to the transaction, does not invalidate the overall agreement, but means that the terms of the

1 record have not been assented to by the party to which it was presented. The terms of the agreement must then be
2 discerned by consideration of all the circumstances, including the general expectations of the parties, applicable
3 usage of trade and course of dealing, and the informational property rights, if any, involved in the transaction. In
4 such cases, courts should be careful to avoid unwarranted forfeiture or unjust enrichment in terms of the conditions
5 or terms of the agreement. An agreement whose payment and other agreed terms reflect a right to use solely for
6 consumer purposes can not be transformed into an unlimited right of commercial use by a failure of assent to the
7 terms of a record.

8 4. *Modifications and Layered Contracting.* The return provisions do not apply to or alter law on
9 modification of an agreement or the law regarding the agreed right of a party to specify particulars of performance.
10 The provisions also do not apply in the commercial context of Section 2B-207(a)(2) where parties begin
11 performance in the expectation that a record containing the contract terms will be presented and adopted later.
12

13 [B. Electronic Contracts: Generally]
14

15 SECTION 2B-113. LEGAL RECOGNITION OF ELECTRONIC RECORDS AND
16 AUTHENTICATIONS.

17 _____ (a) A record or authentication may not be denied legal effect solely because it is in
18 electronic form.

19 _____ [(b) This article does not require that a record or an authentication be generated, stored,
20 sent, received, or otherwise processed by electronic means or in electronic form.]

21 _____ (c) In any transaction, a person may establish requirements regarding the type of
22 authentication or record acceptable to it.]

23 **Definitional Cross References:**

24 "Authentication". Section 2B-102. "Electronic". Section 2B-102. "Record." Section 2B-102.

25 **Reporter's Notes:**

26 1. *General Concept.* This section states a fundamental principle of electronic commerce that
27 frames the remaining provisions of this article on electronic commerce. The fact that a message or record is
28 electronic does not alter or reduce its legal impact. Of course, this principle applies only to transaction within
29 Article 2B. It does not apply to payment orders, documents of title, or similar applications of electronic commerce.

30 2. *Relation to Evidence Issues.* This section only states the affirmative principle that the electronic
31 nature of a record does not allow denying legal validity to it. This does not address the difficulties of proof that
32 may exist, or the resolution of questions about to whom the record or authentication can be attributed.
33

34 SECTION 2B-114. COMMERCIAL REASONABLENESS OF ATTRIBUTION

35 **PROCEDURE.** The commercial reasonableness of an attribution procedure is determined by the
36 court. In making this determination, the following rules apply:

37 (1) An attribution procedure established by statute or regulation is commercially
38 reasonable for transactions within the coverage of the statute or regulation.

1 (2) Except as otherwise provided in paragraph (1), commercial reasonableness is
2 determined in light of the purposes of the procedure and the commercial circumstances at the time
3 the parties agree to or adopt the procedure.

4 (3) A commercially reasonable attribution procedure may use any security device
5 or method that is reasonable under the circumstances.

6 **Uniform Law Source:** Article 4A-201; 202.

7 **Definitional Cross References:**

8 "Attribution procedure": Section 2B-102. "Court": Section 2B-102.

9 **Reporter's Note:**

10 1. *Scope of the Section.* This section provides standards for determining if an attribution procedure
11 is commercially reasonable.

12 2. *Effect of a Commercially Reasonable Procedure.* In this article, an attribution procedure receives
13 enhanced legal effect only if it is commercially reasonable. Conforming to a commercially reasonable attribution
14 procedure for authentication results in authentication as a matter of law. Section 2B-119. Complying with a
15 commercially reasonable procedure for identifying a party or detecting errors or changes creates a rebuttable
16 presumption of identity and the absence of errors or changes in the record. Sections 2B-116 ; 2B-117. On the other
17 hand, failure to use a commercially reasonable attribution procedure does not preclude a finding that authentication
18 occurred or of the identity and integrity of the sender and the record itself. It leaves the parties with general
19 questions of proof.

20 3. *Nature of an Attribution Procedure.* This article does not dictate what constitutes an attribution
21 procedure. Evolving technology and commercial practice make it impractical to predict future developments and
22 unwise to preclude developments by a narrow statutory mandate. This article relies primarily on the parties to
23 select an appropriate procedure.

24 In most cases, an attribution procedure is established by agreement or otherwise adopted by both
25 parties. A procedure of which one party is not aware does not qualify. On the other hand, parties dealing for the
26 first time may adopt a procedure for authentication of messages. These requirements assure an important element
27 of assent as a predicate for the creation of procedures that may affect substantive rights.

28 In some cases, statutes or regulations define a particular methodology as an appropriate
29 procedure. These laws, such as digital signature statutes, establish by law a procedure that complies with the
30 concept of an attribution procedure for purposes of this article. Under subsection (1), procedures established by
31 statute or regulation are per se commercially reasonable within the scope of their coverage.

32 4. *Commercially Reasonable.* The general requirement of commercial reasonableness is that the
33 procedure be a commercially reasonable method of identifying the party as compared to others, a commercially
34 reasonable method of detecting or preventing changes, or a commercially reasonable method of achieving any
35 other purpose relevant to this article and to which the procedure is addressed. This does not require state of the art
36 procedures. Rather, the requirement that a procedure be commercially reasonable in order to attain enhanced legal
37 recognition provides an incentive that encourages good practices and allows a court to provide a direct buffer
38 against over-reaching. It protects parties who lack knowledge of technology and use procedures established by
39 others because if the procedure is found to be not commercially reasonable, it creates no presumption of the party's
40 identity.

41 What is a commercially reasonable procedure takes into account the choices of the parties and the
42 cost relative to value of the transactions. How one gauges commercial reasonableness depends on a variety of
43 factors, including the agreement, the choices of the parties, the then current technology, the types of transactions
44 affected by the procedure, sophistication of the parties, volume of similar transactions engaged in, availability of
45 feasible alternatives, cost and difficulty of utilizing alternative procedures, and procedures in general use for
46 similar types of transactions. The concept is similar to that in Section 4A-202(c). The quality of the procedure
47 may reasonably be tailored to the particular transaction and the degree of risk involved. Additionally, if a
48 procedure results from a fully negotiated agreement of the parties, it should receive deference in terms of its

1 reasonableness applicable to their particular situations. This flows from the principle of assumed risk and that the
2 parties' agreement should ordinarily be enforced. The same principle may apply if the two parties, aware of the
3 risks of a particular procedure, nevertheless agree to use the procedure for a particular transaction. In effect, the
4 parties here have concluded that it is commercially reasonable in their context to accept the risks.
5

6 **[SECTION 2B-115. EFFECT OF REQUIRING COMMERCIALY**

7 **UNREASONABLE ATTRIBUTION PROCEDURE. PROPOSED FOR DELETION**

8 (a) Subject to subsection (b), between parties to an attribution procedure, a party that
9 conditions a transaction on ~~required~~-use of a commercially unreasonable attribution procedure is
10 liable for losses in the transaction for which the procedure was required caused by reasonable
11 reliance on that procedure.

12 (b) The recovery of a party under subsection (a) is limited to losses in the nature of
13 reliance or restitution and does not include:

- 14 (1) loss of expected benefit;
15 (2) consequential damages;
16 (3) losses that could have been prevented by the exercise of reasonable care by the
17 aggrieved party; or
18 (4) a loss the risk of which was assumed by the aggrieved party.

19 (c) For purposes of subsection (a), a person does not require a commercially
20 unreasonable procedure if the person makes available a commercially reasonable alternative.]

21 **Definitional Cross References:**

22 "Attribution procedure": Section 2B-102. "Consequential damages": Section 2B-102. "Electronic": Section 2B-
23 102.

24 **Reporter's Notes:**

25 1. *General Policy and Scope.* This section deals with cases where one party (licensor or licensee)
26 requires the other to use an attribution procedure that is not commercially reasonable and use of that procedure
27 causes a loss in a transaction between the parties either because of undetected errors or because of third party fraud.
28 The section deals only with cases in which a party does in fact require use of the commercially unreasonable
29 procedure. This does not create a principle that loss is always placed on the party whose procedure is not
30 commercially reasonable. It deals with the more limited context where one party demands use of the commercially
31 unreasonable procedure and prohibits alternatives.

32 The rule in this section is subject to Sections 2B-116 and 2B-117. Those sections establish
33 presumptions about electronic records subject to commercially reasonable procedures. A commercially
34 unreasonable procedure does not create those presumptions, leaving the parties to general proof. In addition, if the
35 case is within this section, it may alter loss allocation.

1 2. *Imposed as a Condition.* The loss allocation in this section requires two elements. The first is
2 that the commercially unreasonable procedure be required as a precondition to entering the transaction. This
3 means more than that the procedure is merely made available. The party must insist on the particular procedure
4 and be in a position where no alternatives are available or allowed. A procedure negotiated or jointly selected by
5 the parties, selected by one from among alternatives that include a commercially reasonable option, or a mutually
6 designed procedure, does not fall within this section. Responsibility for loss in such cases and in cases where the
7 procedure allows a fraud in an unrelated transaction lies outside this article.

8 3. *Reasonable Reliance in a Covered Transaction.* The second element of allocating loss under
9 this section is that the loss result from reasonable reliance on the required procedure in a transaction to which the
10 requirement applies. The reliance must be reasonable. Thus, for example, a party that relies on an ordinary E-
11 mail order for a multi-million dollar order may not be acting in reasonable reliance given the size of the
12 transaction. What constitutes reasonable reliance depends on the circumstances, including consideration of the
13 nature of the procedure, the size of the transaction involved, and the existence or non-existence of relevant
14 safeguards or alternatives.

15 The loss must occur in a transaction to which the requirement applies. This is a contract statute
16 that does not attempt to allocate all losses caused by fraudulent behavior. This section allocates loss within affected
17 transactions. For example, if the unreasonable attribution procedure requires use of a bank account number and a
18 third party invades the system and misappropriates the number, the party requiring use of such a number is not
19 responsible for losses caused in unrelated transactions because the thief obtained the number. This section does not
20 address the difficult problem of liability for misuse of important identifiers fraudulently to obtain goods and
21 services from other vendors. The answers to those issues lie in tort law, criminal law, and regulation

22 4. *Party Responsible.* The person that required the procedure is responsible for the loss. In some
23 cases the person imposing the requirement is the licensor and in other cases the licensee. The rule applies in either
24 case. The section does not necessarily create an affirmative right of recovery. In some cases, it merely bars the
25 responsible party from recovering from the other person. Thus, pursuant to a commercially unreasonable
26 attribution procedure a licensor might deliver information to a third party who used the inadequacies of the
27 procedure to impersonate the named licensee. If the licensor had required the procedure, this section allows the
28 licensee to resist any claim by the licensor to charge the licensee for the contract price. It is also likely in such case
29 that, not being entitled to the presumption stated in Section 2B-116, the licensor will be unable to show that the
30 order is attributable to the licensee. On the other hand, if the licensee had required the procedure, the licensor may
31 recover against the licensee for the losses in the nature of reliance.

32 5. *Type of Loss.* The loss must come from use of the procedure. Thus, if an attribution procedure is
33 unreasonable, but the party to whom it attributes a message did actually engage in the transaction and suffered loss
34 due to a breach of contract, this section does not apply. The losses addressed here are from misattribution of who
35 sent a message or from tampering with the content, not losses caused by ordinary breach of contract.

36 The losses are limited to reliance and restitution recovery. This restriction is spelled out in
37 subsection (b). Subsection (b)(3) follows the general principle that a party cannot recover for losses that could have
38 been avoided. This mitigation principle corresponds to general common law and the restatement of the concept in
39 Section 2B-707. Subsection (b)(4) recognizes the concept of assumption of risk. Application of that general equity
40 concept in the circumstances covered in this section, of course, must account for the fact that one party exercised
41 strong leverage to impose an unreasonable procedure on the other. An assumption of risk cannot be found merely
42 in acquiescing to this requirement.

43 6. *Illustrations.* The following suggest some applications of this section.

44 a. *False Identity Cases: No Contract.* Often, if a loss is suffered because a third party
45 fraudulently used an attribution identifier to order information, this section produces results that are parallel to the
46 results that could be inferred under other attribution rules of this article.

47 **Illustration 1.** LR (vendor) required and LE agreed to a procedure for identifying LE in placing orders
48 with LR. Thief, purporting to be LE, obtains a \$10,000 electronic encyclopedia from LR. LR seeks the
49 license fee from LE. Under the general attribution sections, if the procedure is not commercially
50 reasonable, there is no presumption that the sender was LE. Since LE was not the sender, it has no
51 liability. The required attribution procedure caused a loss, but LR is responsible for that loss. It cannot
52 shift that loss to LE.

53 In some false identity cases, the party demanding the use of the attribution procedure may be responsible for
54 reliance losses in transactions to which the requirement applied.

55 **Illustration 2.** LE (purchaser) requires LR to use a procedure under which LE identifies itself when

1 placing orders with LR. Thief uses the procedure fraudulently to obtain a \$10,000 software system from
2 LR posing as LE. Since LE required use of the procedure and it was commercially unreasonable, the loss
3 suffered may be recovered from LE. The amount of loss is measured by reliance, not lost profit. The
4 recovery is the cost (not license price) of the software shipped plus related expenses.

5 *b. True Contract: Errors in Performance.* If an actual contract exists and the error or fraud
6 relates to performance, contract remedies will often provide the primary recovery and, under the principle that
7 precludes double recovery, the reliance loss allocation in this section does not create affirmative recovery.

8 **Illustration 3.** LR (licensor) and LE (licensee) agree to a \$10,000 commercial license. LR requires LE
9 to agree to a procedure for instructions as to where to transmit the software. LE pays the license fee. A
10 third party causes misdirection of the copy. LE demands its software. LR bears responsibility for reliance
11 or restitution loss. LE can recover the fee or enforce the unperformed contract.

12 **Illustration 4.** In Illustration 3, assume that LE did direct transmission of the software, but now denies
13 that it did so. If the procedure were reasonable, LR would have the advantage of a presumption of
14 attribution of the message. Since it was not, LR must prove that LE sent the message. If it can do so, it
15 can enforce the contract. LE suffered no loss due to the attribution procedure.

16 *c. Errors in the Offer and Acceptance.* Problems of garbled or otherwise mistaken offers and
17 acceptances are of long-standing in commercial practice. This section allocates loss based on the reasonableness of
18 the procedure and independent of arcane questions about what terms were accepted and when.

19 **Illustration 5.** LR (vendor) requires that LE use an unreasonable procedure for orders. LE agrees to the
20 procedure. It places an order for ten software widgets. Because the procedure is flawed, the message
21 arrives requesting 100. LR ships on that basis. LE desires to return the ninety excess widgets and not
22 pay. One could argue that no contract exists because of mistake. Alternatively, a contract might be formed
23 on the offer as sent or as received. Case law support exists for each result. This section focuses on
24 reliance loss. Either LE or LR could be said to suffer reliance loss. Since LR required the procedure, it
25 bears responsibility for the loss and cannot demand the price for the ninety widgets unless LE decides to
26 retain them.

27
28 **SECTION 2B-116. DETERMINING TO WHICH PERSON AN ELECTRONIC**

29 **AUTHENTICATION, MESSAGE, RECORD, OR PERFORMANCE IS ATTRIBUTED;**

30 **RELIANCE LOSSES. [see proposed revision]**

31 (a) An electronic authentication, message, record, or performance is attributed to a
32 person if:

33 (1) it was in fact the act of that person or the person's electronic agent; or

34 (2) ~~subject to subsection (b),~~ the person receiving it in accordance with a
35 commercially reasonable attribution procedure for identifying a person, reasonably concluded that
36 it was the action of the other person or the person's electronic agent.

37 (b) Attribution under subsection (a) (2) has the effect provided by the statute, regulation,
38 or agreement establishing the attribution procedure. If the statute, regulation, or agreement do es
39 not specify a different effect, attribution under subsection (a)(2) creates a presumption that the

1 authentication, message, record, or performance was that of the person to which it is attributed -
2 ~~[*proposed alternative: places the burden of establishing on the person to which the~~
3 ~~authentication, record or performance was attributed to show that it was not responsible for the~~
4 ~~authentication, message, record, or performance].~~

5 (c) If subsection (b) applies and the person to which the authentication, message, record,
6 or performance was originally attributed is found to be not responsible in fact, that person is
7 nevertheless liable for losses in the nature of reliance-the cost of performance of the other party if
8 the losses occur because:

9 (1) the person found not otherwise responsible failed to exercise reasonable care;

10 (2) the other party reasonably relied on the belief that the person found not
11 otherwise responsible was the source of the electronic authentication, message, record, or
12 performance; and

13 (3) the use of the attribution procedure creating access material, computer
14 programs, or the like created the appearance that it came from the party person found not
15 otherwise responsible and resulted from acts of a third person that obtained materials enabling it
16 to use the procedure that obtained them from a source under the control of the that party person
17 found not otherwise responsible.

18 **Uniform Law Source:** 4A-202; 4A-205; UNCITRAL Model Law.

19 **Definitional Cross References.**

20 "Access materials": Section 2B-102. "Attribution procedure": Section 2B-102. "Computer program": Section 2B-
21 102. "Electronic": Section 2B-102. "Electronic agent": Section 2B-102. "Electronic message": Section 2B-102.
22 "Good faith": Section 2B-102. "Party": Section 1-201. "Person": Section 1-201. "Presumption": Section 1-201.
23 "Record": Section 2B-102.

24 **Reporter's Notes:**

25 1. *Scope of the Section.* This section deals with when an authentication, message, record or
26 performance is attributed to a particular person. Attribution to a person means that the authentication, message,
27 record, or performance is treated in law as having come from that person. The section enables electronic
28 commerce in an open environment, while stating reasonable standards to allocate risk. The section does not apply
29 to funds transfers, bank accounts, credit card liability, or other subject matter outside Article 2B. It deals with an
30 issue independent of whether the record has been authenticated. Authentication requires an act and an appropriate
31 intent. Attribution deals with determining to whom the act is charged.

32 2. *Act of the Person or Electronic Agent.* Subsection (a)(1) makes a person responsible if it or its

1 agent actually created the authentication, message, or record, or provided the performance. Common law agency
2 rules govern for human agents. In addition, however, a person is responsible for the actions of its electronic agent.
3 Section 2B-102; 2B-116(a)(1). Having decided to use an automated system, the person is responsible for its
4 operations. The rules of subsection (a)(1) parallel the UNCITRAL Model Law. Article 13.

5 3. *Use of Attribution Procedure.* In many cases in electronic commerce, proof of actual involvement
6 is not possible. Subsection (a)(2) makes an authentication, message, record, or performance attributable to a
7 person if there existed a commercially reasonable "attribution procedure" and the other party used the procedure,
8 reasonably concluding that the message came from the other person. "Attribution procedure" is a defined term,
9 referring to a procedure agreed to or adopted by the parties, or created by law, for the particular purpose of
10 attribution of authentication, messages, records, or performances.

11 This procedure yields the result in subsection (a)(2) only if the attribution procedure is
12 commercially reasonable. Section 2B-114.

13 Unlike attribution to a person under subsection (a)(1), however, the effect of attribution under
14 (a)(2) is determined under subsection (b) which, in the absence of other agreement, limits the effect to a [rebuttable
15 presumption] [shift of the burden of proof]. While giving legal relevance to a commercially reasonable attribution
16 procedure creates benefits for electronic commerce, the uncertainties of modern commerce indicate that, as a
17 default rule, it is inappropriate to adopt an absolute rule that the person identified by the procedure is attributed
18 with its results for all purposes.

19 Subsection (b) recognizes that fact. It provides that unless otherwise provided by agreement or by
20 other law or regulation, attribution through a commercially reasonable procedure creates a [rebuttable
21 presumption] [shift of the burden of proof] of the party's responsibility. Section 1-201(3!). How this might be
22 rebutted in litigation, of course, depends on the circumstances. No general standard can be stated. However, since
23 this is a default rule, if the parties agree that following the procedure will have a different effect, that agreement
24 should be enforced. Similarly, if another statute or regulation provides for a different result, that law controls.

25 4. *Reliance Losses.* Subsection (c) deals with when the presumption in (b) is rebutted. If a
26 commercially reasonable procedure was used, but a third party actually sent the message, the relying party may
27 nevertheless recover reliance loss if it proves that the loss was caused by the other party's negligence with reference
28 to the attribution procedure and its use. What constitutes a lack of reasonable care depends on the circumstances,
29 including the nature of the risks involved and the sophistication of the party. A consumer with no experience in
30 attribution methodology would be expected to take fewer precautions in the relatively small transactions in which
31 the consumer engages, than would a sophisticated company using the attribution procedure in reference to high
32 value, large volume, or sensitive information transactions. In either case, the burden of proving a lack of
33 reasonable care by a party rests on the person asserting the right to recover under this subsection.

34 The loss allocation principle recognizes a form of protected reliance where there was reliance on
35 an agreed or otherwise established and commercially reasonable procedure. Since this is reliance-based liability, if
36 the message, performance or context indicates that the indicated source is incorrect or gives reason to doubt the
37 source, reliance may not be protected. This form of loss allocation adopts an intermediate position among the
38 other potentially available loss allocation theories. Unlike in credit card and funds transfer systems, one cannot
39 predict the relative nature of the sending and receiving parties, their economic strength, or technological
40 sophistication. Individuals with limited resources are as likely to be on either side of a transaction in electronic
41 commerce as are large corporations. Because of this, the rule creating a dollar cap for consumer risk for credit
42 cards and funds transfers is not viable in this open system, heterogeneous environment. This context requires a
43 more general structure because the problems will not routinely entail consumer protection or a licensor with better
44 ability to spread loss.

46 SECTION 2B-117. ATTRIBUTION PROCEDURE FOR DETECTION OF

47 CHANGES AND ERRORS: EFFECT OF USE.

48 (a) In this section, "electronic record" means an electronic authentication, message,
49 record, or performance.

SECTION 2B-116. TO WHICH PERSON AN ELECTRONIC AUTHENTICATION, MESSAGE, RECORD, OR PERFORMANCE IS ATTRIBUTED; RELIANCE LOSSES.

(a) In this section, "electronic record" means an electronic authentication, message, record, or performance.

(b) An electronic record is attributed to a person if it was the act of that person or its electronic agent, or if the person is otherwise bound by it under the law of agency. The party relying on attribution of an electronic record to another person has the burden of establishing attribution.

(c) If an attribution procedure exists between the parties with respect to the electronic record, the following rules apply:

(1) The effect of compliance with an attribution procedure created by other law or regulation is determined by that law or regulation.

(2) In all other cases, if the parties agree to, or otherwise adopt an attribution procedure to verify the person from which an electronic record comes, the record is attributable to the person identified by the procedure, if the party relying on that attribution satisfies the burden of establishing that:

(i) the attribution procedure is commercially reasonable;

(ii) the party accepted or relied on the electronic record in good faith and in compliance with the attribution procedure and any additional agreement with or separate instructions of the other party; and

(iii) the attribution procedure indicated that the electronic record was that of the person to which attribution is sought.

(3) If the electronic record is not binding on a person under subsection (b) but is binding under subsection (c), that person nevertheless avoids attribution under subsection (c) for the electronic record if the person satisfies the burden of establishing that the electronic record was not caused directly or indirectly by a person:

(i) entrusted at any time with the right or duty to act for the person with respect to such electronic records or attribution procedure;

(ii) who obtained access to transmitting facilities of the person; or

(iii) who obtained, from a source controlled by the person, information facilitating breach of the attribution procedure.

(d) The provisions of subsection (c) may not be varied by agreement in a consumer transaction except in a manner that provides greater protection to the consumer. In all other cases, the effect of an attribution procedure may be determined by agreement if the attribution procedure is commercially reasonable.

(e) If an electronic record is not binding on a person under subsection (b) and is not effective under subsection (c), the person identified as the source of the electronic record is nevertheless liable for losses of the other party measured by the cost of that party's performance in reliance if the loss occurs because:

(1) the person identified as the source failed to exercise reasonable care;

(2) the other party exercised reasonable care and reasonably relied on the belief that the person identified was the source of the electronic record because access materials, computer programs or the like created the appearance that it came from that person; and

(3) the appearance on which the party relied resulted from acts of a third person that obtained the capability to create that appearance from a source under the control of the person identified as the source of the record.

1 Illustration 2: Same facts as in Illustration 1, except that Consumer did order 110 copies and merely
2 changed his mind. The conditions for application of this section are not met.
3 Illustration 3: Same as in Illustration 1, but Jones' system before shipping sends a confirmation, asking
4 Consumer to confirm an order of 110 copies. Consumer confirms. There was no "electronic error" since
5 the procedure reasonably allowed for correction of the error.
6 4. *Non-consumer Transactions.* This section does not alter common law in transactions that do not
7 involve consumers. The diversity of commercial transactions make a simple rule inappropriate because of the far
8 different patterns of risk and the greater ability of commercial parties to develop tailored solutions to this problem.
9 A court addressing electronic errors in these other contexts should apply general common law, including an
10 inquiry about whether any contract was actually formed. The existence of this remedy in this section for a
11 consumer does not indicate that other remedies under the law of mistake are precluded.
12

13 **SECTION 2B-119. PROOF OF AUTHENTICATION; OPERATIONS OF**
14 **ELECTRONIC AGENT-OPERATIONS.**

15 (a) ~~A person that uses Operations of an electronic agent for are the authentication,~~
16 ~~manifestation of assent, or performance of a person if the person used the electronic agent for~~
17 ~~such purpose. A party is bound by the operations of its the electronic agent, even if no individual~~
18 ~~was aware of or reviewed the agent's operations actions or their results.~~

19 (b) Subject to Section 2B-116, compliance with a commercially reasonable attribution
20 procedure for authenticating a record authenticates the record as a matter of law. ~~Otherwise,~~
21 ~~a~~Authentication may be proven in any manner, including by showing that a party made use of
22 information or access ~~which that~~ could only have been available if it engaged in conduct or
23 operations that authenticated the record or term.

24 (c) Unless the circumstances indicate otherwise, authentication is deemed to have been
25 done with the intent to ~~establish:~~

26 (1) establish a person's identity;

27 (2) establish that person's adoption or acceptance of the authenticated record,
28 term, or contract; and

29 (3) confirm the content the integrity of the record or term as of the time of the
30 authentication.

31 **Definitional Cross References.**

1 "Attribution procedure": Section 2B-102. "Authenticate:" Section 2B-102. "Contract". Section 1-201. "Electronic
2 agent". Section 2B-102. "Information". Section 2B-102. "Informational Rights": Section 2B-102. "Record":
3 Section 2B-102.

4 **Reporter's Notes:**

5 1. *Scope of the Section.* This section deals with authentication (subsections (b) and (c)) and
6 electronic agent operations (subsection a).

7 2. *Electronic Agents.* Subsection (a) states the general principle that operations of an electronic
8 agent bind the party that used the agent for that purpose. Section 2B-116(a)(1) states the analogous principle in
9 reference to attribution rules. Electronic agents are automated systems that respond to or originate messages or
10 performances. They enable important savings in transactional costs in electronic commerce and this article
11 provides legal support sustaining their use in commerce.

12 The concept embodies principles like those under ordinary agency law that the electronic agent
13 function within the scope of its intended purpose. In reference to human agents, this concept is often referred to in
14 terms of whether the human agent acted within the scope of its actual or apparent authority. Here, since the
15 concept deals with automation and the focus is more accurately placed on whether the agent was used for the
16 relevant purpose. Cases of fraud, manipulation and the like are discussed in Section 2B-204.

17 3. *Proof of Authentication.* In dealing with an authentication, two separable issues are (1) whether
18 the symbol or process was executed and intended as an authentication, and (2) to whom the authentication is
19 attributed. Under Subsection (b), compliance with an a commercially reasonable procedure for authentication
20 removes questions about whether an authentication was intended or occurred. It does not resolve attribution issues
21 under Section 2B-116. Subsection (b) deals with whether there was an authentication, while Section 2B-116
22 identifies who is responsible. Ordinarily, the two issues are resolved in a single step. On whether an attribution
23 procedure is commercially reasonable, see Section 2B-114.

24 Proof of authentication can occur in any manner. One of the most important involves showing
25 that a process existed that required an authentication in order to proceed in an automated system. To satisfy the
26 concept of authentication, however, it is not sufficient merely to show that some act was required to proceed. The
27 act must constitute an authentication (e.g., execution of a relevant symbol).

28 4. *Effect of Authentication.* As with common law signatures, an authentication can be used with
29 several different intended effects. Section 2B-102(1). In the absence of contrary indications present in the
30 circumstances, the presumed intent encompasses all such effects. The contrary indications would be present if the
31 attribution procedure was used solely for a single effect. Intention under this section must, as in other contexts, be
32 gauged by objective criteria.

33
34 **SECTION 2B-120. ELECTRONIC MESSAGES: TIMING OF CONTRACT;**

35 **EFFECTIVENESS OF MESSAGE; ACKNOWLEDGING MESSAGES.**

36 (a) Except as otherwise provided in subsection (b) and (c), an electronic record message
37 is effective when received even if no individual is aware of its receipt.

38 (b) ~~If in determining when a contract is formed, if an offer in an electronic message~~
39 evokes an electronic message in response, a contract is formed:

40 (1) when an acceptance is received; or

41 (2) if the response consists of furnishing or giving access to information, when the
42 information or notice of access is received or use is enabled, unless the originating message
43 required acceptance in a different manner.

1 contract. The first arises if one party agreed to the terms of the other. In that case, the terms of the accepted
2 record control subject to the limitations in Section 2B-207 and 2B-208. Agreement can be manifested in any
3 manner except that it cannot be found solely in the "acceptance" that contains a materially varying term. The
4 second is where the exchanged offer and acceptance materially conflict, but a contract is formed solely by conduct.
5 This places the relationship under Section 2B-209 which instructs a court to consider the entire context in
6 determining the terms of the contract.

7 *b. Varying Terms: Non-Material Variance.* If an offer and acceptance do not materially
8 vary, they form a contract. The terms of the contract are the terms of the offer. Section 2B-209 does not apply
9 because the contract is formed by offer and acceptance.

10 Subsection [2B-203A(a)(2)] allows for inclusion of non-material additional terms from the
11 acceptance unless the offeror timely objects to those terms. This rule comes from existing Article 2 and follows the
12 basic principle that the offeror controls the terms of its offer. If the acceptance gives conflicting treatment of a
13 subject contained in the offer and the difference is not material, the offer controls. Standards of materiality in this
14 context include whether the additional terms involve unreasonable surprise when measured against the commercial
15 context, including usage of trade and course of dealing, or whether they so change the effect of the other terms of
16 the offer and acceptance such as to significantly alter the bargain reached. In either context, the terms are not part
17 of the agreement.

18 4. *Conditional Offers and Acceptances.* A person has a right to state and insist on preconditions for
19 acceptance of its offer. Subsection [2B-203B(a)] recognizes that principle. In commercial practice, the most
20 common conditional offer or acceptance limits its effect on the other party's adherence to all of its terms. No
21 principle in contract law precludes a party from enforcing such conditions. However, conditional language in
22 standard terms of a standard form creates special problems in "battle of forms" transactions where either or both
23 parties make an acceptance or offer expressly conditional on its specific terms, but perform irrespective of
24 acceptance of the condition. Subsection [2B-203B(b)] treats this as a question involving the effectiveness of the
25 conditional language. In a standard form, the party desiring enforcement of its conditional language is entitled to
26 that result only if its conduct corresponds to the condition. Conduct corresponds to the condition if the party
27 insisting on the condition precludes further performance unless the other party assents to its terms.

28 *Illustration 1.* Licensee sends a standard order form indicating that its order is conditional on
29 the Licensor's assent to the terms on the Licensee's form. Licensor ships with an invoice
30 conditioning the contract on assent to its terms. Purchaser accepts shipment. Here, neither party
31 acted consistent with the language of condition. A contract exists based on conduct. The terms
32 are governed by 2B-209.

33 *Illustration 2.* In Illustration 1, assume that Licensor refuses to ship, but informs Purchaser that
34 agreement to the Licensor's terms is a condition of shipment. It does not ship until Purchaser
35 agrees to terms. Until that occurs, there is no contract. If it occurs, the contract exists based on
36 the form agreed to.

37 *Illustration 3.* In Illustration 1, assume Licensor ships pursuant to a "conditional" form, but
38 when the shipment arrives, Purchaser refuses it. In a telephone conversation, Licensor agrees to
39 Purchaser's terms. Until that agreement, there is no contract; Purchaser acted in a manner
40 consistent with its conditional language. When agreement occurred, that agreement sets out
41 terms of the contract.

42 SECTION 2B-204. OFFER AND ACCEPTANCE; ELECTRONIC AGENTS. ~~In an~~

43 ~~automated transaction, the following rules apply:~~

44 ~~(a) A contract may be formed by the interaction of electronic agents. A contract is~~
45 ~~formed if the interaction results in the electronic agents² engaging in operations that confirm or~~
46 ~~indicate the existence of a contract a contract is formed unless the operations resulted from fraud~~
47 ~~or electronic mistake, fraud or the like.~~

1 ~~(b2)~~ A contract may be formed by the interaction of an electronic agent and an
2 individual. A contract is formed if the individual takes actions that it is free to refuse to take or
3 makes a statement that the individual has reason to know will:

4 (A) cause the electronic agent to perform, provide benefits, permit the use
5 or access that is the subject of the contract, or instruct a person or an electronic agent to do so; or

6 (B) indicate acceptance or an offer, regardless of other expressions or
7 actions by the individual to which the electronic agent cannot react.

8 ~~(c3)~~ The terms of a contract formed under subsection paragraph (b2) are
9 determined under Section 2B-207 or 2B-208, as applicable, but do not include terms provided by
10 the individual if it had reason to know that the electronic agent could not react to the terms as
11 provided.

12 **Definitional Cross References**

13 "Agreement": Section 1-201. "Automated transaction": Section 2B-102. "Contract": Section 1-201. "Electronic
14 agent": Section 2B-102. "Information": Section 2B-102. "Informational Rights": Section 2B-102. "Party":
15 Section 1-201. "Reason to know": Section 2B-102. "Term": Section 1-201.

16 **Reporter's Notes:**

17 1. *Scope of the Section.* This section deals with two settings: 1) an interaction between two
18 electronic agents and 2) an interaction between a human and an electronic agent. Both interactions can create a
19 contract. In each case, however, contract formation rules take into account the fact that an electronic agent cannot
20 react to terms outside the scope of its programming and, at least in most cases, that the party using the agent does
21 not, by virtue of that use, accept the possibility of agreeing to other terms.

22 Modern systems enable the use of electronic contracting agents by consumers and other licensees
23 as well as by licensors. Intelligent agents that search for information or other products within predefined purchase
24 terms creates a significant new form of comparison shopping that is supported by the rules here.

25 2. *Interaction of Electronic Agents.* An interaction of two electronic agents can create a contract
26 that binds the parties that used the agents to achieve that result if the operations of the electronic devices indicate
27 that a contract exists. This rule follows the basic principle that conduct can create a contract. That would occur,
28 for example, if the interaction results in information being sent by one and accepted in the system of the other. It
29 might also occur if the agents' operations result in recording within their respective systems that a contract has
30 been created. The terms of the contract that result from this interaction are determined under Section 2B-207 or
31 2B-208 as applicable.

32 3. *Electronic Mistake and Fraud.* Assent from the operations of the two electronic agents does not
33 arise if the operations are induced by mistake, fraud or the like. Formation of a contract does not occur if one party
34 or its electronic agent manipulates the programming or response of the other electronic agent in a manner akin to
35 fraud. This, in essence, vitiates the inference of assent which would occur through the normal operations of the
36 agent. Similarly, the inference is vitiated if because of aberrant programming or through an unexpected interaction
37 of the two agents, operations indicating the existence of a contract occur in circumstances that are not within the
38 reasonable contemplation of the person using either electronic agent. In such cases, the circumstances are
39 analogous to mutual mistake. In some cases, especially if the electronic agent is supplied by one party to the
40 purported agreement, it would be appropriate for a court to avoid results that are clearly outside the reasonable

1 expectations of the other party. The concept here is more akin to the law of unilateral mistakes except that it
2 places the risk on the party that supplied the agent for and required its use in a particular transaction.

3 Subsection (1) makes clear that restrictions analogous to common law concepts of fraud and
4 mistake are appropriate to prevent abuse or clearly unexpected results. Courts applying these concepts may refer to
5 cases involving mistake or fraud doctrine even though, in the case of electronic agents, the electronic agent cannot
6 actually be said to have been misled or mistaken. Of course, parties may agree to reallocate the risk of mistake or
7 fraud in a separately formed agreement, such as an EDI agreement setting out a procedure for subsequent
8 electronic ordering.

9 This section does not address the liability of a supplier of the electronic agent whose
10 programming or lack of security causes loss. If such supply contract is within this article, allocation of liability is
11 handled as in any other contractual relationship. Liability under other law is not dealt with in this article.

12 4. *Interaction of Human and Electronic Agent.* Contracts may be formed by an interaction of a
13 human and an electronic agent. The electronic agent's ability to bind the party using it derives from the choice of
14 that party to so use an automated system. A contract is formed if the human makes statements or engages in
15 conduct that indicate assent. Consistent with the concept of manifesting assent, assent may be indicated by taking
16 actions with reason to know that they indicate agreement. Here, that occurs if the acts or statements will cause the
17 electronic agent to deliver benefits or permit the access that is the subject matter of the contract. Statements by the
18 individual purporting to alter or vitiate agreement to which the electronic agent cannot react are ineffective.

19 *Illustration 1.* Tootie is an electronic system for placing orders with Home Shop. If a customer dials the
20 number, a voice instructs the customer to indicate a credit card number, the item number, the quantity, the
21 customer's location, and other data. Customer, after entering the data, verbally states that he will only
22 accept the information if there is a 120 day "no questions" return right. Otherwise: "I don't want the
23 damn things." Customer has reason to know that the electronic system cannot react to the verbal
24 condition. Tootie automatically orders shipment.

25 There is a contract. The verbal condition is ineffective. Stating conditions beyond the capability of the agent to
26 react does not vitiate agreement when there is reason to know that they cannot be dealt with by the electronic
27 system. Agreement is indicated by the steps that initiate shipment.

28 *Illustration 2.* User dials the ATT information system. A computerized voice states: "If you would like
29 us to dial your number, press "1", there will be an additional charge of \$1.00. If you would like to dial
30 yourself, press "2". User states into the phone that he will not pay the \$1.00 additional charge, but will
31 pay .50. Having stated his conditions, User strikes "1." The ATT computer dials the number, having
32 located it in the database.

33 User's "counter offer" is ineffective. The charge includes the additional \$1.00.

34 SECTION 2B-205. FIRM OFFERS. 35

36 (a) An offer by a merchant to enter into a contract which is made in an authenticated
37 record that by its terms gives assurance that the offer will be held open is not revocable for lack of
38 consideration during the time stated or, if a time is not stated, the offer is irrevocable for a
39 reasonable time not exceeding 90 days.

40 (b) An offer by a merchant containing a term providing assurance that the offer will be
41 held open which term is contained in a standard form supplied by the party receiving the offer and
42 used by the party making the offer is ineffective unless the party making the offer authenticates
43 the term.

1 Subsection [2B-206A(a)(3)] acknowledges the common practice of establishing a method for
2 receiving and reacting to submissions as a means of controlling risk and giving guidance. Under this subsection,
3 these procedures have impact in contract law if the submitting party is notified that they exist. Undisclosed
4 procedures are not relevant to a contract analysis. If the submitting party is notified of the procedure, decisions
5 about acceptance or rejection of the submission are funneled through that procedure or, in the case of acceptance,
6 an express decision to accept. This protects both parties. The submitter and the recipient receive the benefit of a
7 more specific set of choices about taking on a contract or rejecting it.

8 5. *Idea Submissions: Consideration* An agreement for submission of an idea carries with it, in the
9 absence of contrary terms, the assumption that the idea has value or uniqueness. That value exists if the idea is
10 concrete, confidential and novel. If, for example, a party agrees for a fee to submit an idea for enhancing the
11 success of audiovisual works, the contract is not satisfied if the idea is "draw more attractive images." This adopts
12 New York law and cases such as *Oasis Music Inc. v. 100 USA, Inc.*, 614 N.Y.S.2d 878 (N.Y. 1994). A submission
13 that does not meet this standard does not breach the contract, unless the agreement gave express assurances that
14 the submission would be novel. The licensee cannot recover payments it already made. Rather, the default rule is
15 that the provider of the non-novel submission cannot enforce any future obligations as to the submitted idea. The
16 basic principle is that a non-novel idea is not adequate consideration for a contract and that a proponent of an idea
17 implicitly represents that the idea has value. This is not met in a case of a non-novel idea.

18 This principle does not require that the idea rise to the level of novelty as that term is used in
19 patent law. The information must not be something that is generally and widely known. Cases on combination
20 secrets and other situations in trade secret law where information has sufficient uniqueness or secrecy to qualify as
21 a trade secret should inform decisions under this standard.

22 Nothing in this section precludes an agreement that does not hinge on the uniqueness of the
23 proposed submission. Whether such agreement exists must be judged based on the fundamental notion that a party
24 does not implicitly contract away its rights, without a fee, to use publicly known information merely because it
25 contracted for "disclosure" of such material.

26 [B. Terms of Records]

27 SECTION 2B-207. ADOPTING TERMS OF RECORDS.

28
29 (a) Except as otherwise provided in Section 2B-208, a party adopts the terms of a record,
30 including a standard form, if ~~it~~ the party agrees to the record, by manifesting assent or otherwise.

31
32 ~~_____ (b) The Adoption of the terms of a record between parties may occur may be adopted as~~
33 ~~the terms of the contract after beginning commencement of performance or use under their~~
34 ~~agreement if the parties y-had reason to know that their agreement would be represented in whole~~
35 ~~or in part by a later record to be agreed and, but at the time performance or use commenced~~
36 ~~there was no opportunity to review the record or a copy of it before performance or use~~
37 ~~commenced or it had not been completed.~~

38
39 (be) If a party adopts the terms of a record, ~~the~~ ese terms become part of the contract
40 without regard to the party's knowledge or understanding of individual terms in the record,
41 except for a term that is unenforceable because it fails to satisfy another requirement of this

1 article.

2 **Definitional Cross Reference:**

3 "Agreement". Section 1-201. "Conspicuous". Section 2B-102. "Contract". Section 1-201. "Information":
4 Section 2B-102. "Informational Rights": Section 2B-102. "Manifest assent." Section 2B-111 "Opportunity to
5 review." Section 2B-112. "Party". Section 1-201. "Record". Section 2B-102. "Standard form". Section 2B-102.
6 "Term". Section 1-201.

7 **Reporter's Notes:**

8 -1. *Scope of the Section.* Article 2B deals separately with forming a contract and the terms of that
9 contract. This section is the primary section on adoption of terms of a record as terms of a contract. Section 2B-
10 208 limits the creation of terms in mass-market licenses and the time over which they can be presented. Section
11 2B-209 deals with cases when records do not create contract terms, but a contract exists because of conduct.

12 This section states basic principles about when and how terms of a record are adopted and also
13 expressly recognizes that commercial deals often involve layered contracting, providing a standard for determining
14 when this type of contract term formation exists. Subsection (b) rejects the idea that a contract and all terms must
15 be formed at a single point in time. It permits layered contracting that reflects commercial practice in cases where
16 the parties have reason to believe that terms will be proposed at some later time. The effect of a failure to agree
17 depends on whether the agreement on terms was a condition to the existence of a contract. See Section 2B-202.

18 2. *Adopting Terms.* If a party agrees to a record, it adopts the terms of the record whether or not
19 the record is a standard form. Standard forms are common in commercial practice because they provide
20 efficiencies for both parties. Treating them in law as less than any other record of a contract would put commercial
21 law in conflict with commercial practice and reduce the efficiencies such records provide. Because of the broad
22 opportunities allowed in the Internet, standard forms will increasingly not be the province of only one party to the
23 deal. This section rejects decisions which hold that a term that is not unconscionable or induced by fraud may still
24 be invalidated because a court holds, after-the-fact, that a party could not have expected it to be in the contract.
25 Absent unconscionability, fraud or similar conduct, commercial parties are bound by the records to which they
26 assent.

27 a. *Knowledge of Terms.* It is not necessary that the adopting party actually read,
28 understand, or negotiate the terms of a record. This rule follows virtually universal law in the United States.
29 Assent to the record encompasses assent to its terms. Unconscionable terms remain unenforceable despite assent.

30 b. *Modes of Assent.* A party is bound by the terms of a record only if it agrees to the
31 record, by manifesting assent or otherwise. The party may authenticate (sign) the record. The party's conduct may
32 indicate assent to a record or a contract. Section 2B-111. The latter focuses on objective manifestations of assent.
33 A party cannot manifest assent to a form or other record unless it has had an opportunity to review that form before
34 reacting. Finally, there are residual modes of assent that satisfy the idea that assent must be objectively expressed,
35 even though they do not fit the precise standards of authentication or manifesting asset.

36 3. *Later Terms: Layered Contracting.* In ordinary commercial practice, while some contracts are
37 formed and their terms fully defined at a single point in time, many commercial transactions involve a rolling or
38 layering process. An agreement exists, but terms are clarified or created over time. That principle is acknowledged
39 in various portions of original Article 2, for example in provisions allowing contracts formed with terms left open.
40 Comments to original Section 2-207 note that later records presented to the other party are treated as proposed
41 modifications or confirming memorandum only in cases of "a proposed deal which in commercial understanding
42 has in fact been closed." Section 2-207, *comment 2*. Where that is not true, the later terms are part of the primary
43 contracting process. Similarly, original Section 2-311 allows enforcement of agreements that permit one party to
44 later specify the particulars of performance (e.g., terms of the contract) after the initial agreement is reached.
45 Consistently, original Section 2-305 allows agreements in which one party later fixes the price.

46 Often, the commercial expectation is that terms will follow or be developed after performance
47 begins. While some courts seem to hold that an initial agreement per se concludes the contracting as a single event
48 notwithstanding ordinary practice and expectations that terms will follow, other courts recognize layered contract
49 formation and term definition, correctly viewing contracting as a process, rather than a single event. *ProCD, Inc.*
50 *v. Zeidenberg*, 86 F.3d 1447 (7th Cir. 1996). Often, performance commences with each party understanding that
51 terms will be provided for later agreement, or otherwise used to define the contract. See *Brower v. Gateway 2000,*
52 *Inc.*, - N.Y.S.2d - (N.Y.A.D. 1998). This section, along with the contract formation principles, explicitly accepts
53 the layering principle and provides a standard for distinguishing when the intent or expectations is to conclude the

1 contract at the initial point as contrasted to an expectation that terms will be provided for later agreement. In
2 information commerce, the circumstances often indicate that initial general assent assumes that terms will be
3 developed or presented later to fill out the details of the transaction. Such circumstances include customary
4 practices in software licensing customs, but also will include use of electronic agents by licensees. For example, a
5 business or a consumer may instruct its electronic agent to search the Internet for car dealers willing to meet pre-
6 set terms and offer prices within a pre-set range. While the business or consumer will expect to stand on the terms
7 accepted by the dealer, both it and the dealer expect the contract to have more details, such as warranty,
8 maintenance, and other standard provisions, without having to consider all such terms in the first interaction of the
9 automated contracting system.

10 Section 2B-207(b) clarifies that contract terms can be proposed and agreed to as part of
11 completing the initial contract even though proposed after the beginning of performance by one or both parties.
12 Such terms are treated as part of the initial contracting process if at the time of initial agreement, the parties had
13 reason to know and, thus, expected that this would occur and that terms of a record to be agreed would provide
14 elaboration of their contract. If, instead, the parties considered their deal to be closed at the outset, then
15 subsequently proposed terms from either party are treated as a proposed modification of the agreement, effective
16 only under concepts applicable to such modifications. The third alternative, of course, is that the initial agreement
17 leaves terms open and allows one part to specify what those terms are at some later date. The act of specifying the
18 terms is, in effect, merely a performance of the contract.

19 In layered contracting terms are created over time. Thus, for example, where the parties reach an
20 initial agreement about a multiple delivery contract and begin shipments before reducing that agreement to more
21 elaborate written terms, the record when agreed to does not modify the original agreement, but reflects an
22 expansion and elaboration as part of that contract. Similarly, the parties might begin performance on a software
23 development agreement while terms are being developed and, ideally, agreed to by counsel and the representatives
24 of the parties. When a final, fully elaborated record is completed and agreed to, it does not amend the contract, but
25 simply becomes part of the now finalized contractual arrangement. Of there is no assent to the record, whether the
26 parties have a contract hinges on whether they regarded assent to the record when developed as a condition to a
27 contractual relationship. If so, and if there is no such agreement, there is no contract and equitable principles
28 apply to avoid unjust enrichment and other effects of the beginning of performance.

29 The concept in subsection (b) differs from Section 2B-305 and original Section 2-311, both of
30 which refer to agreements that give one party or its designate a contractual right to specify or particularize terms of
31 performance. In cases governed by those sections, the party receiving the later terms is not presented with a right
32 to agree to or reject the terms; the terms are in effect part of the original agreement. Where no further assent is
33 required under the agreement, 2B-305 indicates that the terms must be proposed in good faith and in accordance
34 with reasonable commercial standards.

35 Subsection (b) indicates that a layered contracting exists if the parties at the time of the initial
36 agreement had reason to know that this would occur. The "reason to know" standard parallels the standard for
37 determining when acts constitute assent to a contract. Reason to know does not require specific notice or specific
38 language in an original agreement, although such factors may play a role in determining reason to know. It can
39 also be inferred from the entire circumstances, including routine or ordinary practices of which a party is or should
40 be aware. In some areas of commerce, such as many aspects of software contracting and many forms of mail order
41 contracting, the circumstances of the agreement in ordinary commerce give reason to know that terms may be
42 subsequently proposed. In Section 2B-207, the time over which the record can be proposed is referenced to the
43 expectations of the parties under the reason to know standard. At some point, the deal has been closed, but
44 specifying when this occurs in terms of a fixed time standard is impossible in general commerce. It requires an
45 analysis focused on the context and circumstances.

46 The standard set out in subsection 2B-207(b) also carries forward into similar transactions in the
47 mass market in Section 2B-208. Section 2B-208, however, places a time limit on when proposal of the terms must
48 occur and precludes the terms from alter terms that are expressly agreed to by the parties to the license. In
49 addition, of course, Section 2B-208 creates a right to a cost free refund if the proposed terms are unacceptable to
50 the receiving party. See also Section 2B-617.

51 4. *Right to a Return.* In many cases governed by subsection (b) and in mass-market licenses, if
52 assent is sought after the person paid or delivered or became obligated to pay or deliver, the manifestation of assent
53 is not effective unless the person had a right to a return if it chooses to refuse the license. Section 2B-112. This
54 return obligation applies in mass market contracts and in other contracts if the expectation is that the terms will be
55 provided at or before the first use of the information, a typical format in certain types of software contracting. It

1 does not apply in the more open-ended commercial arrangements where there is merely an expectation that terms
2 will be agreed to (or rejected) at some point during performance, such as in the software development agreement
3 mentioned in note 5. In these contexts, general principles of equity apply to deal with the circumstances where
4 there is ultimately a failure to agree.
5

6 **SECTION 2B-208. MASS-MARKET LICENSES.**
7

8 (a) A party adopts the terms of a mass-market license for purposes of Section 2B-207
9 only if the party agrees to the license, by manifesting assent or otherwise, before or during the
10 party's initial performance or use of or access to the information. A term is not part of the license
11 if:

12 (1) ~~if the term is unconscionable under Section 2B-110 or is unenforceable under~~
13 ~~Section 2B-105(a) or (b); or~~

14 (2) subject to Section 2B-301, ~~if the term conflicts with terms to which the parties~~
15 ~~to the license expressly agreed.~~

16 (b) If a licensee party does not have an opportunity to review a mass-market license or a
17 copy of it before becoming the party ~~delivered the information or became obligated to pay and the~~
18 ~~party does not agree, by manifesting assent or otherwise, to the license after having that~~
19 ~~opportunity, the licensee following rules apply: (1) The party is entitled to a return and to:~~

20 (12) ~~The licensee is entitled to: (A) reimbursement of any reasonable expenses~~
21 ~~incurred in complying with the licensor's instructions for return or destruction of the licensed~~
22 ~~subject matter and documentation or, in the absence of instructions, incurred for return postage or~~
23 ~~similar reasonable expense in returning them; and~~

24 (2B) compensation for any reasonable and foreseeable costs of restoring an
25 information processing system to reverse changes in the system caused by the installation, if:

26 (Ai) the installation occurs because information must be installed to enable
27 review of the license; and

28 (Bii) the installation alters the system or information in it but does not

1 restore the system or information upon removal of the installed information because of rejection
2 of the license.

3 (c) In a mass-market transaction, if a licensor does not have an opportunity to review a
4 record proposing terms before the licensor delivers or becomes obligated to deliver the
5 information, and if the licensor does not agree, by manifesting assent or otherwise, to those terms
6 after having that opportunity, the licensor is entitled to a return.

7 **Uniform Law Source:** Restatement (Second) of Contracts § 211.

8 **Definitional Cross Reference:**

9 "Contract": Section 1-201. "Information": Section 2B-102. "Information processing system": Section 2B-102.
10 "Informational Rights": Section 2B-102. "License": Section 2B-102. "Licensor": Section 2B-102. "Manifest
11 assent": Section 2B-111. "Mass-market license": Section 2B-102. "Party": Section 1-201. "Return": Section 2B-
12 102. "Term": Section 1-201.

13 **Reporter's Notes:**

14 1. *Scope of the Section.* This section deals with mass-market licenses, including consumer
15 transactions. It defines the circumstances under which a party's assent to a mass-market license adopts the terms
16 of that record. The section places limitations on the effectiveness of mass-market licenses. The section should be
17 read in connection with Section 2B-207 and Section 2B-111. While most current mass-market licenses are
18 presented by the licensor and accepted by the licensee, modern technology and contracting practices are not
19 necessarily so limited and the section would also apply to a mass-market license presented by a licensee and
20 accepted by a licensor in the mass market.

21 Many mass-market licenses are presented and agreed to at the outset of a transaction; some are
22 presented afterwards. This section deals with both. The costs of return provided for in subsection (b) provide
23 strong incentives for terms of the license to be presented at the outset of the transaction when practicable.

24 Some mass-market licenses are between two parties. Others involve two separate agreements and
25 a three-party transaction. The two contracts in the three-party transaction are: 1) the mass-market license between
26 the publisher and the end user, and 2) the retail agreement between the end user and the retailer. These
27 agreements are not necessarily made at the same time. This section deals with both. The three-party arrangement
28 is also addressed in Section 2B-617.

29 2. *General Mass-Market Rules.*

30 There are a number of ways in which the terms of a mass market or other contract can be
31 specified. This can and does often occur by a general agreement of the parties unrelated to any record containing
32 specific terms. In other cases, as described in Section 2B-305, the parties may agree that the terms or particulars of
33 performance may be specified later by one party. See *TI Brower v. Gateway 2000, Inc.*, 676 N.Y.S.2d 569
34 (N.Y.A.D. 1998). Under Section 2B-305, the later supplied terms are enforceable without further agreement to
35 them if the terms are proposed in good faith and within bounds of commercial reasonableness. This section deals
36 with a third method of deriving the terms of a mass market agreement, obtaining assent to a record containing
37 those terms – either at the outset of the transaction or shortly after it is initially formed.

38 Three limiting principles govern adoption of mass-market licenses regardless of when the license
39 is presented and agreed to by the assenting party. In addition, as outlined in Section 2B-105, fundamental public
40 policy limit enforceability of mass-market terms in some cases. See notes to Section 2B-105(b).

41 a. *Assent and Agreement.* A party adopts the terms of a record only if it agrees to the
42 record by manifesting assent or otherwise indicating its agreement. A party cannot manifest assent unless it had an
43 opportunity to review the record before that assent occurs. This means that the record must be available for review
44 and called to the person's attention in a manner such that a reasonable person ought to have noticed it. Section
45 2B-112. A manifestation of assent requires conduct, including a failure to act, or its statements, indicate assent and
46 that it has reason to know that, in the circumstances, this will be the case. Section 2B-111 and related notes.

47 Adopting the terms of a record for purposes of this section occurs pursuant to Section 2B-207.

1 Under that section, if the terms of the record are proposed for assent by a party only after the party commences
2 performance of the agreement between the parties, the terms become effective under these sections only if the party
3 (e.g., the licensee) had reason to know that terms would be proposed after the initial agreement. Even if reason to
4 know exists, this section requires that the terms be presented not later than the initial use of the information and
5 that, if the mass-market license was not made available before the initial agreement, the person is given a right to a
6 return should it refuse the license.

7 *b. Unconscionability.* Even if a party adopts the terms of a record, a court may invalidate
8 unconscionable terms pursuant to Section 2B-110. Unconscionability doctrine invalidates terms that are bizarre
9 and oppressive and hidden in boilerplate language. For example, a term in a mass-market license that default on
10 the mass-market contract for \$50 software cross defaults all commercial licenses between the parties may be
11 unconscionable if there was no reason for the licensee to anticipate that breach of the small license would
12 constitute breach of an unrelated larger license negotiated between the parties. Similarly, a clause in a mass-
13 market license that grants a license back of all trademarks or trade secrets of the licensee without any discussion of
14 the issue between the parties would ordinarily be unconscionable. The principle is one of prevention of oppression
15 and unfair surprise and not of disturbance of allocation of risks because of superior bargaining power.

16 *c. Conflict with Agreed Terms.* In addition to unconscionability doctrine, this section
17 provides that standard terms in a mass-market form cannot alter the terms expressly agreed between the parties to
18 the license. A term is expressly agreed by the parties if they discuss and come to agreement regarding an issue and
19 their agreement becomes part of their bargain. For example, in a consumer transaction where the consumer
20 requests software compatible with a particular type of machine and the vendor agrees to provide such software, the
21 standard terms of vendor's mass-market contract cannot alter the vendor's agreement with the consumer to provide
22 compatible software. As is true with express warranties, this is subject to traditional parol evidence concepts which
23 bear on the provability of extrinsic evidence that varies the terms of the writing. Additionally, of course, under
24 Section 2B-617 the terms of any publisher's license cannot alter the agreement between the end user and the
25 retailer unless expressly adopted by them as their own agreement.

26 Paragraph (a)(2) preserves the essential bargain of the parties to a mass-market transaction. For
27 example, if a librarian acquires educational software for children from a publisher's retail outlet under an express
28 agreement that the software may be used in its library network, a term in the publisher's license that limits use to a
29 single user computer system conflicts with and is over-ridden by the agreement for a network license. This section
30 does not adopt *Restatement (Second) of Contracts* § 211(c), which has been adopted in only a small minority of
31 states. However, paragraph (a)(2) responds to some of the policy concerns on which that *Restatement* rule is based.

32 3. *Terms Prior to Payment.* If a mass-market license is presented before a price is paid, Article 2B
33 follows general law that enforces a standard form contract if the party assents to it. See, e.g., *Storm Impact, Inc. v.*
34 *Software of the Month Club*, 44 U.S.P.Q.2d 1441 (N.D. Ill. 1997) (on-screen license prevents waiver of copyright
35 and precludes fair use claim).

36 The fact that license terms are non-negotiable or that the contract may constitute a "contract of
37 adhesion" does not invalidate it under general contract law or this article. A conclusion that a contract is a
38 contract of adhesion may, however, require that courts take a closer look at contract terms to prevent
39 unconscionability. See, e.g., *Klos v. Polske Linie Lotnicze*, 133 F.3d 164 (2d Cir. 1998); *Fireman's Fund Insurance*
40 *v. M.V. DSR Atlantic*, 131 F.3d 1336 (9th Cir. 1998); *Chan v. Adventurer Cruises, Inc.*, 123 F.3d 1287 (9th Cir.
41 1997). It should be recognized, however, that this article's concepts of manifest assent and opportunity to review
42 address concerns often relevant to this review. Nevertheless, when applicable, the closer scrutiny followed in
43 general commercial contract law may be appropriate here.

44 Many mass-market transactions involve three parties and two contracts. The publisher's license
45 does not agree to license under terms other than those in the license and that choice should generally be enforced if
46 manifesting assent after an opportunity to review occurs. In digital commerce, the license terms often define the
47 product, for example, in distinguishing between single user and network use, consumer use and commercial use,
48 ordinary private use or rights to public display or performance. See *ProCD v. Zeidenberg*, 86 F.3d 1447 (7th Cir.
49 1996). Market choices of this type provide an important commerce in this field. Often, the license and its
50 enforcement benefit the licensee, giving it rights that would not be present in the absence of an enforceable license.
51 See, e.g., *Green Book International Corp. v. Inunity Corp.*, -- F. Supp. -- (D. Mass. 1998) (shrink wrap granted
52 right to distribute an element of the software).

53 While this section follows general law in enforcing standard form contracts, it adds a significant
54 protection for the party presented with the form. As indicated in subsection (a)(2), the standard terms of the form
55 cannot contradict terms expressly agreed to by the parties to the license and which are admissible in court under

1 parol evidence rules.

2 4. *Terms after Initial Agreement.* In modern commerce, licenses are sometimes presented after
3 initial general agreement between the ultimate licensee and either the retailer or the licensor-publisher. These
4 transactions are a form of layered, or open-term, contracting recognized under original Article 2 and this article. In
5 the software industry, such contracts are supported by both commercial expectations developed by standard practice
6 over several decades and, frequently, by enforcement of copyright or other intellectual property rights held by the
7 publisher. The contracting format allows contracts between end users and remote parties that control copyright or
8 other interest in the information. Enforceability of the license can be important to both parties because it allows a
9 non-infringing exercise of licensed rights by the licensee and the licensor to tailor licensed rights to particular
10 market demand. Such licenses are enforceable under this article, but to prevent abuse, in addition to the general
11 protection created for all mass-market licenses, this section creates additional rights for the licensee.

12 a. *Distribution Methods.* Commercial distribution of copies of digital information does not
13 necessarily parallel distribution involving sale of goods. The differences are grounded in the nature of the subject
14 matter, the property rights involved, and the choices by the rights owner (publisher). In some cases, of course, the
15 publisher sells copies to a distributor for resale. That choice does create a distribution sequence similar to the sale
16 of goods. In other cases, the information is provided directly to the end user on-line and under an agreement
17 directly between the rights owner and the end user. In many cases, however, the publisher distributes through
18 third parties but does not simply sell copies to a distributor for re-distribution. See, e.g., *Microsoft Corp. v. DAK*
19 *Indus., Inc.*, 66 F.3d 1091 (9th Cir. 1995).

20 This is a different distribution system than that used in the sale of goods because the distributor
21 does not receive ownership, but merely a limited distribution license which allows distribution of the copies only if
22 that occurs subject to an end user license with the rights owner or licensor. This method may be used to provide
23 greater or lesser rights to eventual end users than would occur through simple sales of copies. For copyrighted
24 works, the distribution format is based on the rights owner's exclusive right to *distribute* the work in copies. If the
25 distributor does not comply with the license, an eventual transferee is not protected as a bona fide purchaser and is
26 subject to an infringement claim. See *Microsoft Corp. v. Grey Computer*, 910 F. Supp. 1077 (D. Md. 1995);
27 *Microsoft Corp. v. Harmony Computers & Electronics, Inc.*, 846 F. Supp. 208 (ED NY 1994); *Marshall v. New*
28 *Kids on the Block*, 780 F. Supp. 1005 (S.D.N.Y. 1991); *Major League Baseball Promotion v. Colour-Tex*, 729 F.
29 Supp. 1035 (D. N.J. 1990).

30 In this latter distribution system, the license presented to the end user after it acquires a copy
31 from a retailer is between the *rights owner* (or a distributor authorized to license to end users) and the end user,
32 rather than between the end user and *the retailer*. This license creates, for the first time, a contractual relationship
33 between the rights owner and the end user. In this three-party setting (end user, retailer, copyright owner or
34 authorized licensor), the enforceability of the license is important to both parties. It is important to the end user
35 because it is the first time it receives authorization to copy or otherwise use the work from the rights owner. It may
36 also be important to the end user because many mass-market licenses give the end user rights that would not arise
37 if it purchased a copy. A sale of a copy of a copyrighted work does not give the copy owner a number of rights that
38 it may desire. It does not convey a right to make multiple copies, to publicly display the work, to make derivative
39 works from the copy, or, in the case of computer programs, to rent the copy to others. The enforceability of the
40 license is also important for the rights owner because the terms of use and other conditions of the license help
41 define the product it transfers. There are also general marketplace benefits in that the licensing framework allows
42 price and market differentiation that allows product priced for and tailored to market demands of various forms,
43 such as in distinguishing pricing of a consumer as compared to a commercial or educational license.

44 b. *Timing of Assent.* Agreement to the mass-market record can occur before the initial use,
45 but must occur no later than during the initial use of the information. This places an outside limit on layered
46 contracting in the mass market and acknowledges customary practices in the software and other industries
47 applicable to the mass market. The time limitation enacts a potentially significant protection of the licensee's
48 expectations in this type of marketplace. Of course, this time limitation does not prevent subsequent modification
49 of the license at any point in time or performance by a party that defines terms pursuant to agreement.

50 c. *Cost Free Return Right.* In mass-market licenses presented after an initial agreement,
51 three issues are important. One involves preventing unconscionable terms; that issue is identical in all mass-
52 market contracting. The second involves the relationship between the license terms and the express agreement of
53 the parties to the license. This issue also does not change based on when the license is presented. The third issue
54 involves assuring the licensee an opportunity to review and an effective choice to accept or reject a license
55 presented after initial payment. Subsection (b) addresses this issue. It creates a return right that places the end user

1 in a situation whereby it can exercise a meaningful choice regarding licenses presented after initial agreement.
2 This article refers to a return right, rather than a right to a refund, because it recognizes that in the mass market,
3 under developing technologies, the concept of requiring this right may apply to either the licensee or the licensor,
4 whichever is asked to assent to a record presented after the initial agreement.

5 In cases where the form is presented to the licensee after it becomes initially obligated to pay, it
6 must be given a cost free right to say no. This does not mean that the end user can reject the license and use the
7 information. What is created is a right to return to a situation generally equivalent to that which would have
8 existed if the end user had reviewed and rejected the license at the time of the initial agreement. The return right
9 does not apply if the licensee agrees to the license. It is not a means by which a party may rescind an agreement to
10 which it has assented, but rather a method of ensuring that assent in this setting is real. Thus, if the licensee
11 manifests assent to the license because it has reason to know that opening the packet holding the disk of the
12 software constitutes assent to the license, the return right does not apply.

13 This return right also does not arise if there was an opportunity to review the license before
14 making the initial agreement. In subsection (b) the exposure to potential liability for expenses of reinstating the
15 system after review creates an incentive for licensors to make the license or a copy thereof available for review
16 before the initial obligation is created. Subsection (b) does not apply to transactions involving software obtained
17 on-line if the software provider makes available and obtains assent to the license as part of the ordering process.
18 On the other hand, in a mail order transaction, if the license is first received along with the copy of the information
19 that was ordered, subsection (b) applies. The return right under this section includes, but differs from the return
20 right in Section 2B-112(b) as part of the opportunity to review. The return in Section 2B-208 is cost free in that
21 the end user receives reimbursement for reasonable costs of return and, in a case where installation of the
22 information was required to review the license and caused changes in the end user's system, to reasonable costs in
23 returning the system to its initial condition. Of course, the fact that this section states an affirmative right in the
24 mass market to a cost free refund does not affect whether under other law outside of this article, a similar right
25 might exist in other contexts.

26 Subsection (b) contemplates that if a licensor chooses to seek assent to a license after the initial
27 agreement, it has an obligation to reimburse the licensee's expenses incurred if it rejects the license. The expenses
28 incurred in return of the subject matter of the rejected license must be reasonable and foreseeable. The costs of
29 return do not include attorney fees or the cost of using an unreasonably expensive means of return or to airplane
30 tickets, lost income or the like unless such expenses are required by instructions of the licensor. The expense
31 reimbursement refer to ordinary expenses such as the cost of postage.

32 Similarly, in cases where expenses of restoring the system are incurred because the information
33 was required to be installed in order to review the license, expenses chargeable to the licensor must be both
34 reasonable and foreseeable. The reference here is to actual, out-of-pocket expenses and not to compensation for
35 lost time or lost opportunity. The losses here do not encompass consequential damages. Moreover, they must be
36 foreseeable. A party may be reasonably charged with ordinary requirements of a licensee that are consistent with
37 others in the same general position, but cannot be held responsible for losses caused by the particular
38 circumstances of the licensee of which it had no reason to know. A twenty dollar software license provided in the
39 mass market should not expose the provider to significant loss unless the method of presenting the license can be
40 said ordinarily to cause such loss. Similarly, it is ordinarily not reasonable to provide recovery of disproportionate
41 expenses associated with eliminating minor and inconsequential changes in a system that do not affect its
42 functionality. On the other hand, the provider is responsible to cover actual expenses that are foreseeable from the
43 method used to obtain assent.
44

45 SECTION 2B-209. TERMS WHEN OF CONTRACT FORMED BY CONDUCT.

46 (a) Except as otherwise provided in subsections (b) and (c) and subject to Section 2B-
47 301, if a contract is formed solely by conduct of the parties, in determining the terms of the
48 contract, a court shall consider the terms and conditions to which the parties expressly agreed,
49 course of performance, course of dealing, or usage of trade, the nature of the parties' conduct, the

1 in law, rather than in another contract.

2 4. *International Issues.* Intellectual property rights are territorial in character. They extend only
3 within the territory of the state that creates them, although some deference internationally occurs through multi-
4 lateral treaties. Subsection (c)(2) parallels this and provides that the obligations created about exclusivity and
5 infringement extend only within this country and to a country specifically referenced in the license or warranty.
6 Specification in the license of particular countries or "worldwide" in this sense refers only to specifications or
7 representations made with express reference to the non-infringement warranty, such as "Licensor warrants non-
8 infringement worldwide." Other references in a license may not be intended to create a warranty. For example, a
9 grant of a license for worldwide use may in the circumstances be no more than a permission to use the information
10 worldwide without risk of a lawsuit by the licensor, rather than a warranty that worldwide use will not infringe
11 other rights. In the case of a "worldwide" warranty, the obligation extends only to countries that have property
12 rights treaties with the United States. In the absence of such relationships, the rights created under United States
13 law cannot create rights in the other country and, thus, the warranty cannot extend there.

14 5. *Disclaimer.* As with all other warranties, the warranties in the section can be disclaimed. This
15 section provides for such disclaimer in language based on original Article 2. This requires specific language or
16 circumstances indicating that the warranties are not given. Consistent with the general approach of contract law as
17 a planning tool, illustrative language is provided. Subsection (d) limits the conditions under which the warranty of
18 this section can be disclaimed or modified, it does not limit or preclude avoidance or modification of the hold
19 harmless obligation that might arise under subsection (a). If the circumstances or language indicate no intent to
20 hold harmless, that agreement is enforceable and this subsection does not require proof that the language is
21 conspicuous.

22
23

SECTION 2B-402. EXPRESS WARRANTY.

24 (a) Subject to subsection (c), an express warranty by a licensor is created as follows:

25 (1) An affirmation of fact or promise made by the licensor to its licensee in any
26 manner, including in a medium for communication to the public such as advertising, which relates
27 to the information and becomes part of the basis of the bargain creates an express warranty that
28 the information to be furnished under the agreement shall conform to the affirmation or promise.

29 (2) Any description of the information which is made part of the basis of the
30 bargain creates an express warranty that the information shall conform to the description.

31 (3) Any sample, model, or demonstration of a final product which is made part of
32 the basis of the bargain creates an express warranty that the performance of the information shall
33 reasonably conform to the performance of the sample, model, or demonstration, taking into
34 account such differences as would appear to a reasonable person in the position of the licensee
35 between the sample, model, or demonstration and the information as it will be used.

36 (b) It is not necessary to the creation of an express warranty that the licensor use formal

1 words such as "warranty" or "guarantee", or state a specific intention to make a warranty.

2 However, an express warranty is not created by:

3 _____ (1) an affirmation or prediction merely of the value of the information or
4 informational rights;

5 _____ (2) a display or description of a portion of the information to illustrate the
6 aesthetics, market appeal, or the like, of informational content; or

7 _____ (3) a statement purporting to be merely the licensor's opinion or commendation of
8 the information or informational rights.

9 (c) This article does not alter or establish any standards under which an express warranty
10 or an express contractual obligation for published informational content is created or not created.

11 If an express warranty or contractual obligation is created for published informational content
12 and is breached, the remedies of the aggrieved party are those pursuant to this article and the
13 agreement.

14 **Uniform Law Source: Section 2A-210. Section 2-313.**

15 **Definitional Cross References.**

16 "Aggrieved party": Section 1-201. "Agreement": Section 2B-102. "Information": Section 2B-102. "Informational
17 content": Section 2B-102. "Licensee": Section 2B-102. "Licensor": Section 2B-102. "Party": Section 1-201.
18 "Published informational content": Section 2B-102. "Remedy": Section 1-201. "Value": Section 1-201.

19 **Reporter's Note:**

20 1. *Scope and Basis of Section.* This section adopts original Article 2 law on express warranties,
21 except with respect to published informational content, where it preserves current law. "Express" warranties rest
22 on "dickered" aspects of the individual bargain and go so clearly to the essence of that bargain that, as indicated in
23 Section 2B-406(a), words of disclaimer in a standard form cannot alter the dickered terms. "Implied" warranties,
24 on the other hand, rest on a common factual situation or set of conditions so that no particular language is
25 necessary to evidence them and they will exist unless disclaimed.

26 2. *Basis of the Bargain.* Subsection (a) adopts the "basis of the bargain" originally created in
27 Article 2. This allows courts and parties to draw on a body of case law for distinguishing express warranties from
28 puffing and other, unenforceable statements, representations or promises. While there are many factual issues, this
29 standard provides better guidance than would an entirely new standard. The "basis of the bargain" concept is that
30 express affirmations, promises and the like are enforceable as express warranties if they are within the matrix of
31 elements that constitutes and defines the bargain of the parties, but that they are not express warranties if they are
32 not part of that basis for the contract. The standard does not require that a licensee prove actual reliance on a
33 particular statement, affirmation or promise in deciding to enter into the contract, but does require proof that the
34 statement, affirmation or promise played a role in reaching or defining the bargain. This standard enables the
35 creation of express obligations on the more general showing that statements about the information are part of the
36 deal and basic to it. On the other hand, express warranty law deals with the elements of a bargain and is not a
37 surrogate for regulation. It does not support imposing liability in contract for all statements of a licensor made
38 about an information product, even if not brought to the attention of the licensee. This holds as well for

1 advertising. If the licensee knows of the advertisement by the vendor and it became part of the basis of the bargain
2 with the vendor, the advertisement may create an .

3 The question is whether statements of the licensor made to the licensee have in the circumstances
4 and in objective judgment become part of the basic bargain. No specific intention to make a warranty is necessary.
5 In actual practice affirmations of fact describing the information and made by the licensor about it during the
6 bargain are ordinarily regarded as part of the description of the information unless they are mere puffing,
7 predictions, or otherwise not an enforceable part of the bargain. No reliance on such statements need be shown in
8 order to weave them into the fabric of the agreement. Rather, to take such affirmations, once made, out of the
9 agreement requires clear affirmative proof. The issue normally is one of fact. This is true also of the question of
10 whether product documentation may create an express warranty. Whether the documentation is reviewed before or
11 after the initial deal, the test is the same. If it contains affirmations of fact or promises that otherwise qualify and it
12 became part of the basis of the bargain, an express warranty may arise.

13 The question is whether language, samples, or demonstrations are fairly to be regarded as part of
14 the contract. If language is used after the closing of the deal, (as when the licensee on taking delivery asks for and
15 receives an additional assurance), the assurance may become a modification of the contract and does not need to be
16 supported by further consideration if it is otherwise reasonable. Section 2B-304. Alternatively, under the layered
17 contract formulation established in Article 2 and employed here, that assurance may simply be treated as a further
18 elaboration of the actual terms of the contract.

19 3. *Relation to Disclaimers.* The basic principle is that the purpose of the law of warranty is o
20 determine what it is that the licensor has in essence agreed to provide. A contract is normally a contract for
21 something describable and described. These descriptions, if part of the bargain, are an express warranty. This
22 article follows the general principle, as in original Article 2, that the obligations in a proven express warranty
23 cannot other than in exceptional cases be materially deleted. A contract term generally disclaiming "all warranties,
24 express or implied" cannot be given literal effect under Section 2B-406(a). This does not mean that the parties,
25 if they consciously desire, cannot make their own bargain as the desire, including a bargain that does not
26 encompass the purported express warranty. But in determining what they have agreed upon consideration should
27 be given to the fact that the probability is small that a real price is intended to be exchanges for a pseudo-
28 obligation. Thus, for example, a contract for a "word-processing program" that contains the general disclaimer
29 noted above is nevertheless a contract for an information product that meets the basic description of a "word-
30 processing program."

31 4. *Puffing and Expressions of Opinion.* Subsection (b) retains current law to the effect that puffing
32 or mere statements of opinion do not form an express warranty. The law on the distinction between an actionable
33 representation and puffing is long and well-developed. The distinction requires a determination based on the
34 circumstances of the particular transaction. It reflects that in common experience some statements and predictions
35 cannot fairly be viewed as entering into the bargain. In transactions involving computer programs as with other
36 commercial information, the closer the statement relates to describing the technical specifications, technical
37 performance or product description of the information, the more likely it is to be an express warranty when
38 communicated to the licensee, while the more the statement pertains to predictions about expected benefits that
39 may result from use of the information, the more likely it will be found to be puffing. Of course, whether or not a
40 statement is an express warranty does not affect whether the statement in context might yield a remedy under the
41 law of fraud or misrepresentation.

42 Subsection (b) also refers to statements or demonstrations pertaining to aesthetics and market
43 appeal. Aesthetics, as used here, refers to questions of the artistic character, tastefulness, beauty or pleasing
44 character of the informational content, not to statements pertaining to how a person uses the information or to what
45 is the essential nature of the information itself. Thus, for example, a statement that a clip art program contains
46 easily useable images of "horses" or images of "working people," if it becomes part of the basis of the bargain,
47 creates an assurance that the subject matter of the clip art program is horses or working people and that the images
48 are usable. However, it does not purport to state that they are tasteful or artistically pleasing.

49 5. *Advertising as a Source of Express Warranty.* Paragraph (a)(1) provides that advertising may
50 create an express warranty if the advertising statements otherwise conform to the standards for creation of an
51 express warranty under this section. This expands the scope of express warranty law in some states. Statements
52 made in advertising, of course, often reflect puffing or mere expressions of opinion and do not create an express
53 warranty. As with other statements, a warranty arises only if the statement becomes part of the bargain and a
54 bargain actually occurs. The affirmation of fact made in the advertising must be known by the licensee, influence
55 and in fact become part of the basis of the bargain under which it acquired the information.

1 In the absence of that relationship, liability for false advertising, if any, would not be under
2 contract law, but under tort or advertising law rules. This section does not create a false advertising claim under
3 the guise of contract law.

4 6. *Descriptions.* Paragraph (a)(2) makes specific some of the principles described above about
5 when a description of the information becomes an express warranty. The description need not be by words.
6 Technical specifications, blueprints and the like can afford more exact descriptions than mere language and, if
7 made part of the basis of the bargain, become express warranties. Of course, all descriptions by merchants must be
8 read against the applicable trade usage and in light of the concepts of general rules as to merchantability resolving
9 any doubts about the meaning of the description. The description requires a commercially reasonable
10 interpretation.

11 7. *Samples and Models.* Subsection (a)(3) expands current Article 2 by expressly referring to
12 express warranties created by demonstrations of information. In addition, subsection (a)(3) carries forward the
13 Article 2 principle that express warranties may be created by descriptions, samples or models.

14 The basic treatment of samples, models and demonstrations is no different than the treatment of
15 statements. Although the underlying principles are unchanged, the facts are often ambiguous when something is
16 shown to be illustrative in nature. In mercantile experience, the mere exhibition of a "sample", a "model" or a
17 "demonstration" does not of itself show whether it is merely intended to "suggest" or to "be" the character of the
18 subject-matter of the contract.

19 Representations created by demonstrations and models must be gauged by what inferences would
20 be communicated to a reasonable person in light of the nature of the demonstration, model, or sample. In the
21 world of goods, showing a sample of a keg of raw beans by lifting out a cup-full communicates one inference,
22 while a demonstration of a complex database program running ten files creates an entirely different inference if the
23 ultimate intended use of the system is to process ten million files. This difference also applies to beta models of
24 software which are used on a test or a demonstration basis and may contain elements that are not carried forward
25 into the ultimate product. In such cases, the parties ordinarily understand that what is being demonstrated on a
26 small scale or what is being tested on a beta model basis is not necessarily representative of actual performance or
27 of what will eventually be the product. The basic rule, as with any other purported express warranty, is that any
28 affirmation model or demonstration must be interpreted in a reasonable fashion that reflects the circumstances of
29 the test or demonstration. The court's discussion in *NMP Corp. v. Parametric Technology Corp.*, 958 F. Supp.
30 1536 (S.D. Okla. 1997) illustrates the issue in respect to software demonstrations.

31 8. *Published Informational Content.* Subsection (c) preserves current law for published
32 informational content. This section does not create any express warranty for published informational content, but
33 does not preclude the imposition of any liability under other law or the creation of an express contractual
34 obligation. While there are many reported cases dealing with express warranties in goods and using the standards
35 adopted here, no case law for published informational content uses Article 2 standards. See Joel R. Wolfson,
36 *Express Warranties and Published Informational Content under Article 2B: Does the Shoe Fit?*, 16 John Marshall
37 Journal of Computer & Info. Law 384 (1997). This subject matter entails significant First Amendment interests
38 and general public policies that favor encouraging public dissemination of information. Courts that deal with
39 liability pertaining to published informational content must balance contract themes with these more general social
40 policies.

41 This section leaves undisturbed existing law dealing with how obligations are established with
42 reference to published informational content. The cases tend to deal with obligations of this type as questions of
43 express contractual obligation, rather than in language relating to warranties. Thus, a promise to provide an
44 electronic encyclopedia obligates the party to deliver that type of work and is not fulfilled by delivery of a
45 computerized work of fiction. In other cases where the issues focus on the quality of the content or the like, courts
46 if inclined to find contract liability will do so under general contract law theory. Many, however, will conclude
47 that the level of risk in the published informational content situation and the potentially stifling effect that contract
48 liability might have on the dissemination of speech should lean toward limiting or excluding liability. See *Daniel*
49 *v. Dow Jones & Co., Inc.*, 520 N.Y.S.2d 334 (N.Y. City Ct. 1987). In some other cases, liability may arise under
50 tort law theories, such as in *Hansberry v. Hearst*, 81 Cal. Rptr. 519 (Cal. App. 1968). However, this section rejects
51 the seemingly simple, but ultimately inappropriate step of merely adopting Article 2 concepts from sales of goods
52 to this much different context. That would risk a large and largely unknown change of law and over-reaching of
53 liability in a sensitive area. It would create uncertainty that would in itself chill public dissemination informational
54 content while courts grapple with adapting entire new standards of liability to this area.

55 Where there is a contract obligation that is breached, the remedies of this article apply and

1 replace remedies under common law for breach of contract. This includes all provisions of Part 7 of this article,
2 including standards that measure and exclude or limit damages.

3 9. *Third Parties.* This section deals with express warranties made by the licensor to its licensee. It
4 does not deal with the enforceability under contract or tort theory of representations made by remote parties and
5 relied on by an ultimate user of the information. The case law in tort dealing with such issues pertaining to
6 information does not generally parallel cases dealing with the manufacture and sale of goods. Information
7 providers have been held liable to third parties in only a few, atypical cases. This article does not expand or
8 exclude such third party liability, however it may develop under tort law.
9

10 **SECTION 2B-403. IMPLIED WARRANTY: MERCHANTABILITY OF**
11 **COMPUTER PROGRAM.**

12 (a) Unless the warranty is disclaimed or modified, a merchant licensor of a computer
13 program warrants:

14 (1) to the end user that the computer program is reasonably fit for the ordinary
15 purpose for which it is distributed;

16 (2) to a distributor that:

17 (A) the program is adequately packaged and labeled as the agreement or
18 the circumstances may require; and

19 (B) in the case of multiple copies, the copies are within the variations
20 permitted by the agreement, of even kind, quality, and quantity, within each unit and among all
21 units involved; and

22 (3) that the program conforms to the promises or affirmations of fact made on the
23 container or label, if any.

24 (b) Unless disclaimed or modified, other implied warranties may arise from course of
25 dealing or usage of trade.

26 (c) A warranty created under this section does not apply to informational content,
27 including its aesthetics, market appeal, accuracy, or subjective quality, whether or not included in
28 or created by a computer program.

29 **Uniform Law Source: Section 2-314; 2A-212. Revised.**
30 **Definitional Cross References.**

1 "Agreement": Section 1-201. "Computer program": Section 2B-102. "Contract": Section 1-201. "Delivery":
2 Section 2B-102. "Informational content": Section 2B-102. "Licensor". Section 2B-102. "Merchant". Section 2B-
3 102.

4 Reporter's Notes:

5 1. *Background and Policy.* This section generally applies the Article 2 warranty of merchantability to
6 computer programs. Since it applies to all computer programs provided by a merchant, it creates a merchantability
7 warranty for cases that under prior law are services contracts with no warranties or with obligations limited to making a
8 reasonable effort and exercising ordinary care. The merchantability warranty does not depend on how the program is
9 delivered, whether it be electronically or in a tangible copy. It flows from the presumed nature of a commercial
10 undertaking in which the supplier of the program is a merchant dealing with that type of information. Disclaimer or
11 modification of the warranty of merchantability or any part of the warranty is dealt with in Section 2B-406.

12 Article 2B warranties stem from a combining of three different legal traditions. One is from Article 2
13 and focuses on the quality of the product, creating an implied warranty that the result delivered will conform to ordinary
14 standards for products of that type. The second is from common law dealing with licenses, services and information
15 contracts, which in many states focuses on the process or performance effort, rather than the result. The third is from
16 common law pertaining to services in some states and information contracts. It disallows implied obligations of accuracy
17 in information transferred other than in a special relationship of reliance. In this and the following section, Article 2B
18 distinctions are drawn between computer programs, on the one hand, and information or services, on the other hand.

19 The implied merchantability warranty and the warranty in Section 2B-404 pertaining to the
20 accuracy of data may both apply to the same transaction and the same information product. The one applies to the
21 program and its functions, while the other applies to the accuracy of data in an appropriate relationship.

22 2. *Merchantability.* The content of the merchantability obligation turns basically on the meaning of
23 the terms of the agreement as recognized in the applicable business, trade or industry. A computer program
24 delivered under an agreement by a merchant must be of a quality fit for the purpose for which it was distributed.
25 The implied warranty is made by all merchant-licensors. It does not apply to non-merchants. Non-merchants,
26 however, like merchants, are obviously subject in appropriate cases to claims grounded in fraud or other theories
27 premised on misrepresentation.

28 a. *Concept of Merchantability.* Merchantability does not require perfection, but the concept
29 is that the subject matter of the warranty must fall generally within the average standards applicable in commerce
30 for information of the type.

31 In 1998, a popular operating system program for small computers used by both consumers and
32 commercial licensees contained over ten million lines of code or instructions. In the computer these instructions
33 interact with each other and with code and operations of other programs. This contrasts with a commercial jet
34 airliner popular in that year that contained approximately six million parts, many of which involved no interactive
35 function. A typical consumer goods product contains fewer than one hundred parts. A typical book has fewer than
36 one hundred fifty thousand words. In the software environment, it is virtually impossible to produce software of
37 complexity that contains no errors in instructions that intermittently cause the program to malfunction, so-called
38 "bugs." The presence of errors in general commercial products is fully within common commercial expectation.
39 Indeed, in programs of complexity, the absence of errors would be unexpected. In this commercial environment,
40 the contract law issue is whether the level of error exceeds the bounds of ordinary merchantability. This occurs
41 only if the significance of the errors or their number lies outside ordinary commercial expectations for the
42 particular type of program.

43 b. *Fit for Ordinary Purposes.* The program must be fit for the ordinary purpose for which
44 it is distributed. Ordinary purposes focuses on expected end user applications of the type to which the product as
45 distributed was addressed. To an extent greater than in reference to sales of goods, computer programs are often
46 adapted to and employed in ways that go well beyond the uses expected when the distribution occurs. Use of
47 ordinary, mass-market database programs in the context of highly sensitive or commercial applications does not
48 change the warranty into one assuring fitness for ordinary purposes of such use. The focus is to the market and
49 types of uses to which the program is directed. Ordinarily, of course, that also defines the ordinary actual use of
50 the program. In any event, to be fit for ordinary purposes does not require that the program be the best fit or the
51 perfect application for that use. If the transfer is to a person acquiring the program for re-distribution by sale, the
52 program must be honestly resellable because it is what it purports to be.

53 3. *Aesthetics.* Subsection (c) makes clear a rule that would apply in any event. Merchantability
54 does not apply to the aesthetics of a product under this article. Aesthetics, as used here, refer to questions of the
55 artistic character, tastefulness, beauty or pleasing nature of informational content. These are matters of personal

1 taste, rather than elements of any standard of merchantability. On the other hand, merchantability standards are
2 appropriately addressed to whether the information is what its description purports it to be and to whether it is or is
3 not useable by the transferee. Thus, for example, if the complaint about the images created by a program is that
4 they are not attractive, merchantability does not apply. If the complaint is that the commands and images are
5 blurred and not useable, an issue of merchantability exists. A statement that a clip art program contains images of
6 "horses" creates an assurance that the subject matter of the clip art program is horses or working people and that
7 the images are usable. It does not purport to state that they are tasteful or artistically pleasing or whether they are
8 brown, beige, white or green.

9 4. *Cause of Action for Breach.* In a cause of action for breach of warranty, as with all products, it is
10 of course necessary to show not only the existence of the warranty, but that the warranty was broken and that the
11 breach of the warranty was the proximate cause of the loss sustained. In such an action, in complex computer
12 systems involving different hardware and software, the loss must be connected to defects in the computer program
13 for which a breach of warranty is claimed. Proof that losses were caused by events after the program was installed
14 and unconnected to it operate as a defense.
15

16 SECTION 2B-404. IMPLIED WARRANTY: INFORMATIONAL CONTENT.

17 (a) Unless the warranty is disclaimed or modified, a merchant that, in a special
18 relationship of reliance with a licensee, collects, compiles, processes, provides, or transmits
19 informational content, warrants to its licensee that there is no inaccuracy in the informational
20 content caused by the merchant's failure to perform with reasonable care.

21 (b) A warranty does not arise under subsection (a) with respect to :

22 (1) published informational content; or

23 (2) a person that acts as a conduit or provides only editorial services in collecting,
24 compiling, or distributing informational content identified as that of a third person.

25 (c) The warranty under this section does not come within Section 1-102(3).

26 **Uniform Law Source:** Restatement (Second) of Torts 552.

27 **Definitional Cross References.**

28 "Informational content". Section 2B-102. "Licensee". Section 2B-102. "Merchant". Section 2B-102. "Party".
29 Section 1-201. "Published informational content". Section 2B-102.

30 **Reporter's Notes:**

31 1. *Scope and Effect.* This section recognizes a new implied warranty present in some informational
32 content contracts, consulting, data processing or similar agreements. The warranty focuses on the accuracy of data,
33 but does not create an absolute liability or absolute assurance of no inaccuracy. Instead, it creates a protected assurance in
34 such contracts that no inaccuracies are caused by a failure of reasonable care. This section does not create a non-
35 disclaimable duty of reasonable care.

36 2. *Accuracy.* A party that provides or processes information in a special relationship of reliance warrants
37 that no inaccuracy exists due to the provider's lack of reasonable care in performing its obligations under the contract.

38 a. *Ordinary Standards as Described.* The presence of an inaccuracy relates to expectations
39 gauged by ordinary standards of the relevant trade under the circumstances. In most large commercial databases, ordinary
40 expectations assume that some data will be inaccurate. Variations or error rates within the range of commercial
41 expectations of the business, trade or industry do not breach the warranty established in this section. If greater than

1 ordinary accuracy is desired that desire must be expressed in the terms of the agreement and provide for greater than
2 normal expectations of accuracy. For example, if in reference to a particular type of database the normal expected error
3 rate is twenty percent, an error rate of fifteen percent does not create an inaccuracy within this section and does not breach
4 the warranty. On the other hand, if in a database of thousands of medical treatments for various allergic reactions the
5 commercial expectation is that the error rate should be no more than three percent, an error rate of ten percent may create
6 an inaccuracy that results in breach of this implied warranty if caused by a failure to exercise reasonable care in compiling
7 the information.

8 In addition, inaccuracy is gauged by reference to what the data purport to be under the agreement. This
9 section follows cases such as *Lockwood v. Standard & Poor's Corp.*, 175 Ill.2d 529, 689 N.E.2d 1140, 228 Ill.Dec.
10 719 (Ill. App. 1997). A contract to estimate the number of users of a product in Houston does not imply an obligation to
11 provide an accurate count, but merely requires an estimate. That estimate, if honestly made and given cannot breach this
12 warranty.

13 *b. Accuracy and Aesthetics.* The warranty is that information is not inaccurate because of
14 a lack of reasonable care. Informational content is accurate if, within applicable understandings of the level of
15 permitted errors, the informational content correctly portrays the objective facts to which it relates. This warranty
16 is not a warranty about the aesthetics, subjective quality, or marketability of informational content. These are subjective
17 issues. Assurances on these issues require express agreement to give such assurances.

18 *c. Adequate Results.* One who hires an expert for purposes of consultation or data-related
19 services relying on that expert's skills cannot expect infallibility. As under common law, reasonable efforts, not
20 perfect results, provide the appropriate standard in the absence of express contract terms to the contrary. The
21 analysis of the New York court in an analogous setting indicates the policy for the rule adopted here for those who
22 collect, compile or process informational content. *Milau Associates v. North Avenue Development Corp.*, 42
23 N.Y.2d 482, 398 N.Y.S.2d 882, 368 N.E.2d 1242 (N.Y. 1977).

24 3. *Merchants in a Reliance Relationship.* The implied warranty arises only if the licensor is a
25 merchant with respect to the particular activity. In addition, the information must have been provided in a "special
26 relationship of reliance" between the licensor and the licensee. If the absence of such relationship, the mere fact
27 that one person provides information to another creates no implied obligation beyond good faith.

28 *a. Reliance Relationships.* The requirement of a special relationship of reliance is
29 fundamental to the implied obligation and to balancing the interest of protecting client expectations while not imposing
30 excessive liability risk on informational content providers in a way that might chill their information-providing activities.
31 This stems in part from cases applying *Restatement (Second) of Torts* § 552. The special element of reliance comes from
32 the relationship itself, a relationship characterized by the provider's knowledge that the particular licensee plans to rely on
33 the data in its own business and expects that the provider will tailor the information to its needs. The obligation arises
34 only for those persons who possess unique or specialized expertise, or who are in a special position of confidence
35 and trust with the licensee such that reliance on the inaccurate information is justified and the party has a duty to
36 act with care. See *Murphy v. Kuhn*, 90 N.Y.2d 266, 682 N.E.2d 972 (N.Y. 1997).

37 The relationship also requires that the provider make the information available as part of its own
38 business in providing such information. The licensor must be in the business of providing that type of information. This
39 adopts the rationale of cases holding that information provided as part of a differently focused commercial relationship,
40 such as the sale or lease of goods, does not create protected expectations about accuracy except as might be created under
41 warranty law. The court in *A.T. Kearney v. IBM*, 73 F.3d 238 (9th Cir. 1997) describes many of the relevant issues.
42 See also *Picker International, Inc. v. Mayo Foundation*, 6 F. Supp.2d 685 (ND Ohio 1998).

43 An equally fundamental aspect of a special reliance relationship is that the information provider
44 is specifically aware of and personally tailors information to the needs of the licensee. A special relationship does
45 not arise for information made generally available to a group in standardized form even if those who receive the
46 information subscribe to an information service they believe relevant to their commercial needs. The information
47 must be personally tailored for the recipient. The transaction involves more than merely making information available.

48 It does not require a fiduciary relationship, but does require indicia of special reliance.

49 *b. Published Informational Content.* The implied warranty does not apply to published
50 informational content. By definition, published informational content is information transferred other than in a reliance
51 relationship. Published informational content is informational content made available to the public as a whole or to a
52 range of subscribers on a standardized, rather than personally tailored basis. This includes a wide variety of commercially
53 important general distribution or subscription services providing informational content. It includes, for example, an
54 Internet Website listing information of local restaurants, their prices and their quality, as well as services that provide data
55 about current stock or monetary exchange prices to subscribers.

1 Published informational content is the subject matter of general commerce in ideas, political, economic,
2 entertainment or the like, whose distribution entails fundamental public policy interests in supporting distribution and not
3 chilling this process through liability risks. In the new technology era to which this article is addressed, many
4 information systems analogous to newspapers, magazines, or books and are made available digitally or in on-line
5 arrangements. Their traditional counterparts have never been exposed to contractual liability risks based on claims
6 of mere inaccuracy and treating the new systems differently would reject the wisdom of prior law. A computerized
7 database is the "functional equivalent of a traditional news service." These services have no contractual liability for
8 mere inaccuracies in data in part because ordinary expectations anticipate the presence of errors and in part
9 because of fundamental public policies supporting the free flow of information and free expression. Creating and
10 applying a lower standard that creates greater liability for an electronic data provider than applies to a public
11 library, book store, or newsstand would place an undue burden on the free flow of information. This policy
12 underlies the results in *Cubby, Inc. v. CompuServ, Inc.*, 3 CCH Computer Cases 46,547 (S.D.N.Y. 1991) and in
13 *Daniel v. Dow Jones & Co., Inc.*, 520 N.Y.S.2d 334 (N.Y. City Ct. 1987).

14 4. *Reasonable Care.* The primary obligation is that there is no inaccuracy in the data. An
15 inaccuracy in informational content, however, creates no liability unless the inaccuracy results from a failure to
16 exercise reasonable care. This corresponds to common law standards in many states for implied obligations in
17 contracts involving services or information content. What constitutes reasonable care depends on the
18 circumstances. Where the nature of the subject matter involves significant risks of personal injury if data are
19 inaccurate, a higher degree of care can be expected than in situations in which the recipient reasonably should have
20 other sources and judgments that will influence its decision, rather than mere reliance on the specific information
21 provided in a transaction within this section.

22 5. *Conduits and Editing.* The implied warranty applies only to information provided by the
23 licensor. Subsection (b) clarifies that there is no warranty with respect to third party content where the provider
24 identifies the information as coming from that third party. The implied warranty does not apply to parties engaged
25 in editing informational content of another person. See *Doubleday & Co. v. Curtis*, 763 F.2d 495 (2d Cir.), cert.
26 dismissed, 474 U.S. 912 (1985); *Windt v. Shepard's McGraw-Hill, Inc.*, 1997 WL 698182 (ED Pa. Nov. 5, 1997)

27 A person collecting, summarizing or transmitting the third party data acting as a conduit does
28 not create the same expectations about performance as does a direct information provider. Whatever expectations
29 arise focus on the third party identified as the originator of the information. In these cases, however, that third
30 party may not be contractually obligated to the licensee. Whether or not a contract exists, however, the conduit's
31 obligation and the licensee's reasonable expectations with respect to it do not entail an obligation regarding the
32 accuracy of the third party data. Concerning the policy issues in dealing with conduits, see *Zeran v. America On-*
33 *Line, Inc.*, 129 F.3d 327 (4th Cir. 1997). Merely providing a conduit for third party data should not create an
34 obligation to ensure the care exercised in reference to the data provided by the third party. On the related issue of
35 tort liability for publishers who are not also authors, *Winter v. G.P. Putnam's Sons*, 938 F.2d 1033 (9th Cir. 1991)
36 (describes policy interests that also support subsection (b)).

37 6. *Relationship to Tort Law.* Since this section creates a new warranty analogous to the theory of
38 negligent misrepresentation, disclaimer or non-existence of the implied warranty should have a strong bearing on
39 potential existence of the tort claim in the same transaction. In cases involving economic loss, a disclaimer of this
40 warranty in most cases forecloses a tort claim based on the same facts. However, this section does not foreclose
41 development of other approaches to liability for information products under tort law. Most courts have held that published
42 information products are not products for purposes of a product liability claim and that there is little or no duty of
43 reasonable care owed to third parties in screening advertising or similar material for publication. See *Winter v. G.P.*
44 *Putnam's Sons*, 938 F.2d 1033 (9th Cir. 1991). There are cases to the contrary on both points, however. Since these are
45 issues under tort law, this article neither precludes nor encourages further exploration of the tort law questions.

46 7. *Disclaimer.* This warranty may be disclaimed pursuant to Section 2B-406. For an analogous
47 case under common law, see *Rosenstein v. Standard and Poor's Corp.*, 636 N.E.2d 898 (Ill. App. 1993). The
48 warranty is that there are no inaccuracies in the information caused by a lack of care. It is, therefore, not subject to
49 the general rule that duties of reasonable care cannot be disclaimed by contract. Section 1-102. What is disclaimed
50 is a warranty related to the accuracy of the content, not the exercise of reasonable care with respect to the
51 information. That disclaimer is not affected by Section 1-102. No obligation of reasonable care is created under
52 this section.

53
54 **SECTION 2B-405. IMPLIED WARRANTY: LICENSEE'S PURPOSE SYSTEM**

1 **INTEGRATION.**

2 (a) Unless the warranty is disclaimed or modified, if a licensor at the time of contracting
3 has reason to know any particular purpose for which the information is required and that the
4 particular licensee is relying on the licensor's skill or judgment to select, develop, or furnish
5 suitable information, the following rules apply:

6 (1) Except as otherwise provided in paragraph (2), there is an implied warranty
7 that the information is ~~be~~-fit for that purpose.

8 (2) If from all the circumstances, it appears that a licensor was to be paid for the
9 amount of its time or effort regardless of the fitness of the resulting information, the implied
10 warranty is that the information will not fail to achieve the licensee's particular purpose as a result
11 of the licensor's lack of reasonable care.

12 (b) There is no warranty under subsection (a) with regard to:

13 (1) the aesthetics, market appeal, or subjective quality of informational content; or

14 (2) published informational content, but there may be a warranty with regard to
15 the licensor's selection among published informational content from different providers.

16 (c) If an agreement requires a licensor to provide or select a system consisting of
17 computer programs and goods, and the licensor has reason to know that the licensee is relying on
18 the skill or judgment of the licensor to select the components of the system, there is an implied
19 warranty that the components provided or selected will function together as a system.

20 (d) The warranty under this section is not governed by the limitations ~~does not come~~
21 within Section 1-102(3).

22 **Uniform Law Source: Section 2-315; 2A-213. Substantially revised.**

23 **Definitional Cross References.**

24 "Agreement": Section 1-201. "Computer program": Section 2B-102. "Information": Section 2B-102.

25 "Informational content": Section 2B-102. "Licensee": Section 2B-102. "Licensor": Section 2B-102. "Published

26 informational content": Section 2B-102. "Reason to know": Section 2B-102

27 **Reporter's Note:**

1 1. *General Approach.* This section reconciles diverse case law and, in subsection (c), recognizes a
2 new implied warranty. Subsection (a)(1) states as a general rule that in some cases reliance creates an implied
3 warranty of fitness for the licensee's particular purpose. Subsection (a)(2) applies the common law "efforts"
4 standard in other cases. This bifurcation deals with the issue of whether the appropriate implied obligation is an
5 obligation to produce a result (present in sales of goods) or an obligation to make an effort to achieve a result
6 (common law). Under prior case law in software and other fields, the decision is based on whether a court views
7 the transaction as a sale of goods (result) or a contract for services (effort). The reported decisions are split and
8 often lack a principled basis for distinction.

9 2. *Warranty of Fitness.* Subsection (a)(1) follows original Section 2-315. Whether or not this
10 warranty arises in any individual case is basically a question of fact to be determined by the circumstances at the
11 time of contracting. A "particular purpose" differs from the ordinary purpose for which the information is used in
12 that it envisages a specific use by the licensee which is peculiar to the nature of its business whereas the ordinary
13 purposes for which information products are used are those envisaged in the concept of merchantability. Although
14 normally this warranty arises only if the licensor is a merchant with appropriate "skill or judgment," if the
15 circumstances justify the warranty it may be appropriate in the case of a non-merchant licensor.

16 The warranty does not exist if there is no reliance in fact or if the particular purposes are not
17 made known to the licensor. This warranty requires particularization of the needs of the licensee in the context.

18 No express exclusion is made for cases where the information product is identified by a trade
19 name. The designation of an item by a trade name, or indeed in any other definite manner, is only one of the facts
20 to be considered on the question of whether the licensee actually relied on the licensor, but it is not of itself decisive
21 of the issue. However, if the licensee is insisting on a particular brand, it is not relying on the licensor's skill or
22 judgment is making the selection and no warranty results. But the mere fact that the product acquired has a known
23 trade name is not sufficient in itself to indicate nonreliance if it was recommended by the licensor. A similar
24 principle is expressly stated in subsection (b)(2) relating to the selection from among various publishers.

25 The warranty obligates the licensor to meet known licensee needs if the circumstances indicate
26 that the licensee is relying on the provider's expertise to achieve this result. There are many development contract
27 and other situations where no reliance exists, including cases where the licensee provides the contract performance
28 standards, rather than relying on the provider to fill needs of the licensee. The express terms of the agreement
29 require that the product meet the specifications, but no reliance exists on whether fulfilling the specifications will
30 meet applicable needs.

31 3. *Services Warranty.* Subsection (a)(2) applies to cases that more closely resemble services
32 contracts and carries forward the type of implied obligation most appropriate in such cases. The subsection
33 recognizes that a skilled service provider does not guaranty a result suitable to the other party unless it expressly
34 agrees to do so. *Milau Associates v. North Avenue Development Corp.*, 42 N.Y.2d 482, 398 N.Y.S.2d 882, 368
35 N.E.2d 1242 (N.Y. 1977). Subsection (a)(2) provides a standard to determine when a contract calls for services and
36 effort, rather than result. The test centers on whether the circumstances indicate that the service provider would be paid
37 for time or effort, regardless of the fitness of the result. Such payment terms typify a services contract. Other standards
38 evolved under general common law may also indicate that the parties intended a services obligation as delineated in
39 subsection (a)(2). What constitutes reasonable care or effort depends on the project involved and other circumstances of
40 the relationship. *Micro Manager, Inc. v. Gregory*, 147 Wisc.2d 500, 434 N.W.2d 97 (Wisc. App. 1988).

41 4. *Aesthetics and Published Information.* Subsection (b) makes clear that the warranty does not
42 apply to published informational content or to aesthetics associated with the information. Aesthetics, as used here,
43 refer to questions of the artistic character, tastefulness, beauty or pleasing nature of informational content. These
44 are matters of personal taste, rather than elements of any standard of implied warranty. On the other hand,
45 warranty standards are appropriately addressed to whether the information is what its description purports it to be
46 and to whether it is or is not useable by the transferee. Thus, for example, if the complaint about images created by
47 a program is that they are not attractive, no implied warranty applies. If the complaint is that the commands and
48 images are blurred and not useable, a warranty issue may exist.

49 5. *System Integration.* Subsection (c) creates a new implied warranty that requires systems performance
50 in cases of systems integration contracts. While related to the implied fitness warranty, it expands that concept creating
51 new protection for licensees. The warranty is that the selected components will function as a system. This does not mean
52 that the system, other than as stated in subsection (a), will meet the licensee's needs. Neither does it mean that use of the
53 system does not or may not infringe third party rights. This warranty simply creates an assurance that the parts will
54 functionally operate as a system. This is an additional assurance beyond the fact that each component must be separately
55 functional.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

SECTION 2B-406. DISCLAIMER OR MODIFICATION OF WARRANTY.

(a) Words or conduct relevant to the creation of an express warranty and words or conduct tending to disclaim or modify an express warranty must be construed wherever reasonable as consistent with each other. Subject to Section 2B-301 with regard to parol or extrinsic evidence, the disclaimer or modification is inoperative to the extent that this construction is unreasonable.

(b) Except as otherwise provided in subsections (c), (d), and (e), to disclaim or modify an implied warranty or any part of it, but not the warranty in Section 2B-401, the following rules apply:

(1) To disclaim or modify an implied warranty arising under Section 2B-403 language must mention "merchantability", or "quality", or use words of similar import. To disclaim or modify an implied warranty arising under Section 2B-404, language must mention "accuracy", or use words of similar import.

(2) Language to disclaim or modify an implied warranty arising under Section 2B-405 must be in a record. It is sufficient to state "There is no warranty that this information or efforts will fulfill any of your particular purposes or needs", or words of similar import.

(3) Language is sufficient to disclaim all implied warranties if it individually disclaims each implied warranty or, except for the warranty in Section 2B-401, if it states "Except for express warranties stated in this contract, if any, this [information] [computer program] is being provided with all faults, and the entire risk as to satisfactory quality, performance, accuracy, and effort is with the user", or words of similar import.

(4) Language that is sufficient under Article 2 or 2A to disclaim or modify an implied warranty of merchantability is sufficient to disclaim or modify the warranties under

1 Sections 2B-403 and 2B-404. Language that is sufficient under Article 2 or 2A to disclaim or
2 modify an implied warranty of fitness for a particular purpose is sufficient to disclaim or modify
3 the warranties under Section 2B-405.

4 (5) In a mass-market transaction, language in a record that disclaims or modifies
5 an implied warranty must be conspicuous.

6 (c) Unless the circumstances indicate otherwise, all implied warranties, but not the
7 warranty in Section 2B-401, are disclaimed by expressions like "as is" or "with all faults" or other
8 language that in common understanding call the licensee's attention to the disclaimer of warranties
9 and makes plain that there are no implied warranties.

10 (d) When the licensee before entering into the contract has examined the information or
11 the sample or model as fully as it desired or it has refused to examine the information, there is no
12 implied warranty with regard to defects which an examination ought in the circumstances to have
13 revealed to the licensee.

14 (e) An implied warranty may ~~can~~ also be disclaimed or modified by course of
15 performance, course of dealing, or usage of trade.

16 (f) If a contract requires ongoing performance or a series of performances by the licensor,
17 language of disclaimer or modification which complies with this section is effective with respect
18 to all performances under the contract.

19 (g) Remedies for breach of warranty may be limited in accordance with this article.

20 **Uniform Law Source: Section 2A-214. Revised.**

21 **Definitional Cross References.**

22 "Computer program": Section 2B-102. "Conspicuous": Section 2B-102. "Contract": Section 1-201. "Information":
23 Section 2B-102. "Licensee": Section 2B-102. "Licensor": Section 2B-102. "Mass-market license": Section 2B-
24 102. "Record": Section 2B-102.

25 **Reporter's Note:**

26 1. *General Structure and Policy.* This section brings together various rules relating to the
27 disclaimer of warranties, except for the statutory warranties under Section 2B-401. The general approach
28 corresponds to existing Article 2 and Article 2A. This article does not alter consumer protection statutes which in
29 some states preclude disclaimer of warranties in consumer cases. See Section 2B-105. With respect to implied
30 warranties, this section follows fundamental policies of U.S. law which recognize that parties may disclaim or limit

1 warranties. Implied warranties are default rules whose contractual disclaimer and limitation is integral to the
2 contract choice paradigm under which commerce occurs and to the ability of a party to control the risk it elects to
3 undertake.

4 2. *Express Warranties.* Subsection (a) restates original Article 2. It uses modern language of
5 "disclaimer" and "modification," rather than prior Article 2 language, without substantive change. General
6 language of disclaimer cannot alter or avoid express warranties. While courts should construe contract terms of
7 disclaimer and language of express warranty as consistent with each other whenever reasonable, in cases of
8 inconsistency, the express warranty language controls. In effect, express warranties cannot be disclaimed, but as
9 always, the parties' agreement controls. For example, the language of the agreement, including language styled as
10 a disclaimer, may indicate that a purported warranty did not in fact become part of the basis of the bargain and is
11 not, therefore, an express warranty.

12 Express warranties arise in various ways, including by description of the information itself. Since
13 they cannot be disclaimed, express product descriptions are an important balance in contracts that comprehensively
14 disclaim all implied warranties. The information must conform to its express description. A word processing
15 system for a particular computer system that is delivered with a disclaimer of all implied warranties, must still
16 meet the express warranty describing it as a "word processing" program for a particular type of hardware.
17 However, that goes less to quality of the program than to the fact of the program if without content being a
18 program.

19 While express warranties survive general disclaimers, the licensor is protected against unfounded
20 claims of oral express warranties by the provisions of this article on parol and extrinsic evidence and the terms of
21 its contract, and against unauthorized representations by the law of agency. Remedies for breach of an express
22 warranty are dealt with in other sections of this article and may be modified in accordance with this article.

23 3. *Disclaimers and Fraud.* This article does not alter the law of fraud. In some cases, liability for
24 fraud may arise despite the presence of a general disclaimer of warranties. Thus, if the licensor makes an
25 intentional misrepresentation of an existing material fact on which the licensee reasonably relied, it may be liable
26 for fraud even though such disclaimer eliminates contractual warranty liability. A failure to disclose known
27 material problems in a product being provided pursuant to a license may constitute fraud if an obligation to
28 disclose arises under that law. The court's discussion in *Strand v. Librascope, Inc.*, 197 F. Supp. 743 (E.D. Mich.
29 1961) illustrates one such circumstance. While general disclaimers do not foreclose liability for intentional fraud in
30 most states, disclaimers or other denials of obligation specific to the particular facts may foreclose a claim in fraud
31 because they eliminate the element of fraud that requires reasonable reliance on a material misrepresentation.

32 4. *Disclaimer of Implied Warranties in a Record.* Subsection (b) brings together various provisions
33 on disclaimer of implied warranties. These rules are subject to the provisions of subsections (c), (d) and (e).

34 a. *When a Record is Required.* This article follows original Article 2. Disclaimer of the
35 implied warranty of merchantability is not required to be in a record, nor is a disclaimer of a warranty in Section
36 2B-404 required to be in a record. However, as in original Article 2, the rule is different for disclaimer of the
37 "fitness" warranty. This must be in a record, except in cases governed by subsections (c), (d) or (e).

38 b. *Merchantability and Accuracy Warranties.* Under subsection (b)(1), to disclaim the
39 warranty of merchantability or accuracy of data, the disclaimer must mention merchantability or accuracy, or use
40 words of similar import. Use of the specific term "merchantability" is allowed, but not required. The use of
41 alternative words, of course, must in fact communicate the nature of the disclaimer. The other language suffices if
42 it reasonably achieves the purpose of clearly indicating that the warranty is not given in the particular case.

43 c. *Conspicuousness.* Subsection (b)(5) requires that if language of disclaimer is in a
44 record, that language must be conspicuous in cases involving a mass-market license. This provides additional
45 protection against surprise in such retail market environments. Article 2B does not require that the language be
46 conspicuous in other types of transaction. Outside the mass market, benefits of requiring conspicuous language are
47 off-set by the trap created for persons drafting contracts and the difficulty of reliably meeting this requirement in
48 electronic commerce. Also, unlike what might have been expected when original Article 2 developed, implied
49 warranties are routinely disclaimed in modern commercial transactions. Original Article 2 requires a conspicuous
50 disclaimer only if the disclaimer is in writing.

51 d. *Fitness Warranty.* Subsection (b)(2) provides language adequate to disclaim the
52 warranty under Section 2B-405. The language is more explicit than under Article 2, but use of the specific
53 language is not mandatory. This language works, but other language may also be sufficient if it reasonably
54 achieves the purpose of indicating that the warranty is not given.

55 e. *Disclaimer of All Warranties.* Subsection (b)(3) recognizes that in some cases all

1 implied warranties are disclaimed. The subsection sets out language sufficient for this purpose. The disclaimer of
2 all warranties using this language is, of course, subject to the requirement of a record and, in the case of mass-
3 market transactions, the requirement that the disclaimer be conspicuous.

4 *f. Article 2 and 2A Disclaimers.* Subsection (b)(4) provides for cross-article validity of
5 disclaimer language. The intent is to avoid requiring parties to make a priori determinations about Article 2B or
6 Article 2 (or 2A) coverage particularly when "mixed" transactions will be increasingly common. Language
7 adequate to disclaim a warranty under one of these articles is adequate to disclaim the equivalent warranty under
8 Article 2B.

9 4. *Disclaimers of Implied Warranties By the Circumstances.* Subsections (c), (d) and (e) deal with
10 common factual situations in which the circumstances of the transaction are in themselves sufficient to call the
11 licensee's attention to the fact that no implied warranties are made or that a certain implied warranty is being
12 excluded.

13 *a. "As is" Disclaimers.* This provision follows original Article 2. Terms such as "as is"
14 and "with all faults" in ordinary commercial usage are understood to mean that the licensee takes the entire risk as
15 to the quality of the information involved. The terms here are in fact merely a particular application of subsection
16 (e) which provides for exclusion of modification of implied warranties by usage of trade. They provide an
17 important means of conducting business in many areas of commerce. They also accommodate electronic
18 commerce which may require in many contexts "short" or summary terms defining the contract because of limited
19 space in records. The language need not be in a record.

20 *b. Excluding Warranties by Inspection.* Subsection (d) also follows original Article 2.
21 Implied warranties may be excluded or modified by the circumstances where the licensee examines the information
22 or a sample or model of it before entering into the contract. "Examination" as used in subsection (d) is not
23 synonymous with inspection before acceptance or at any other time after the contract has been made. It goes rather
24 to the nature of the responsibility assumed by the licensor at the time of the making of the contract. Of course if
25 the buyer discovers the defect and uses the information anyway, or if it unreasonably fails to examine the
26 information before using it, resulting damages may be found to result from his own action rather than from a
27 breach of warranty. It goes to the nature of the obligation undertaken by the licensor at the time of the transaction.

28 In order to bring the transaction within the scope of the "refused to examine" language of this
29 subsection, it is not sufficient that the information merely be available for inspection. There must in addition be a
30 demand or offer by the licensor that the licensee examine the information. This puts the licensee on notice that it
31 is assuming the risk of defects which the examination ought to reveal.

32 Application of the doctrine of "caveat emptor" in all cases where the buyer examines the goods
33 regardless of statements made by the seller is, however, rejected. Thus, if the offer of examination is accompanied
34 by words as to their merchantability or specific attributes and the buyer indicates clearly that he is relying on those
35 words rather than on his examination, they may give rise to an "express" warranty. In such case the question is
36 one of fact as to whether a warranty of merchantability has been expressly incorporated in the agreement.
37 Disclaimer of such an express warranty is governed by subsection (a).

38 The particular licensee's skill and the normal method of examining information in the
39 circumstances determine what defects are excluded by the examination. A failure to notice defects which are
40 obvious cannot excuse the licensee. However, an examination under circumstances which do not permit extensive
41 testing would not exclude defects that could be ascertained only by such testing. A merchant licensee examining a
42 product in its own field will be held to have assumed the risk as to all defects which a merchant in the field ought
43 to observe, while a non-merchant licensee will be held to have assumed the risk only for such defects as an
44 ordinary person might be expected to observe.

45 *c. Course of Dealing, etc.* Subsection (e) is from original Article 2. It permits disclaimer
46 or other elimination of implied warranties by course of performance, course of dealing or usage of trade. It is
47 consistent with the U.C.C. concept of practical construction of contracts established under Article 2 and continued
48 in this article.

49 *d. Detailed Specifications.* If a licensee gives precise and complete specifications, this is a
50 frequent circumstances by which the implied performance warranties may be excluded. The warranty of fitness
51 will not normally apply because there is usually no reliance on the licensor. The warranty of merchantability in
52 such a transaction must be considered in connection with Section 2B-408 on cumulation and conflict of warranties.
53 As in Article 2, in the case of an inconsistency, the implied warranty of merchantability is displaced by any express
54 warranty that the information will conform to the specifications. Thus, if the licensee gives detailed specification
55 as to the information, neither the implied warranty of fitness nor the implied warranty of merchantability normally

1 will apply unless consistent with the specifications.

2

3

SECTION 2B-407. MODIFICATION OF COMPUTER PROGRAM. A licensee

4

that modifies a copy of a computer program, other than by using a capability of the program

5

intended for that purpose in the ordinary course, does not invalidate any warranty regarding

6

performance of an unmodified copy; but does invalidate any warranties, express or implied,

7

regarding performance of the modified copy. A modification occurs if a licensee alters code in,

8

deletes code from, or adds code to the computer program.

9

Definitional Cross References.

10

"Computer program". Section 2B-102. "Copy". Section 2B-102. "Licensee". Section 2B-102.

11

Reporter's Notes:

12

1. *Scope of Section.* This section deals with the effect of modifications in computer program code on the continued existence of performance warranties that might extend to the modified program. The rule applies only to the modified copy. If the defect existed in the unmodified copy, the modifications have no effect. Modifications other than changes made using an aspect of the program intended for that purpose eliminate any performance warranties extending to the modified copy. This applies only to warranties related to the performance of software. It does not apply to title and non-infringement warranties.

18

The basis for the rule in this section lies in the fact that because of the complexity of software systems, changes may cause unanticipated and uncertain results. The complexity of software means that it will often not be possible to prove to what extent a change in one aspect of a program altered its performance as to other aspects.

22

2. *Application.* The section voids the warranties unless the agreement indicates that modification does not alter performance warranties. The section covers cases where the licensee makes changes that are not part of the program options. Thus, if a user employs the built-in capacity of a word processing program to tailor a menu of options suited to the end user's use, this section does not apply. If, on the other hand, the end user modifies code in a way not made available in the program options, that modification voids any performance warranties as to the altered copy.

28

This section does not apply where the parties jointly work on development of a program, with each being authorized by the agreement to change code created by the other or created by both parties. Who constitutes the licensor in such cases is not clear, but the joint project characteristic takes the case out of this section. What warranties arise in the joint development context is determined by whose is the licensor and by the agreement of the parties, which agreement is defined and construed in light of the circumstances of the transaction, including the course of dealing and usage of trade.

34

35

SECTION 2B-408. CUMULATION AND CONFLICT OF WARRANTIES.

36

Warranties whether express or implied shall be construed as consistent with each other and as

37

cumulative, but if this construction is unreasonable, the intention of the parties determines which

38

warranty is dominant. In ascertaining that intention, the following rules apply:

39

(1) Exact or technical specifications displace an inconsistent sample or model or general

40

language of description.

1 (2) A sample displaces inconsistent general language of description.

2 (3) Express warranties displace inconsistent implied warranties other than an implied
3 warranty under Section 2B-405(a).

4 **Uniform Law Source:** § 2-317.

5 **Definitional Cross Reference.**

6 "Party": Section 1-102.

7 **Reporter's Note:** This section follows original Article 2.

8

9 **SECTION 2B-409. THIRD-PARTY BENEFICIARIES OF WARRANTY.**

10 (a) Except for published informational content, a warranty to a licensee extends to
11 persons for whose benefit the licensor intends to supply the information or informational rights
12 and which rightfully use the information in a transaction or application of a kind in which the
13 licensor intends the information to be used.

14 (b) A warranty to a consumer extends to each individual consumer in the licensee's
15 immediate family or household if the individual's use was reasonably expected by the licensor.

16 (c) A contractual term that excludes or limits third-party beneficiaries is effective to
17 exclude or limit a contractual obligation or contract liability to third persons except individuals
18 described in subsection (b).

19 (d) A disclaimer or modification of a warranty or remedy which is effective against the
20 licensee is also effective against a-third persons under this section.

21 **Definitional Cross References.**

22 "Consumer transaction": Section 2B-102. "Information": Section 2B-102. "Licensee": Section 2B-102.
23 "Licensor": Section 2B-102. "Party": Section 1-201. "Person": Section 1-201. "Published informational
24 content": Section 2B-102. "Remedy": Section 1-201. "Rights": Section 1-201. "Term": Section 1-201.

25 **Reporter's Notes:**

26 1. *Scope of the Section.* This section utilizes third-party beneficiary concepts based on the contract
27 law theory of "intended beneficiary" and on the *Restatement (Second) of Torts* § 552 dealing with the scope of
28 liability to third parties for a provider of information. It expands both where they apply to uses within the
29 household of the licensee. The section does not address products liability law, leaving that law and other forms of
30 tort law for development by the courts.

31 2. *Liability to Third Parties.* Dealing with an informational content product, the California
32 Supreme Court in *Bily v. Arthur Young & Co.*, 3 Cal.4th 370, 11 Cal. Rptr. 2d 51, 834 P2d 745 (1992),
33 commented:

34 By confining what might otherwise be unlimited liability to those persons whom the engagement is
35 designed to benefit, the Restatement rule requires that the supplier of information have notice of potential

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53

third party claims, thereby allowing it to ascertain the potential scope of its liability and make rational decisions regarding the undertaking.

To impose liability under contract-related theories, the information provider must have known of and clearly intended to have an effect on third parties. This is a third party beneficiary concept and requires a conscious assumption of risk or responsibility for particular third parties. Even within that standard, courts should not be aggressive in finding the requisite intent.

All of this relates to the unique role of information in our culture and to the uniquely difficult nature of proving a causal connection between a release of information and harmful effects. The cases and this section also reflect sensitivity to the risk that placing excessive liability exposure on information providers without their express undertaking may chill the willingness of those providers to disseminate information.

3. *Product Liability Law.* This Section does not deal with products liability issues. It neither expands nor restricts tort concepts that might apply for third party risk. Article 2B leaves development or non-development of any appropriate liability doctrine to common law courts. Indeed, few courts impose third party tort liability in transactions involving information. The *Restatement (Third) on Products Liability*, recognizing this, notes that informational content is not a product for that law. The only reported cases that impose product liability on information involve air flight charts. The cases analogized the technical charts to a compass or similar, physical instrument. These cases have not been followed in other contexts. Most courts specifically decline to treat information content as a product, including the Ninth Circuit, which decided two of the air flight chart cases, but later commented that public policy accepts the idea that information once placed in public moves freely and that the originator does not owe obligations to those remote parties who obtain it. *Winter v. G. P. Putnam's Sons*, 938 F.2d 1033 (9th Cir. 1991); *Berkert v. Petrol Plus of Naugatuck*, 216 Conn. 65, 579 A.2d 26 (Conn. 1990).

While there may be a different policy for software embedded in tangible products, this article does not deal with embedded software. Section 2B-104. Contract issues regarding the software that operates the brakes in an automobile sold to a consumer fall within Article 2.

4. *Intended Effect Required.* Subsection (a) derives from and should be interpreted in light of both the contract law concept of "intended beneficiary" and the concept in the *Restatement (Second) of Torts* § 552. In both instances, liability is restricted to intended third parties and those in a special relationship with the information provider. Intention requires more than that the person be within a general category of those who may use the information (.e.g., all readers). There must be a closer and more clearly known connection to the particular third party. The liability covers use in transactions that the provider of information intended to influence. The section also must be considered in light of the scope of warranties under this article which create no implied warranty of accuracy pertaining to published informational content.

Illustration: LR contracts for publication of a text on chemical interactions. Publisher obtains an express warranty that LR exercised reasonable care in researching. Publisher distributes the text to the general public. Some data are incorrect. Neither Publisher (which makes no warranty for published information), nor LR (excluded under (a)) makes a warranty to a general buyer of the book.

5. *Household and Family Use.* Subsection (b) modifies intended beneficiary concepts to per se include the family of an individual, consumer licensee. This covers both personal injury and economic losses and applies to consumer use by the indicated persons. To apply, the use by the family members must be authorized under the license and the licensee must be an individual (with a family), not a corporation. The section assumes that the licensor had some reason to anticipate that the information would be used in the licensee's household. Thus, the mere fact that a household member in fact uses a commercial data compression system licensed to a professional does not extend the warranty to the individual consumer in that person's household. On the other hand, the provider of mass-market word processing software might reasonably expect acquisition of it for use of the software at home. Ordinarily, for this rule to apply, the software must be provided in a consumer transaction or be such as is commonly used for consumer purposes.

6. *Limitation by Contract.* The policy adopted here focuses on the information provider's original intent with respect to third parties. Subsections (c) and (d) flow from the fact that the basis of this section lies in beneficiary status, rather than product liability. A disclaimer or a statement excluding intent to effect third parties excludes liability under this section. This follows current law. *Rosenstein v. Standard and Poor's Corp.*, 636 N.E.2d 898 (Ill. App. 1993) applied a variation of this rule in the case of an information product.

PART 5

1 available in a manner consistent with contract terms or industry.
2 a. *General Standards of Availability.* As indicated in subsection (a)(3), availability is
3 subject to contractual specification, but in the absence of contract terms, the appropriate reference is to general
4 standards of the industry involving the particular type of transaction. Thus, a contract involving access to a news
5 and information service would have different accessibility expectations than would a contract to provide remote
6 access to systems for processing air traffic control data. See *Reuters Ltd. v. UPI, Inc.*, 903 F.2d 904 (2d Cir. 1990);
7 *Kaplan v. Cablevision of Pa., Inc.*, 448 Pa. Super. 306, 671 A.2d 716 (Pa. Super. 1996).
8 b. *Content Changes.* The access agreement does not bind the provider of access to making
9 available particular information unless the express contract terms require this. Access is granted to the
10 information or other resources provided as they exist at the time of the particular access. Databases may be added,
11 modified or deleted consistent with this core obligation.
12 4. *Use of Received Information.* The access contract may or may not contain provisions that restrict
13 use of information obtained through the access. If there are no restrictions provided in the agreement, subsection
14 (a)(2) indicates that the information is received on an unrestricted basis, subject only to intellectual property rights
15 and any separate agreement concerning that information. For example, if an access contract merely enables access
16 to news articles, but does not limit their use by the licensee, no limitation exists other than under copyright law.
17 In contrast, if a transaction allowing access or a separate agreement establish conditions or
18 limitations on the use of the information obtained through the access, those license terms would be governed under
19 Article 2B. They are interpreted and enforced pursuant to other provisions of this article and, of course, the terms
20 of the agreement itself. Once the information is received by the licensee, however, it is ordinarily no longer
21 appropriate to construe the relationship as an access contract, but rather, it is simply a license. For example, if
22 licensee uses the access provided by its contract with ABC Corporation to acquire a copy of a spreadsheet program,
23 when the program is received by the licensee, the rights and remedies of the parties with respect to use of the
24 program are governed by the agreement with respect to that program and, in the absence of agreed terms, by the
25 default rules of this article regarding software licenses. As to the software, the relationship ceased to be an access
26 contract when the software was received by the licensee. Of course, the terms of the license may be found in the
27 agreement establishing the access contract or in a separate agreement concerning the licensed information.
28 The restrictions that might arise are not necessarily based on creation of a license. In some cases,
29 a mere copyright notice may adequately restrict the right to use the information obtained through the on-line
30 access. *Storm Impact, Inc. v. Software of the Month Club*, 1998 WL 456572 (N.D. Ill. 1998) (On-screen limitation
31 precluding commercial use of software enforced and resulting use infringed; court did not clarify whether the
32 notice was a license or merely limited permission granted by posting the software on the Internet).
33

34 SECTION 2B-616. CORRECTION AND SUPPORT AGREEMENTS.

35 (a) If a person agrees to correct performance problems or provide similar services with
36 respect to information other than as an effort to cure its own breach of contract, the following
37 rules apply:

38 (1) Except as otherwise provided in paragraph (2), the person:

39 (A) shall perform at a time and, place and in a manner consistent with the
40 express terms of the agreement and, to the extent not stated in ~~dealt with by~~ the express terms, at
41 a time and, ~~place~~ and in a manner that is reasonable in light of ordinary standards of the business,
42 trade, or industry; and

43 (B) does not undertake that its services will correct all performance

1 problems unless the agreement expressly so provides.

2 (2) If the services are provided by a licensor of the information as part of a limited
3 remedy, the licensor undertakes that its performance will provide the licensee with information
4 that conforms to the agreement to which the limited remedy applies.

5 (b) A licensor is not required to provide instruction or other support for the licensee's use
6 of information or access. A person that agrees to provide support shall make the support
7 available in a manner and with a quality consistent with the express terms of the support
8 agreement and, to the extent not stated in the dealt with by express terms, at a time and place and
9 in a manner that is reasonable in light of ordinary standards of the business, trade, or industry.

10 Uniform Law Source: Restatement (Second) of Torts § 299A.

11 **Definitional Cross Reference:**

12 "Agreement": Section 1-201. "Contract": Section 1-201. "Information": Section 2B-102. "Licensee": Section 2B-
13 102. "Licensor": Section 2B-102. "Person": Section 2B-102. "Remedy": Section 1-201. "Term": Section 1-201.

14 **Reporter's Notes:**

15 1. *Scope of the Section.* This section provides default rules regarding contracts to correct errors or
16 to provide support in use of information. A support agreement is an agreement to make available advisory or
17 consulting services relating to the use of the information. The default rules do not apply if the parties have
18 otherwise agreed. Agreement altering these terms does not depend on express terms of a record, but can be found
19 or inferred from the circumstances surrounding the contracting, applicable usage of the trades, in course of dealing
20 and the like.

21 2. *Nature of the Error Correction Obligation.* Obligations to correct performance problems are
22 different from an obligation to provide updates or new versions of software to remedy warranty breaches. In
23 modern practice, contracts to provide updates are a source of revenue for software providers. The reference to error
24 correction covers contracts where, for example, a vendor agrees to be available to come on site and correct or
25 attempt to correct problems in the software for a fee. This is a services contract. An agreement to provide updates
26 or new versions, on the other hand, is more in the nature of an installment contract calling for deliveries as new
27 versions of the software are developed and made available for general distribution. While the new versions often
28 cure problems in earlier versions and the two types of contracts overlap, the update arrangement deals with new
29 products. This article makes no attempt to set standards by which this distinction can be made in fact, but courts
30 faced with the issue must necessarily refer to the terms of the agreement of the parties and general industry
31 standards.

32 3. *Services Obligation.* Most agreements to correct problems are services contracts. In most cases,
33 the obligation is as stated in subsection (a)(1). The obligation parallels the obligation that any services provider
34 undertakes: a duty to act consistent with the standards of the business to complete the task. A services provider
35 does not guaranty that its services yield a perfect result. The standard measures a party's performance by reference
36 to standards of the relevant trade or industry.

37 4. *Services in Lieu of Warranty.* Subsection (a)(2) recognizes an alternative formulation of the
38 provider's obligations in contracts where the promisor agrees to a particular outcome. This obligation arises if the
39 repair obligation is part of a limited remedy in lieu of a warranty. The prototype is the "replace or repair" warranty.
40 The obligation to correct errors in that context is to complete a product that conforms to the contract. What
41 performance conforms to the contract, of court, hinges on the terms of that agreement as interpreted in light of
42 usage of trade, course of performance and the like. If the services performance fails to yield a conforming product,
43 what remedy is available depends on other rules in this article, such as the conditions for cancellation and rules on

1 perfect tender or substantial performance.

2 5. *Support Agreements.* Subsection (b) provides a default rule regarding support agreements. As a
3 form of services contract, the appropriate standard is an obligation consistent with reasonable standards of the
4 industry.

5

6 SECTION 2B-617. CONTRACTS INVOLVING PUBLISHERS, DEALERS, AND

7 END USERS.

8 (a) In this section:

9 (1) "Dealer" means a merchant licensee that receives information directly or
10 indirectly from a licensor for sale or license to end users.

11 (2) "End user" means a licensee that acquires a copy of the information from a
12 dealer by delivery on a physical medium for the licensee's own use and not for sale, license,
13 transmission to third parties, or for public display or performance for a fee.

14 (3) "Publisher" means a licensor, other than a dealer, that offers a license to an end
15 user with respect to information distributed to the end user by a dealer.

16 (b) In a contract between a dealer and an end user, if the end user's right to use the
17 information or informational rights is subject to a license from the publisher and there was no
18 opportunity to review the license before the end user became obligated to pay the dealer, the
19 following rules apply:

20 (1) The contract between the end user and the dealer is conditioned on the end
21 user's agreement to the publisher's license.

22 (2) If the end user does not agree, by manifesting assent or otherwise, to the terms
23 of the publisher's license, the end user has a right to a refund on return of the information to the
24 dealer. A right to a refund under this paragraph is a return for purposes of Sections 2B-112 and
25 2B-208.

26 (3) The dealer is not bound by the terms, and does not receive the benefits, of an
27 agreement between the publisher and the end user unless the dealer and end user adopt those

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

Transition Notes

1. Further efforts to conform this definition with 2B-102(a)(12) are required. See Revised 1-201(11).

2. The Drafting Committee agreed that there should be a "safe harbor" for conspicuous and that the safe harbor should vary depending upon the medium used in the record. Thus, sub (B) proposes a safe harbor for a written record and sub (c) proposes a safe harbor for an electronic record.

Questions to be resolved: (1) Should the definition be the same for Articles 2, 2A and 2B? (2) If so, what is the better definition? (3) Should a common definition for all be in Article 1?

SECTION 2-103. SCOPE.

(a) This article applies to transactions in goods, including remedial promises.

Alternative A [Article 9]

[(b) If a transaction involves both goods and software, this article applies to the goods and not the software. However, if goods contain software embedded in the goods in such a manner that the software is customarily considered to be part of the goods or that by becoming the owner of the goods, the person acquires a right to use the software in connection with the goods, this article applies to both the goods and the software.]

Alternative B [derived from Article 2B]

[(b) If a transaction involves a copy of computer information that is contained in and sold as part of goods, the following rules apply:

(1) this article applies to the goods; and

(2) this article applies to a copy of the computer information unless [the copy of the computer information is separately licensed and];

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

1 (B) the predominate purpose of the transaction is to give the purchaser of
2 the goods access to or use of the computer information.]

3 (c) Except as otherwise provided in subsection (b), to the extent that another article of
4 [the Uniform Commercial Code] applies to a transaction in goods, this article does not apply to
5 [the part of the transaction governed solely by the other article] [the subject matter or related
6 rights and remedies governed by the other article].

7 (d) This article does not apply to a foreign exchange transaction.

8 **Comments**

9 1. **Source.** Subsection (a) follows the first clause of former 2-102 except that the phrase
10 "Unless the context otherwise requires" is deleted. Subsection (b), which is derived from 9-
11 102(a)(44), is new. Subsection (c) amplifies the second clause of former 2-102. Subsection (d) is
12 new.

13 2. **Transactions in goods.** The phrase "transactions in goods" in subsection (a) usually
14 means a contract for the sale of goods, particularly in sections where the word "contract" or the
15 phrase "contract for sale" are used. In sections where those words are not used, "transaction"
16 does not include a lease of goods, see Article 2A, or a security interest in goods, see Article 9,
17 but could include a contract where both goods and services are provided, such as a contract to
18 deliver and install goods. When Article 2 applies to mixed goods and service transactions is left
19 for judicial inclusion or exclusion under the "predominant purpose" test, where factors such as
20 the language of the contract, the usual business of the seller or supplier, and the relative cost of
21 the goods and the services and whether they are segregated assist to determine whether a sale of
22 goods predominates. See, e.g, *Princess Cruises, Inc. v. General Electric Co.*, 143 F.3d 828 (4th
23 Cir. 1998), reviewing the cases and applying the test. If goods predominate, the transaction is
24 treated as a contract for sale and is within the scope of Article 2.

25 A "transaction in goods" could include a bailment or consignment of goods. These
26 transactions are not within the scope of Article 2. Article 2, however, may be extended by
27 analogy to transactions in goods not specifically covered.

28 3. **Remedial promises.** Article 2 does apply to remedial promises made by a seller in a
29 transaction in goods. 2-102(2). Thus, if a seller makes and breaches a remedial promise, Article
30 2 governs enforcement by the buyer. See 2-408(b)(2), 2-408(f), 2-409(a), 2-409(c), 2-409(d), 2-
31 810(a)(3), 2-814(b)(3), and 2-827(c).

1 4. Transactions involving goods and [software].

2 Alternative A to Subsection (b) follows 9-102(a)(44).

3 Alternative B to Subsection (b) is derived from Article 2B.

4
5 Both definitions are under review.

6 The enactment of Article 2B should help to end recurring disputes over whether contracts
7 to develop or to license software should be treated as “transactions in goods” for purposes of
8 Article 2. See, e.g., *Micro Data Systems, Inc. v. Dharma Systems, Inc.*, 148 F.3d 649 (7th Cir.
9 1998). They are not.

10 5. Overlaps with other UCC articles. Subsection (c) is new and replaces the language
11 in former 2-102 that Article 2 “does not apply to any transaction which although in the form of
12 an unconditional contract to sell or present sale is intended to operate only as a secured
13 transaction.” This language, which applied to “either-or” transactions, did not deal with cases
14 where two or more articles applied to the same transaction.

15 There is no tension between articles if, for example, the transaction is a contract for sale
16 and no security interest is created in the goods or if the transaction is exclusively a security
17 agreement. Similarly, if the transaction is a “true lease” rather than a sale of goods or a secured
18 transaction, Article 2A alone applies.

19 In a contract for sale, the most likely overlap is with Article 9. The seller, the buyer, or
20 some third person may create a security interest in the goods sold or a security interest may arise
21 under Article 2. In these cases, Article 9 not Article 2 applies to the creation, perfection, priority
22 and enforcement of the security interest. For example, a security interest arising when the seller
23 ships under reservation, 2-604, is subject to Article 9, but 9-113 {9-110} expressly refers some
24 aspects of perfection and enforcement back to Article 2.

25 In cases where Article 2 gives the seller or buyer interests in the goods that are not
26 security interests, however, Article 2 rather than Article 9 governs the rights and remedies
27 between seller and buyer. These rights, however, may be subject to security interests in the same
28 goods perfected under Article 9 by third persons. For example, a reclaiming seller under 2-
29 816(b) is subject to the rights of a good faith purchaser for value, including a secured party,
30 whose rights vest before the seller takes possession. 2-816(c).

31 [If payment is by letter of credit, 2-308 and 2-605 deal with the duty of the buyer to
32 provide and the effect of furnishing or not of the letter of credit, but Article 5 defines the critical
33 terms and covers all aspects of the transaction until the letter of credit is paid or dishonored.]

34 6. Foreign exchange transactions. Subsection (d), which is new, excludes “foreign

1 exchange transactions” from the scope of Article 2. Although a currency exchange is a sale of
2 goods, i.e., a swap, see 2-301(a), an exchange where delivery is “through funds transfer, book
3 entry accounting, or other form of payment order, or other agreed means to transfer a credit
4 balance” is not governed by Article 2. Rather, Article 4A or other applicable federal law applies.
5 2-102(a)(21). On the other hand, if the parties agree to a forward transaction where, ultimately,
6 dollars are to be physically delivered in exchange for the delivery of Euros, the transaction is not
7 within the exclusion and Article 2 applies.

8 **7. International sales.** CISG applies to “contracts of sale of goods” where the
9 jurisdictional requirements of the Convention are satisfied. Art. 1(1). Article 3 excludes
10 transactions where a party who orders goods to be manufacturer or produced supplies a
11 “substantial part of the materials necessary for such manufacture or production,” Art. 3(1), or
12 where the “preponderant part” of the obligation of the party furnishing goods “consists in the
13 supply of labour or other services.” Art. 3(2).

14 CISG does not apply to sales of consumer goods, certain obligations to pay money,
15 “ships, vessels, hovercraft or aircraft,” and electricity. Art. 2.

16 **Cross References:**

17 **Definitional Cross References:**

18 **SECTION 2-104. TRANSACTION SUBJECT TO OTHER LAW.**

19 (a) A transaction subject to this article is also subject to:

20 (1) [list any certificate of title statutes covering automobiles, trailers, mobile
21 homes, boats, farm tractors, or the like], except as to the rights of a buyer in the ordinary course
22 of business under Section 2-504(c) whose rights arise before a certificate of title covering the
23 goods is effective in the name of any other buyer;

24 (2) any applicable law that establishes a different rule for consumers; or

25 (3) any other law of this State to which the subject matter of this article is subject,
26 such as laws dealing with:

27 (A) the sale of agricultural products;

28 (B) the transfer of blood, blood products, human tissues, and organs;

1 6. Statute of limitations. Subsection (d) states that a cause of action for breach of
2 warranty of title or against infringement accrues for purposes of the statute of limitations as
3 determined under 2-814(c). The accrual time is when the buyer "discovers or should have
4 discovered the breach" not when the goods are tendered. Thus, the buyer has four years from
5 that discovery to bring a law suit. 2-814(a). No tolling period is imposed. Thus, if the buyer
6 should have first discovered the breach 10 years after delivery, the cause of action accrues then
7 and the buyer still has 4 years to bring suit. On this issue, no distinction is drawn between the
8 warranty of title and the warranty against infringement.

9 Without subsection (d), a cause of action for breach of warranty under subsection (a)
10 would accrue when the breach occurred even though the plaintiff did not have knowledge of the
11 breach. 2-814(b)(1). Under the Uniform Sales Act the statute ran from the time of delivery or
12 when quiet possession was disturbed. See *Menzel v. List*, 246 N.E.2d 742 (N.Y. 1969). Former
13 Article 2 did not impose a warranty of quiet possession. Thus, if the warranty was breached
14 upon tender of delivery but the owner did not replevy the goods until five years later, the statute
15 of limitations had run unless the seller made an express warranty explicitly extending to future
16 performance. Some courts have stretched to achieve this result. See *Balog v. Center Art*
17 *Gallery-Hawaii, Inc.*, 745 F. Supp. 1556 (D.Haw. 1990)(warranty that art work "genuine"
18 explicitly extended to future performance). Subsection (d) resolves this problem.

19 7. International sales. CISG Art. 41 provides simply that the seller "must deliver goods
20 which are free from any right or claim of a third party, unless the buyer agreed to take the goods
21 subject to the right or claim." Art. 42(1), a more complex provision, gives the buyer some
22 protection against goods delivered by the seller which are subject to claims of a third party
23 "based on industrial property or other intellectual property" if the seller "knew or could not have
24 been unaware" of the claim and the claim is based on the law of a State where the parties
25 contemplated that the goods would be used or resold. There is no obligation, however, if the
26 buyer "knew or could not have been unaware of the right or claim" or the buyer furnished
27 technical drawings or designs of the goods with which the seller complied. Art. 42(1).

28 SECTION 2-403. EXPRESS WARRANTY TO IMMEDIATE BUYER.

29 (a) Any representation made by the seller to the immediate buyer, including a
30 representation made in any medium of communication to the public, including advertising, which
31 relates to the goods and becomes part of the basis of the bargain creates an express warranty that
32 the goods will conform to the representation or, with respect to a sample or model, that the whole
33 of the goods will conform to the sample or model.

34 (b) It is not necessary to create an express warranty that the seller use formal words such

1 as "warranty" or "guaranty" or have a specific intention to make a warranty. However, a
2 representation merely of the value of the goods or an affirmation purporting to be merely the
3 seller's opinion or commendation of the goods does not create an express warranty under
4 subsection (a).

5 (c) A representation, including a representation made in any medium of communication
6 to the public, including advertising, which was made to the immediate buyer and which relates to
7 the goods becomes part of the basis of the bargain unless:

8 (1) the immediate buyer knew that the representation was not true;

9 (2) a reasonable person in the position of the immediate buyer would not believe
10 that the representation was part of the agreement; or

11 (3) in the case of a representation made in any medium of communication to the
12 public, including advertising, the immediate buyer did not know of the representation at the time
13 of the sale.

14 (d) A right of action for breach of warranty under this section accrues as provided under
15 Section 2-814.

16 **Comments**

17 1. Source: Former Section 2-313.

18 2. **Representations.** Under subsection (a), express warranty obligations are created
19 through representations, including advertising, made by sellers to immediate buyers that become
20 part of the basis of the bargain. The assumption is that the bargain between the parties is
21 otherwise enforceable as a contract and is subject to other requirements of this Article, such as
22 the statute of frauds, 2-201, and the parol evidence rule, 2-202, 2-406(a). For the extent to which
23 representations protect others besides the immediate buyer, see 2-408, 2-409.

24 The definition of representation in 2-401(5) includes a promise by the seller about the
25 quality or the performance of the goods. Thus, a seller may either affirm to the buyer that the

1 goods are X or may promise that the goods when delivered will be X, or may promise that the
2 goods will perform like X after delivery. All are terms in the contract, but are treated as
3 representations under Part 4.

4 3. **Puffing.** Subsection (b) follows 2-313(2) of current Article 2. Although preserving
5 the distinction between express warranty and puffing, subsection (b) does not provide a clear test
6 to distinguish the two. Presumably a buyer must first be reasonable under the circumstances in
7 believing that a representation rather than puffing was made, and then argue that the
8 representation became part of the basis of the bargain. See 2-408(b) and (c). However, a
9 representation or affirmation that is "puffing" is not a representation under subsection (a) that can
10 become part of the basis of the bargain.

11 There are a number of factors relevant to drawing the line between representations and
12 puffing. For example, the buyer might be unreasonable if the seller's representations taken in
13 context (1) were verbal rather than written, (2) were general rather than specific, (3) related to the
14 consequences of buying rather than the goods themselves, (4) were "hedged" in some way, (5)
15 related to experimental rather than standard goods, (6) concerned some aspects of the goods but
16 not a hidden or unexpected non-conformity, (7) were phrased in terms of opinion rather than fact,
17 or (8) were not capable of objective measurement. See *Federal Signal Corp. v. Safety Factors,*
18 *Inc.*, 886 P.2d 172 (Wash. 1994), where the court held that the trial court erred in not making
19 findings of fact where the seller stated that a new product was "better than" an earlier,
20 comparable model. See also, *Jordan v. Pascar, Inc.*, 37 F.3d 1181 (6th Cir. 1994)
21 (representations about strength of fiberglass roof which shattered and caused personal injury
22 when the truck rolled over were "puffing" as a matter of law). See also, Ivan L. Preston,
23 *Regulatory Positions Toward Advertising Puffery of the Uniform Commercial Code and the*
24 *Federal Trade Commission*, 16 J. Public Policy & Marketing 336 (1997).

25 4. **Basis of the bargain.** The "part of the basis of the bargain" requirement stated in 2-
26 313(1)(a) is retained in subsection (a). Unlike current 2-313, however, subsection (c) states when
27 a representation becomes part of the basis of the bargain and this should help to resolve the
28 disagreement over what that phrase means. See e.g., Holdych & Mann, *The Basis of the Bargain*
29 *Requirement: A Market and Economic Based Analysis of Express Warranties*, 45 De Paul L.
30 *Rev.* 781 (1996). There is no intention to change the interpretation of former 2-313 and the
31 comments that an affirmation of fact becomes part of the basis of the bargain unless one of the
32 exceptions in subsection (c) is established. *Buettner v. R.W. Martin & Sons, Inc.*, 47 F.3d 116
33 (4th Cir. 1995) (Virginia law); *Tomie Farms, Inc. v. J.R. Simplot, Inc.*, 862 P.2d 299 (Idaho
34 1993); *Torres v. Northwest Engineering Co.*, 949 P.2d 1004 (Hawaii App. 1998); *Weng v.*
35 *Allison*, 678 N.E.2d 1254 (Ill.App. 1997); *Keith v. Buchanan*, 220 Cal. Rptr. 392 (Cal. App.
36 1985)..

7 Subsection (c) states that a representation, including representations by advertising,
8 becomes part of the basis of the bargain unless one or more of the three conditions are satisfied.
9

1 Subsection (c)(1) excludes if the immediate buyer to whom the representation was made
2 knew that the representation was not true. If, however, the buyer had doubts about the truth or
3 accuracy of the representation but the seller continued to affirm, an express warranty can be
4 created. See *Rogath v. Siebenmann*, 129 F.3d 261 (2d Cir. 1997) (buyer's doubt about accuracy
5 of representation does not preclude express warranty).

6 Subsection (c)(2) states another defense, that a "reasonable person" in the position of the
7 immediate buyer would not believe that the representation was part of the agreement. Thus, the
8 buyer can know of and believe the representation but still be unreasonable in that belief. For
9 example, if the buyer brings its own expert to the bargaining table and relies upon her judgment
10 that the goods are of quality X, it is unlikely that the buyer was influenced by or relied upon the
11 seller's affirmation that the quality was Y rather than X. Such an assertion or belief, under the
12 circumstances, would be unreasonable.

13 **[Proposed Explanatory Comment**

14 A reasonable person in the position of the immediate buyer would not believe that a
15 seller's representation became part of the basis of the bargain if no such reasonable person
16 would have been influenced by or relied on the representation in entering the contract or
17 any modification thereof.]

18 Subsection (c)(3) states that when the immediate buyer claims an express warranty
19 created by advertising there is no express warranty if the immediate buyer did not know of the
20 representation at the time of the sale. This gives a bit more protection to sellers who represent
21 through advertising than when other representations are involved.

22 5. **Temporal issues.** "Agreement" is defined as the "bargain of the parties in fact." 1-
23 201(3). So "basis of the bargain" is another way of saying "basis of the agreement." Since
24 agreements can be made both before and after a contract is formed, there is no artificial time at
25 which an express warranty must be made. Thus, a representation, including those made by
26 advertising, made before or after contract formation can become part of the basis of the bargain.
27 If a representation is made after the contract is formed, the requirements for a modification in 2-
28 209(a) must be satisfied. See *Downie v. Abex Corp.*, 741 F.2d 1235 (10th Cir. 1984).]

29 6. When a cause of action accrues under this section for purposes of the statute of
30 limitations is stated in 2-814.

31 7. **International sales.** CISG covers express warranty problems with spare language that
32 does not mention the word "warranty." Article 35(1) provides that the seller "must deliver goods
33 which are of the quantity, quality and description required by the contract and which are
34 contained or packaged in the manner required by the contract." Article 35(2)(c) provides that
35 unless the parties have agreed otherwise, goods do not conform to the contract unless they
36 "possess the qualities of goods which the seller has held out to the buyer as a sample or model."

1 warranty of merchantability.

2 Note that the implied warranty of merchantability may be disclaimed or modified to the
3 extent provided in 2-406, and may be subordinated by an express warranty, see 2-407(3).
4 Moreover, certain transactions, such as the furnishing of blood or body parts, may be regulated
5 by so-called state "blood shield" statutes. See 2-104(a)(3).

6 2. **Content.** Subsection (b) follows 2-314(2) with the following changes: (a) The phrase
7 "agreed description" rather than "contract description" is used in (b)(1); (b) The phrase "goods of
8 that description" rather than "for which such goods" is used in (b)(3). This emphasizes the
9 importance of the agreed description in determining fitness for ordinary purposes; (c) The phrase
10 "or circumstances" is added after "the agreement" in (b)(5). The "circumstances" may indicate
11 to the seller that the buyer might be misled about the goods and require an adequate label; and
12 (d) The word "any" replaces "the" in the first line and the phrase "if any" is deleted.

13 Subsection (b) states the minimum standards of merchantability which are derived, in
14 large part, from the agreed description of the goods. These standards supplement 2-403(a),
15 where a description of the goods may be a representation that creates an express warranty. For
16 example, suppose that the seller describes the goods as a "3 horse power lawn mower that will
17 start on the first pull and cut grass up to five inches tall." More than a core description is
18 involved here. The seller represents the ease of starting and the capabilities of the mower. On
19 the other hand, suppose the agreed description is simply "power lawn mower" and there are no
20 other representations. If the power mower does not start on the first pull or will only cut grass up
21 to two inches tall, the buyer cannot rely on 2-403 for recovery and must fall back on 2-404.
22 Note, however, that many of the merchantability standards still overlap with representations that
23 could be express warranties under 2-403.

24 For the "power mower to be merchantable:

25 (a) It must pass without objection in the trade under the agreed description. Would sellers
26 and buyers in the trade and familiar with trade descriptions object to goods described as a power
27 mower that would not start on the first pull? See *Agoos Kid Co., Inc. v. Blumenthal Import*
28 *Corp.*, 184 N.E. 279 (Mass. 1933) (trade description under Uniform Sales Act).

29 (b) In a lot of 50 identical lawn mowers, it must be of "fair average quality" within the
30 description. Thus, if 49 lawn mowers of the same description started on five pulls or less and
31 one took 20 pulls, that "one" would, arguably, be unmerchantable.

32 (c) The goods must be fit for the "ordinary purposes for which goods of that description
33 are used." This is one of the most important and frequently invoked standards. Here, evidence of
34 ordinary purposes is required. What do goods described as a "power lawn mower" do and what
35 would a reasonable buyer expect it to do? A power mower that would not start in less than 20
36 pulls or would not cut an ordinary lawn or created a danger of injury to the operator might be

1 unmerchantable.

2 (d) If the agreement permits variations of kind or quality, the particular goods must be
3 within those variations. Thus, if a commercial buyer buys 20 power lawnmowers and the
4 agreement states that the seller can furnish three different makes and that all makes must start in
5 five pulls or less, a lawnmower of a different make or a lawnmower that won't start in less than
6 10 pulls is probably unmerchantable.

7 (e) The goods must be adequately contained, packaged or labeled as required by the
8 agreement or the circumstances.

9 (f) The goods must conform to any representation made on the container or label.

10 3. Subsection (c) follows 2-314(3). An implied warranty may arise from a course of
11 dealing or usage of trade.

12 **4. Personal injuries**

13
14 Suppose that an unmerchantable lawn mower caused personal injuries to the buyer, who
15 was operating the goods. Without more, the immediate buyer can sue the seller for breach of the
16 implied warranty of merchantability and recover for injury to person or property "proximately
17 resulting" from the breach. 2-806(2).

SI

18 This opportunity does not resolve the tension between warranty law and tort law where
19 goods cause damage to person or property. The primary source of that tension arises from
20 disagreement over whether the concept of defect in tort and the concept of merchantability in
21 Article 2 are coextensive where personal injuries are involved, i.e., if goods are merchantable
22 under warranty law can they still be defective under tort law and if goods are not defective under
23 tort law can they be unmerchantable under warranty law? The answer to both questions is yes
24 only if the contract standard for merchantability, e.g., reasonable expectations, and the tort
25 standard for defect are different. Even though the outcome under different standards will be the
26 same in most cases, i.e., unmerchantable goods are frequently defective and defective goods are
27 frequently unmerchantable, there are a few exceptions, especially where design defects are
28 involved. See *Castro v. QVC Network, Inc.*, 139 F.3d 114 (2d Cir. 1998) (goods not defective in
29 tort may be unmerchantable in warranty under New York law).

30 The tension between merchantability in warranty and defect in tort where personal
31 injuries or damage to property are involved should be resolved as follows:

32 **When recovery is sought for injury to person or property, whether goods are**
33 **merchantable is to be determined by applicable state products liability law.**

34 **When, however, a claim for injury to person or property is based on an implied**

1 warranty of fitness under Section 2-405 or an express warranty under Sections 2-
2 403 or 2-408, this Article determines whether an implied warranty of fitness or an
3 express warranty was made and breached, as well as what damages are recoverable
4 under Section 2-806.

5 To illustrate, suppose that the seller makes a representation about the safety of the lawn
6 mower that becomes part of the basis of the buyer's bargain. The buyer is injured when the gas
7 tank cracks and a fire breaks out. If the lawnmower without the representation is not defective
8 under applicable tort law, it is not unmerchantable under 2-404. On the other hand, if the
9 lawnmower did not conform to the representation about safety, the seller has made and breached
10 an express warranty and the buyer may sue under Article 2.

11 5. **International sales.** Article 35(2) of CISG provides that unless the parties have
12 agreed otherwise, goods do not conform with the contract unless they are "fit for the purposes for
13 which goods of the same description would ordinarily be used" or are adequately contained and
14 packaged. CISG, however, "does not apply to the liability of the seller for death or personal
15 injury caused by the goods to any person." Art. 5.
16

17 **SECTION 2-405. IMPLIED WARRANTY OF FITNESS FOR PARTICULAR**

18 **PURPOSE.** Subject to Section 2-406, if a seller at the time of contracting has reason to know
19 any particular purpose for which the goods are required and that the buyer is relying on the
20 seller's skill or judgment to select or furnish suitable goods, there is an implied warranty that the
21 goods are fit for that purpose.

22 **Comments**

23 1. **Source:** Follows former Section 2-315.

24 2. **Scope and content.** This section covers the case where the buyer has particular
25 purposes or needs for goods and there is no express warranty that the goods will meet those
26 purposes or the particular purposes are not ordinary purposes for which goods of that description
27 are used. The requirements, however, a somewhat exacting.

28 Although the seller need not be a merchant (any seller can make an implied warranty of
29 fitness) the seller at the time of contracting must have reason to know of any particular purpose
30 for which the goods are required. Normally, this purpose is communicated by the buyer to the
31 seller.

32 The seller at the time of contracting must also have reason to know that the buyer is

1 relying on the seller's skill or judgment to select or furnish suitable goods. Thus, if the buyer
2 furnishes detailed specifications for goods that satisfy particular purposes and asks the seller to
3 follow them, the buyer is not relying on the seller's skill and judgment and the seller has reason
4 to know it.

5 The buyer's particular and ordinary purpose usually are different. Goods that are
6 merchantable may not be fit for particular purposes. In some cases, a buyer may claim a breach of
7 the fitness warranty when the goods, in fact, are unmerchantable. In these cases, the elements
8 of both warranties must be properly plead and proved. See Van Wyck v. Norden Laboratories,
9 Inc., 345 N.W.2d 81 (Iowa 1984).

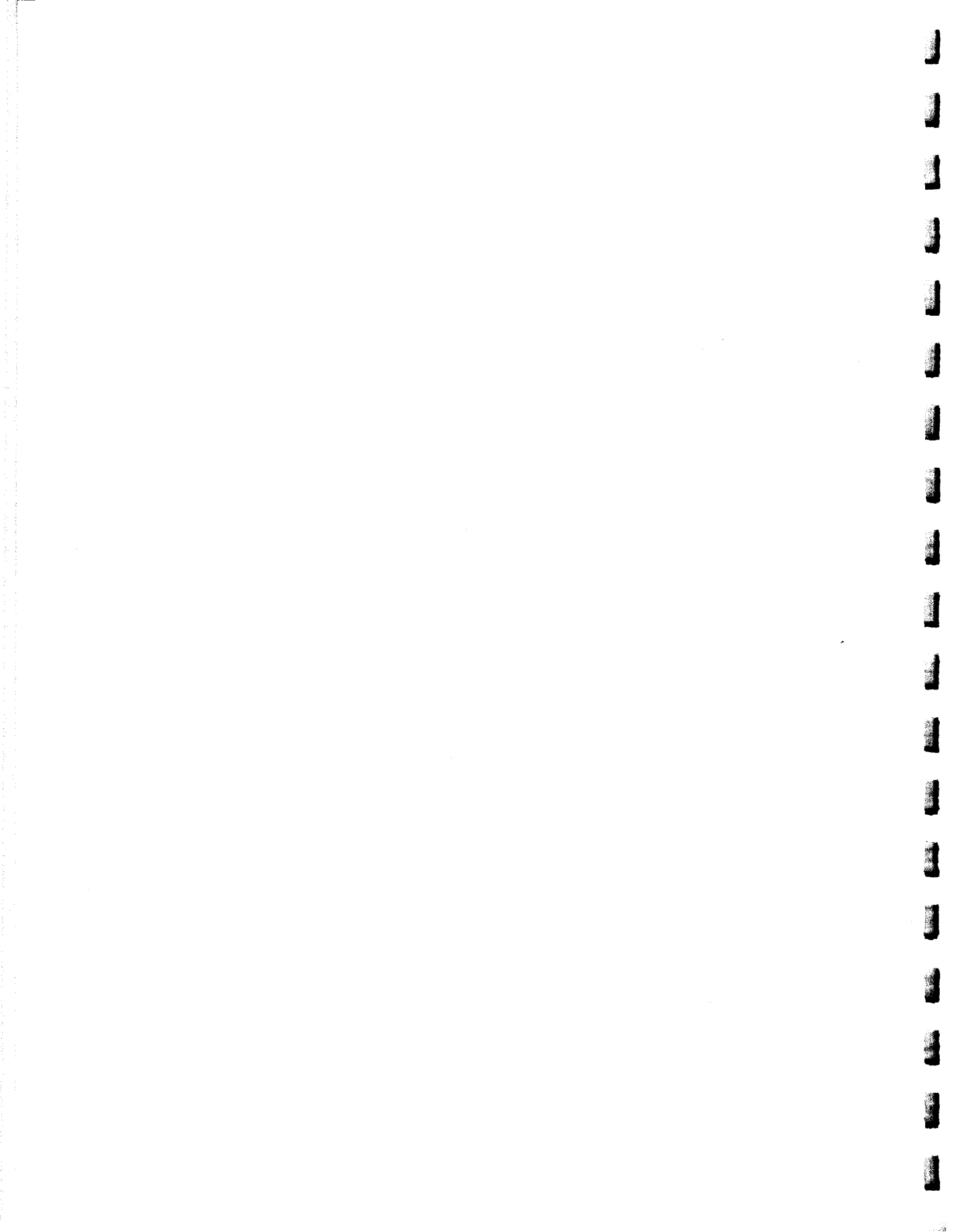
10 Finally, the implied warranty of fitness may be disclaimed under 2-406.

11 **Example.** S manufactures and sells iron products. B, a state conservation agent, wants to
12 purchase iron collars to attach the steel blade of a hoe to a wooden handle. The purpose of the
13 hoe is to plant pine seedlings and the strength of the collar required depends upon the type of soil
14 involved. Most collars will work in sandy or clay soil but a stronger collar and blade is required
15 in rocky conditions. After some discussion, S agreed to supply B with 2,000 "hoe dad" collars
16 for \$10 each. After delivery, B learned that the hoedads worked well in sandy and clay soil but
17 that 80% of the hoedads broke when used in rocky soil. On these facts, it is unlikely that S made
18 and breached a warranty: (1) There was no express warranty that the collars were fit for use in
19 rocky soil; (2) The collars were fit for the ordinary purposes for which the collars were used, i.e.,
20 sandy or clay soil; and (3) B did not reveal to S offely upon S to furnish goods that met the
21 particular purpose required, i.e., effective use in rocky soil.

22 2. CISG. Article 35(2)(b) provides that unless the parties have otherwise agreed, goods
23 do not conform with the contract unless they are "fit for any particular purpose expressly or
24 impliedly made known to the seller at the time of the conclusion of the contract, except where the
25 circumstances show that the buyer did not rely, or that it was unreasonable for him to rely, on the
26 seller's skill and judgement."

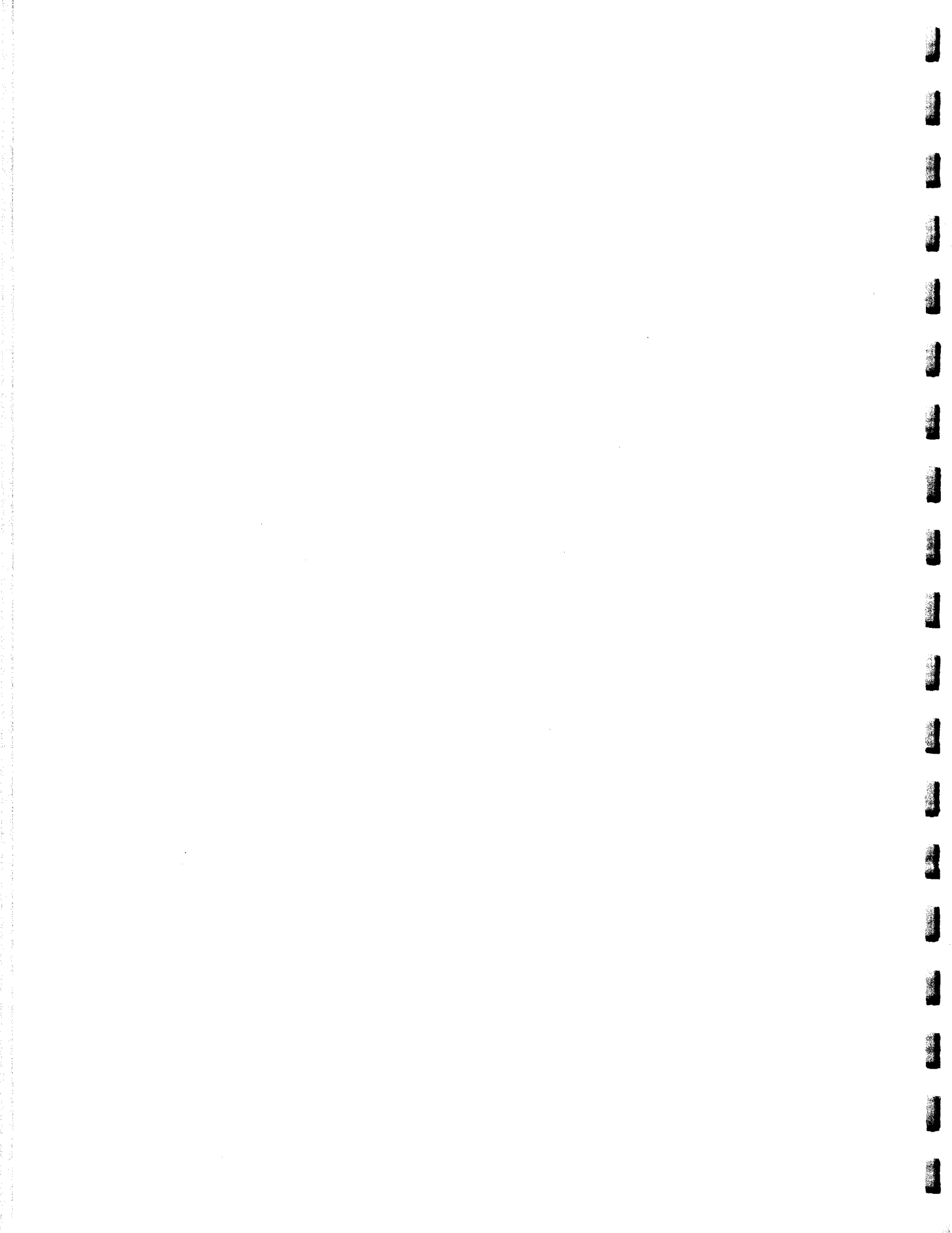
27 **SECTION 2-406. DISCLAIMER OR MODIFICATION OF WARRANTY.**

28 (a) Words or conduct relevant to the creation of an express warranty and words or
29 conduct tending to disclaim or modify an express warranty must be construed wherever
30 reasonable as consistent with each other. Subject to Section 2-202 with regard to parol or
31 extrinsic evidence, words or conduct disclaiming or modifying an express warranty are
32 ineffectiv inoperative [style] to the extent that this construction is unreasonable.



UPDATE ON LEGISLATION CONCERNING THE YEAR 2000

Jay E. Ingle
Jackson & Kelly
Lexington, Kentucky



UPDATE ON LEGISLATION CONCERNING THE YEAR 2000

TABLE OF CONTENTS

I. STATE EFFORTS AT LEGISLATION B-1

II. FEDERAL EFFORTS AT LEGISLATION B-2

III. ENACTED LEGISLATION B-3

A. Year 2000 Readiness And Disclosure Act B-3

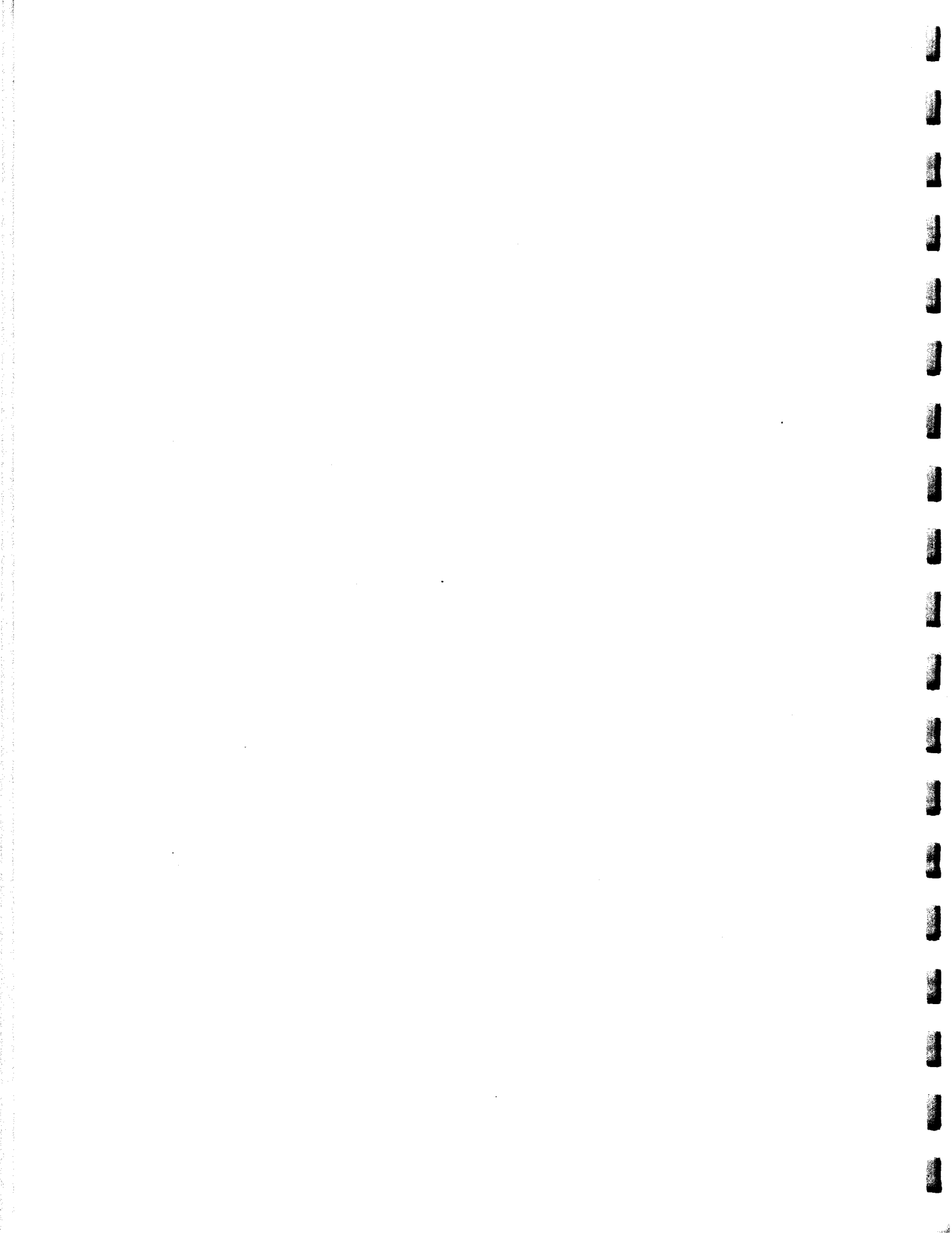
B. Small Business Year 2000 Readiness Act B-6

IV. PENDING FEDERAL LEGISLATION B-7

V. POTENTIAL FUTURE LEGISLATION B-12

EXHIBIT A: Year 2000 Information Disclosure Act B-15

EXHIBIT B: Small Business Year 2000 Readiness Act B-27



Y2K LEGISLATIVE UPDATE

With predictions of litigation costs of as much as one trillion dollars and images of volumes upon volumes of lawsuits crowding the courts, legislative efforts to cope with the Y2K problem have been plentiful at both the state and federal level. While some legislation has already been enacted, most is either pending or soon to be filed. Much of the legislation at the state level has focused on the exposure of state and local governments, while the federal effort has focused on limiting the liability of potential defendants. What follows is a general overview of the efforts to date.

I. State Efforts at Legislation

Many states have been quick to initiate legislation protecting both private businesses and state and local governments from liability for Y2K related issues. Most of the measures which afford protection to the private sector do so through a "good faith" defense, limitations on damages, and other means also seen in the federal proposals discussed later.

At the same time, many states are pushing litigation to protect the state itself. At least one attorney general has advised that current immunity protection would be sufficient to shield that attorney general's state from any Y2K liability exposure, but most state legislatures are undertaking an effort to pass new laws which specifically address

state and local government immunity for Y2K-related lawsuits.

Nevada was the first state to pass legislation addressing the liability of state government in 1997. Since then, at least six other states have passed legislation addressing liability of state government, including California, Florida, Georgia, Hawaii, South Dakota, and Virginia. Approximately another thirty states and the District of Columbia have some sort of legislation introduced which would curb the ability to seek damages from state or local governments. Some of these different efforts include complete immunity, damages limited to actual damages, immunity from punitive damages, and immunity from all actions except personal injury and death.

II. Federal Efforts at Legislation

The attempts at federal legislation regarding the litigation of Y2K-related suits has certainly been a hot topic of late. Five separate bills have been introduced in the Senate and House of Representatives which address the litigation aspects of Y2K failures. Even as this update was being drafted, Congress continues to battle over the key features of such a bill. As of May 3, 1999, none of these efforts had been passed by either house.

Legislation regarding litigation aspects has not been the only topic for Congress related to Y2K, however. Several bills relating to government preparedness and funding for particular agencies and commissions have been enacted. Two bills have already been

acted which address concerns of the private sector. Several more are possibly forthcoming in the next few months as well.

The following review of federal legislative efforts is broken down into three sections: i) enacted legislation; ii) pending legislation; and iii) potential future legislation. This review should cover the two bills already enacted, the handful of bills currently pending, and the possible forthcoming bills.

III. Enacted Legislation

To date, two Y2K bills dealing directly with the private sector have been enacted. The first, the Year 2000 Readiness and Disclosure Act, addresses the need for businesses to disclose their efforts at prevention and remediation without fear of exposure to liability. The second, the Small Business Year 2000 Readiness Act, provides means of assisting small businesses in their efforts to cure and cope with any Y2K failures.

A. Year 2000 Readiness and Disclosure Act

The Year 2000 Readiness and Disclosure Act, Senate Bill 2392, was signed into law by President Clinton on October 19, 1998. Its stated purpose is to promote the free disclosure and exchange of information regarding Y2K readiness. The Act was generally a response to the hesitancy of many businesses to respond to Y2K questionnaires out of

fear that they would only be exposing themselves to liability by any representations made in response to those questionnaires. The main effect of the Act is to prohibit Y2K readiness disclosure statements from being admissible to prove the truth of the matters asserted therein.

Section 4 of the Act expressly makes readiness disclosure statements inadmissible to prove the accuracy or truth of any year 2000 statement therein, with two exceptions. First, a readiness disclosure statement is admissible as the basis for a claim of anticipatory breach. Second, the court shall have discretion to admit the statement if it determines that the maker's use of the readiness disclosure statement amounts to bad faith or fraud or is otherwise beyond what is reasonable to effect the purposes of the Act.

The Act also addresses the standard for liability for providing false, misleading, and inaccurate Y2K statements. The maker is not liable for a false, misleading, or inaccurate statement unless a plaintiff establishes *by clear and convincing evidence* that

- (1) the year 2000 statement was material; and
- (2)(A) to the extent the year 2000 statement was not a republication, that the maker made the year 2000 statement--
 - (i) with actual knowledge that the year 2000 statement was false, inaccurate, or misleading;

(ii) with intent to deceive or mislead; or
(iii) with a reckless disregard as to the accuracy of
the year 2000 statement; or

(B) to the extent the year 2000 statement was a
republication, that the maker of the republication made the year
2000 statement--

(i) with actual knowledge that the year 2000 statement
was false, inaccurate, or misleading;

(ii) with intent to deceive or mislead; or

(iii) without notice in that year 2000 statement that--

(I) the maker has not verified the contents of the
republication; or

(II) the maker is not the source of the
republication and the republication is based on
information supplied by another person or entity
identified in that year 2000 statement or republication.

The Act also addresses the standard for defamation suits based on Y2K disclosure
statements. The maker of a disclosure statement is not liable for defamation unless, in
addition to all other elements for defamation under applicable law, the plaintiff
establishes *by clear and convincing evidence* that the statement was made with

knowledge that it was false or with reckless disregard as to its truth or falsity.

The Year 2000 Readiness and Disclosure Act also states that a disclosure statement will generally not be interpreted as an amendment to a contract or warranty unless allowed for by the contract itself or if made as part of a contract or amendment thereto. In addition, it provides for a Year 2000 Internet Website for posting readiness disclosure statements. Posting of such statements on the website is deemed as adequate notice of the statement in certain situations.

A copy of the Year 2000 Readiness and Disclosure Act is attached as **Exhibit A**.

B. Small Business Year 2000 Readiness Act

While the efforts of large corporations and government have garnered much of the attention regarding Y2K readiness, many commentators agree that it is the small business that it is the most at risk and the most likely to be unprepared. A small business often has very little surplus capital and must operate on a positive cash flow basis. As such, a Y2K failure has much greater consequences for a small company since it could literally destroy the company. At the same time, small companies also have fewer resources to use in addressing potential Y2K problems and, as a general rule, are far behind in preparation.

As a result, Congress enacted the Small Business Year 2000 Readiness Act, Senate Bill 314, to assist small businesses in fighting the Y2K battle. The Act directs the Small

Business Association to set up a limited-term loan guarantee program through December 31, 2000. The loan program will allow eligible small businesses to obtain additional funds from the SBA for use in addressing potential problems and to provide relief for substantial economic injuries which occur as a direct result of Y2K problems. The SBA is expected to guarantee approximately \$500 million dollars in loans through the end of the program.

Normally, SBA-guaranteed loans allow for 80% of capital for loans up to \$100,000 and 75% for loans in excess of \$100,000. Under the Act, the percentage of capital on SBA-guaranteed loans is raised to 90% on loans up to \$100,000 and 85 % in excess of \$100,000. It also allows the SBA to guarantee the total outstanding loans for a business up to one million dollars for Y2K, while the normal maximum is \$750,000.

A copy of the Small Business Year 2000 Readiness Act is attached as **Exhibit B**.

IV. Pending Federal Legislation

Five different bills have been introduced in Congress which address the litigation aspects of the Y2K problem. To date, none have been passed, although several have come very close over the last several weeks. The five proposed bills are as follows:

- The Y2K Act, Senate Bill 96 (McCain)
- Year 2000 Fairness and Responsibility Act, Senate Bill 461 (Hatch, Feinstein)

- Y2K Fairness in Litigation Act, Senate Bill 738 (Dodd)
- The Year 2000 Consumer Protection Act of 1999, House Bill 192 (Manzullo)
- Year 2000 Readiness and Responsibility Act , House Bill 775 (Davis-Moran)

Each of these bills has touched on the idea of easing the litigation burden on potential defendants and the court system through various means.

The bills as initially proposed all seem to agree on a waiting period before a claimant could file suit. The consensus seems to require notice to the potential defendant which allows the potential defendant thirty days to respond to the complaint and an additional sixty days to correct the problem. The bills also all seem to emphasize the use of alternative dispute resolution, either through voluntary or required mediation or arbitration.

Where the bills seem to differ is in weighing the protection for business against the needs of consumers. While most of the bills started with at least some form of cap on damages, the bill proposed by Senator Dodd, and backed by President Clinton at the time, contained no caps whatsoever. Others limit the amount of damages other than actual damages, limit punitive damages, and limit liability for individual officers and directors.

In addition, House Bill 775 proposed to limit attorneys' fees.

Over the last few weeks, the Senate has seen considerable debate and compromise in attempting to forge a bill which will garner enough votes to pass the Senate. On April 26, 1999, Senate Bill 96 came before the Senate for debate. Several of the key provisions of Senate Bill 96 as it went before the Senate included:

- 90 day cooling off period
- damages not recoverable where plaintiff could have avoided failure
- Punitives capped to \$250,000 unless fraud w/ intent to injure plaintiff
- Non-economic loss damages limited to 3 times actual loss or \$250,000, whichever is greater
- Non-economic loss damages limited to \$50,000 for businesses with fewer than 25 full-time employees and individuals with a net worth no greater than \$500,000
- a defendant could avoid liability for plaintiff's economic loss if it showed due diligence and reasonable care was taken to prevent or fix the Y2K problem
- Directors' and officers' liability limited to \$100,000 unless a material misstatement was made or information was withheld
- Federal and state governmental immunity from punitive damages
- All claims are treated as a breach of contract claim, regardless of how stated

- The Bill would not cover personal injury or wrongful death cases

Needless to say, the proposed bill sparked much heated debate. Much of the complaint set forth by Democrats was that the bill looked more like tort reform than a bill designed to reduce Y2K costs. Senator Dodd also continued his strong stance, and presumably the position of the White House, in opposing a bill with any form of caps whatsoever.

By the afternoon of Tuesday, April 27, 1999, key players in the Senate effort to craft a Y2K bill met behind closed doors in an attempt to find compromise. Included in the meetings were Sen. John McCain (R-Arizona), chief sponsor of Senate Bill 96; Sen. Orrin Hatch (R-Utah) and Sen. Dianne Feinstein (D-California), sponsors of Senate Bill 461; and Sen. Christopher Dodd (D-Connecticut), sponsor of Senate Bill 738, among others.

On Wednesday, April 28, 1999, it seemed as though a compromise had been reached. The compromise offered the following changes:

- eliminates punitive damage caps for businesses with more than 50 employees
- retains the punitive damage cap for businesses with fewer than 50 employees
- eliminates personal liability caps for officers and directors

- preserves state evidentiary standards for certain claims, such as fraud
- allows for proportional liability (rather than joint and several) to ensure that defendants will not pay for more than the damages for which they are responsible, with exceptions when a plaintiff has a modest net worth who cannot collect from one or more defendants and the defendants have intentionally injured the plaintiff

The Bill would continue to not cover personal injury and wrongful death claims, would not interfere with parties who have already agreed on Y2K terms and conditions, and would require mitigation of damages.

By Thursday, April 29, 1999, however, the compromise bill stalled. The bipartisan group which forged the compromise quickly became partisan again. The Bill was scheduled to come to the floor for approval, but a new debate arose as Senate Democrats suggested several amendments to the Bill. Republicans balked at the amendments stating that they were unrelated, criticizing most notably an amendment that would increase the minimum wage. Senators John Kerry (D-Massachusetts) and Charles Robb (D-Virginia) were also crafting an alternative bill which eliminates liability caps altogether. While the Clinton administration has threatened to veto Senate Bill 96, it apparently would endorse such an alternative bill with no liability caps.

While the Senate compromise locked up, the House began to take action again. Rep. Zoe Lofgren (D-California) offered a substitute bill to House Bill 775. The main difference would be that Lofgren's substitute would eliminate corporate and personal liability caps. Lofgren's substitute would apparently include the 90 day cooling off period, require pleading with specificity, and proportionate liability, among other provisions. The House was scheduled to resume debate on May 4, 1999. President Clinton has endorsed Lofgren's proposal while threatening to veto House Bill 775.

In summary, as of May 3, 1999, the concept of Y2K litigation legislation is a very real one, but the details of a final bill are sketchy. The key features could be ironed out soon and could greatly affect lawsuits brought for damages from Y2K failures.

V. Potential Future Legislation

At least two additional pieces of legislation are possibly forthcoming in the future months. First, the Department of Housing and Urban Development has suggested that it may seek additional funding and possibly legislation from Congress to aid local housing authorities and business partners. While the Department has reported that its own preparations are advancing smoothly, it has expressed concern that some local housing authorities may not have the resources for full preparation. The Department is also concerned with the level of readiness for many of the business partners on which the Department and local authorities rely.

Representative Tom Davis (R-Va.) has also publicly stated that he is drafting a bill to assist state and local governments in purchasing Y2K products and services. The bill, tentatively named the Year 2000 Compliance Assistance Act, would allow state and local governments to purchase such products and services through the multiple awards schedule administered by the General Service Administration's Federal Supply Service. Such an option would give state and local governments more flexibility through cooperative purchasing.

YEAR 2000 INFORMATION DISCLOSURE ACT

S. 2392 -- ENACTED AND SIGNED INTO LAW

105th Congress, Second Session

Date Introduced: 07/30/98

Version Date: 10/01/98

Version type: Enrolled (finally passed both houses)

Sponsor: Bennett R. (R-UT)

AN ACT

To encourage the disclosure and exchange of information about computer processing problems, solutions, test practices and test results, and related matters in connection with the transition to the year 2000.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Year 2000 Information and Readiness Disclosure Act".

SEC. 2. FINDINGS AND PURPOSES.

(a) **FINDINGS.**--Congress finds the following:

(1)(A) At least thousands but possibly millions of information technology computer systems, software programs, and semiconductors are not capable of recognizing certain dates in 1999 and after December 31, 1999, and will read dates in the year 2000 and thereafter as if those dates represent the year

1900 or thereafter or will fail to process those dates.

(B) The problem described in subparagraph (A) and resulting failures could incapacitate systems that are essential to the functioning of markets, commerce, consumer products, utilities, government, and safety and defense systems, in the United States and throughout the world.

(C) Reprogramming or replacing affected systems before the problem incapacitates essential systems is a matter of national and global interest.

(2) The prompt, candid, and thorough disclosure and exchange of information related to year 2000 readiness of entities, products, and services--

(A) would greatly enhance the ability of public and private entities to improve their year 2000 readiness; and

(B) is therefore a matter of national importance and a vital factor in minimizing any potential year 2000 related disruption to the Nation's economic well-being and security.

(3) Concern about the potential for legal liability associated with the disclosure and exchange of year 2000 readiness information is impeding the disclosure and exchange of such information.

(4) The capability to freely disseminate and exchange information relating to year 2000 readiness, solutions, test practices and test results, with the public and other entities without undue concern about litigation is critical to the ability of public and private entities to address year 2000 needs in a timely manner.

(5) The national interest will be served by uniform legal standards in connection with the disclosure and exchange of year 2000 readiness information that will promote disclosures and exchanges of such information in a timely fashion.

(b) PURPOSES.--Based upon the powers contained in article I, section 8, clause 3 of the Constitution of the United States, the purposes of this Act are--

(1) to promote the free disclosure and exchange of information related to year 2000 readiness;

(2) to assist consumers, small businesses, and local governments in effectively and rapidly responding to year 2000 problems; and

(3) to lessen burdens on interstate commerce by establishing certain uniform legal principles in connection with

the disclosure and exchange of information related to year 2000 readiness.

SEC. 3. DEFINITIONS.

In this Act:

(1) ANTITRUST LAWS.--The term "antitrust laws"--

(A) has the meaning given to it in subsection (a) of the first section of the Clayton Act (15 U.S.C. 12(a)), except that such term includes section 5 of the Federal Trade Commission Act (15 U.S.C. 45) to the extent such section 5 applies to unfair methods of competition; and

(B) includes any State law similar to the laws referred

to in subparagraph (A).

(2) **CONSUMER.**--The term "consumer" means an individual who acquires a consumer product for purposes other than resale.

(3) **CONSUMER PRODUCT.**--The term "consumer product" means any personal property or service which is normally used for personal, family, or household purposes.

(4) **COVERED ACTION.**--The term "covered action" means a civil action of any kind, whether arising under Federal or State law, except for an action brought by a Federal, State, or other public entity, agency, or authority acting in a regulatory, supervisory, or enforcement capacity.

(5) **MAKER.**--The term "maker" means each person or entity, including the United States or a State or political subdivision thereof, that--

(A) issues or publishes any year 2000 statement;

(B) develops or prepares any year 2000 statement; or

(C) assists in, contributes to, or reviews, reports or comments on during, or approves, or otherwise takes part in the preparing, developing, issuing, approving, or publishing of any year 2000 statement.

(6) **REPUBLICATION.**--The term "republication" means any repetition, in whole or in part, of a year 2000 statement originally made by another.

(7) **YEAR 2000 INTERNET WEBSITE.**--The term "year 2000 Internet website" means an Internet website or other similar electronically accessible service, clearly designated on the website or service by the person or entity creating or controlling the content of the website or service as an area where year 2000 statements concerning that person or entity are posted or otherwise made accessible to the general public.

(8) **YEAR 2000 PROCESSING.**--The term "year 2000 processing" means the processing (including calculating, comparing, sequencing, displaying, or storing), transmitting, or receiving of date data from, into, and between the 20th and 21st centuries, and during the years 1999 and 2000, and leap year calculations.

(9) **YEAR 2000 READINESS DISCLOSURE.**--The term "year 2000 readiness disclosure" means any written year 2000 statement--

(A) clearly identified on its face as a year 2000 readiness disclosure;

(B) inscribed on a tangible medium or stored in an electronic or other medium and retrievable in perceivable form; and

(C) issued or published by or with the approval of a person or entity with respect to year 2000 processing of that person or entity or of products or services offered by that person or entity.

(10) **YEAR 2000 REMEDIATION PRODUCT OR SERVICE.**--The term

"year 2000 remediation product or service" means a software program or service licensed, sold, or rendered by a person or entity and specifically designed to detect or correct year 2000 processing problems with respect to systems, products, or services manufactured or rendered by another person or entity.

(11) YEAR 2000 STATEMENT.--

(A) IN GENERAL.--The term "year 2000 statement" means any communication or other conveyance of information by a party to another or to the public, in any form or medium--

(i) concerning an assessment, projection, or estimate concerning year 2000 processing capabilities of an entity, product, service, or set of products and services;

(ii) concerning plans, objectives, or timetables for implementing or verifying the year 2000 processing capabilities of an entity, product, service, or set of products and services;

(iii) concerning test plans, test dates, test results, or operational problems or solutions related to year 2000 processing by--

(I) products; or

(II) services that incorporate or utilize products; or

(iv) reviewing, commenting on, or otherwise directly or indirectly relating to year 2000 processing capabilities.

(B) NOT INCLUDED.--For the purposes of any action brought under the securities laws, as that term is defined in section 3(a)(47) of the Securities Exchange Act of 1934 (15 U.S.C. 78c(a)(47)), the term "year 2000 statement" does not include statements contained in any documents or materials filed with the Securities and Exchange Commission, or with Federal banking regulators, pursuant to section 12(i) of the Securities Exchange Act of 1934 (15 U.S.C. 781(i)), or disclosures or writing that when made accompanied the solicitation of an offer or sale of securities.

SEC. 4. PROTECTION FOR YEAR 2000 STATEMENTS.

(a) EVIDENCE EXCLUSION.--No year 2000 readiness disclosure, in whole or in part, shall be admissible against the maker of that disclosure to prove the accuracy or truth of any year 2000 statement set forth in that disclosure, in any covered action brought by another party except that--

(1) a year 2000 readiness disclosure may be admissible to

serve as the basis for a claim for anticipatory breach, or repudiation of a contract, or a similar claim against the maker, to the extent provided by applicable law; and

(2) the court in any covered action shall have discretion to limit application of this subsection in any case in which the court determines that the maker's use of the year 2000 readiness disclosure amounts to bad faith or fraud, or is otherwise beyond what is reasonable to achieve the purposes of this Act.

(b) FALSE, MISLEADING AND INACCURATE YEAR 2000 STATEMENTS.--

Except as provided in subsection (c), in any covered action, to the extent that such action is based on an allegedly false, inaccurate, or misleading year 2000 statement, the maker of that year 2000 statement shall not be liable under Federal or State law with respect to that year 2000 statement unless the claimant establishes, in addition to all other requisite elements of the applicable action, by clear and convincing evidence, that--

(1) the year 2000 statement was material; and

(2)(A) to the extent the year 2000 statement was not a republication, that the maker made the year 2000 statement--

(i) with actual knowledge that the year 2000 statement was false, inaccurate, or misleading;

(ii) with intent to deceive or mislead; or

(iii) with a reckless disregard as to the accuracy of the year 2000 statement; or

(B) to the extent the year 2000 statement was a republication, that the maker of the republication made the year 2000 statement--

(i) with actual knowledge that the year 2000 statement was false, inaccurate, or misleading;

(ii) with intent to deceive or mislead; or

(iii) without notice in that year 2000 statement that--

(I) the maker has not verified the contents of the republication; or

(II) the maker is not the source of the republication and the republication is based on information supplied by another person or entity identified in that year 2000 statement or republication.

(c) DEFAMATION OR SIMILAR CLAIMS.--In a covered action arising under any Federal or State law of defamation, trade disparagement, or a similar claim, to the extent such action is based on an allegedly false, inaccurate, or misleading year 2000 statement, the maker of that year 2000 statement shall not be liable with respect to that year 2000 statement, unless the claimant establishes by clear and convincing evidence, in addition to all other requisite elements of the applicable action, that the year 2000 statement was

made with knowledge that the year 2000 statement was false or made with reckless disregard as to its truth or falsity.

(d) YEAR 2000 INTERNET WEBSITE.--

(1) **IN GENERAL.--**Except as provided in paragraph (2), in any covered action other than a covered action involving personal injury or serious physical damage to property, in which the adequacy of notice about year 2000 processing is at issue, the posting, in a commercially reasonable manner and for a commercially reasonable duration, of a notice by the entity charged with giving such notice on the year 2000 Internet website of that entity shall be deemed an adequate mechanism for providing that notice.

(2) **EXCEPTION.--**Paragraph (1) shall not apply if the court finds that the use of the mechanism of notice--

(A) is contrary to express prior representations regarding the mechanism of notice made by the party giving notice;

(B) is materially inconsistent with the regular course of dealing between the parties; or

(C) occurs where there have been no prior representations regarding the mechanism of notice, no regular course of dealing exists between the parties, and actual notice is clearly the most commercially reasonable means of providing notice.

(3) **CONSTRUCTION.--**Nothing in this subsection shall--

(A) alter or amend any Federal or State statute or regulation requiring that notice about year 2000 processing be provided using a different mechanism;

(B) create a duty to provide notice about year 2000 processing;

(C) preclude or suggest the use of any other medium for notice about year 2000 processing or require the use of an Internet website; or

(D) mandate the content or timing of any notices about year 2000 processing.

(e) LIMITATION ON EFFECT OF YEAR 2000 STATEMENTS.--

(1) **IN GENERAL.--**In any covered action, a year 2000 statement shall not be interpreted or construed as an amendment to or alteration of a contract or warranty, whether entered into by or approved for a public or private entity.

(2) **NOT APPLICABLE.--**

(A) **IN GENERAL.--**This subsection shall not apply--

(i) to the extent the party whose year 2000 statement is alleged to have amended or altered a

contract or warranty has otherwise agreed in writing to so alter or amend the contract or warranty;

(ii) to a year 2000 statement made in conjunction with the formation of the contract or warranty; or

(iii) if the contract or warranty specifically provides for its amendment or alteration through the making of a year 2000 statement.

(B) **RULE OF CONSTRUCTION.**--Nothing in this subsection shall affect applicable Federal or State law in effect as of the date of enactment of this Act with respect to determining the extent to which a year 2000 statement affects a contract or warranty.

(f) SPECIAL DATA GATHERING.--

(1) **IN GENERAL.**--A Federal entity, agency, or authority may expressly designate a request for the voluntary provision of information relating to year 2000 processing, including year 2000 statements, as a special year 2000 data gathering request made pursuant to this subsection.

(2) **SPECIFICS.**--A special year 2000 data gathering request made under this subsection shall specify a Federal entity, agency, or authority, or, with its consent, another public or private entity, agency, or authority, to gather responses to the request.

(3) **PROTECTIONS.**--Except with the express consent or permission of the provider of information described in paragraph (1), any year 2000 statements or other such information provided by a party in response to a special year 2000 data gathering request made under this subsection--

(A) shall be exempt from disclosure under subsection (b)(4) of section 552 of title 5, United States Code, commonly known as the "Freedom of Information Act";

(B) shall not be disclosed to any third party; and

(C) may not be used by any Federal entity, agency, or authority or by any third party, directly or indirectly, in any civil action arising under any Federal or State law.

(4) EXCEPTIONS.--

(A) **INFORMATION OBTAINED ELSEWHERE.**--Nothing in this subsection shall preclude a Federal entity, agency, or authority, or any third party, from separately obtaining the information submitted in response to a request under this subsection through the use of independent legal authorities, and using such separately obtained information in any action.

(B) **VOLUNTARY DISCLOSURE.**--A restriction on use or disclosure of information under this subsection shall not apply to any information disclosed to the public with the

express consent of the party responding to a special year 2000 data gathering request or disclosed by such party separately from a response to a special year 2000 data gathering request.

SEC. 5. TEMPORARY ANTITRUST EXEMPTION.

(a) EXEMPTION.--Except as provided in subsection (b), the antitrust laws shall not apply to conduct engaged in, including making and implementing an agreement, solely for the purpose of and limited to--

(1) facilitating responses intended to correct or avoid a failure of year 2000 processing in a computer system, in a component of a computer system, in a computer program or software, or services utilizing any such system, component, program, or hardware; or

(2) communicating or disclosing information to help correct or avoid the effects of year 2000 processing failure

(b) APPLICABILITY.--Subsection (a) shall apply only to conduct that occurs, or an agreement that is made and implemented, after the date of enactment of this Act and before July 14, 2001.

(c) EXCEPTION TO EXEMPTION.--Subsection (a) shall not apply with respect to conduct that involves or results in an agreement to boycott any person, to allocate a market, or to fix prices or output.

(d) RULE OF CONSTRUCTION.--The exemption granted by this section shall be construed narrowly.

SEC. 6. EXCLUSIONS.

(a) EFFECT ON INFORMATION DISCLOSURE.--This Act does not affect, abrogate, amend, or alter the authority of a Federal or State entity, agency, or authority to enforce a requirement to provide or disclose, or not to provide or disclose, information under a Federal or State statute or regulation or to enforce such statute or regulation.

(b) CONTRACTS AND OTHER CLAIMS.--

(1) IN GENERAL.--Except as may be otherwise provided in subsections (a) and (e) of section 4, this Act does not affect, abrogate, amend, or alter any right established by contract or tariff between any person or entity, whether entered into by a public or private person or entity, under any Federal or State law.

(2) OTHER CLAIMS.--

(A) **IN GENERAL.**--In any covered action brought by a consumer, this Act does not apply to a year 2000 statement expressly made in a solicitation, including an advertisement or offer to sell, to that consumer by a seller, manufacturer, or provider of a consumer product.

(B) **SPECIFIC NOTICE REQUIRED.**--In any covered action, this Act shall not apply to a year 2000 statement, concerning a year 2000 remediation product or service, expressly made in an offer to sell or in a solicitation (including an advertisement) by a seller, manufacturer, or provider, of that product or service unless, during the course of the offer or solicitation, the party making the offer or solicitation provides the following notice in accordance with section 4(d):

"Statements made to you in the course of this sale are subject to the Year 2000 Information and Readiness Disclosure Act (XX U.S.C. XX). In the case of a dispute, this Act may reduce your legal rights regarding the use of any such statements, unless otherwise specified by your contract or tariff."

(3) **RULE OF CONSTRUCTION.**--Nothing in this Act shall be construed to preclude any claims that are not based exclusively on year 2000 statements.

(c) **DUTY OR STANDARD OF CARE.**--

(1) **IN GENERAL.**--This Act shall not impose upon the maker of any year 2000 statement any more stringent obligation, duty, or standard of care than is otherwise applicable under any other Federal law or State law.

(2) **ADDITIONAL DISCLOSURE.**--This Act does not preclude any party from making or providing any additional disclosure, disclaimer, or similar provisions in connection with any year 2000 readiness disclosure or year 2000 statement.

(3) **DUTY OF CARE.**--This Act shall not be deemed to alter any standard or duty of care owed by a fiduciary, as defined or determined by applicable Federal or State law.

(d) **INTELLECTUAL PROPERTY RIGHTS.**--This Act does not affect, abrogate, amend, or alter any right in a patent, copyright, semiconductor mask work, trade secret, trade name, trademark, or service mark, under any Federal or State law.

(e) **INJUNCTIVE RELIEF.**--Nothing in this Act shall be deemed to preclude a claimant from seeking injunctive relief with respect to a year 2000 statement.

SEC. 7. APPLICABILITY.

(a) EFFECTIVE DATE.--

(1) **IN GENERAL.--**Except as otherwise provided in this section, this Act shall become effective on the date of enactment of this Act.

(2) **APPLICATION TO LAWSUITS PENDING.--**This Act shall not affect or apply to any lawsuit pending on July 14, 1998.

(3) **APPLICATION TO STATEMENTS AND DISCLOSURES.--**Except as provided in subsection (b)--

(A) this Act shall apply to any year 2000 statement made beginning on July 14, 1998 and ending on July 14, 2001; and

(B) this Act shall apply to any year 2000 readiness disclosure made beginning on the date of enactment of this Act and ending on July 14, 2001.

(b) PREVIOUSLY MADE READINESS DISCLOSURE.--

(1) **IN GENERAL.--**For the purposes of section 4(a), a person or entity that issued or published a year 2000 statement after January 1, 1996, and before the date of enactment of this Act, may designate that year 2000 statement as a year 2000 readiness disclosure if--

(A) the year 2000 statement complied with the requirements of section 3(9) when made, other than being clearly designated on its face as a disclosure; and

(B) within 45 days after the date of enactment of this Act, the person or entity seeking the designation--

(i) provides individual notice that meets the requirements of paragraph (2) to all recipients of the applicable year 2000 statement; or

(ii) prominently posts notice that meets the requirements of paragraph (2) on its year 2000 Internet website, commencing prior to the end of the 45-day period under this subparagraph and extending for a minimum of 45 consecutive days and also uses the same method of notification used to originally provide the applicable year 2000 statement.

(2) **REQUIREMENTS.--**A notice under paragraph (1)(B) shall--

(A) state that the year 2000 statement that is the subject of the notice is being designated a year 2000 readiness disclosure; and

(B) include a copy of the year 2000 statement with a legend labeling the statement as a "Year 2000 Readiness Disclosure".

(c) EXCEPTION.--No designation of a year 2000 statement as a year 2000 readiness disclosure under subsection (b) shall apply with respect to any person or entity that--

(1) proves, by clear and convincing evidence, that it relied on the year 2000 statement prior to the receipt of notice described in subsection (b)(1)(B) and it would be prejudiced by the retroactive designation of the year 2000 statement as a year 2000 readiness disclosure; and

(2) provides to the person or entity seeking the designation a written notice objecting to the designation within 45 days after receipt of individual notice under subsection (b)(1)(B)(i), or within 180 days after the date of enactment of this Act, in the case of notice provided under subsection (b)(1)(B)(ii).

SEC. 8. YEAR 2000 COUNCIL WORKING GROUPS.

(a) IN GENERAL.--

(1) WORKING GROUPS.--The President's Year 2000 Council (referred to in this section as the "Council") may establish and terminate working groups composed of Federal employees who will engage outside organizations in discussions to address the year 2000 problems identified in section 2(a)(1) to share information related to year 2000 readiness, and otherwise to serve the purposes of this Act.

(2) LIST OF GROUPS.--The Council shall maintain and make available to the public a printed and electronic list of the working groups, the members of each working group, and a point of contact, together with an address, telephone number, and electronic mail address for the point of contact, for each working group created under this section.

(3) BALANCE.--The Council shall seek to achieve a balance of participation and representation among the working groups.

(4) ATTENDANCE.--The Council shall maintain and make available to the public a printed and electronic list of working group members who attend each meeting of a working group as well as any other individuals or organizations participating in each meeting.

(5) MEETINGS.--Each meeting of a working group shall be announced in advance in accordance with procedures established by the Council. The Council shall encourage working groups to hold meetings open to the public to the extent feasible and consistent with the activities of the Council and the purposes of this Act.

(b) FACA.--The Federal Advisory Committee Act (5 U.S.C. App.)

shall not apply to the working groups established under this section.

(c) PRIVATE RIGHT OF ACTION.--This section creates no private right of action to sue for enforcement of the provisions of this section.

(d) EXPIRATION.--The authority conferred by this section shall expire on December 31, 2000.

SEC. 9. NATIONAL INFORMATION CLEARINGHOUSE AND WEBSITE.

(a) NATIONAL WEBSITE.--

(1) IN GENERAL.--The Administrator of General Services shall create and maintain until July 14, 2002, a national year 2000 website, and promote its availability, designed to assist consumers, small business, and local governments in obtaining information from other governmental websites, hotlines, or information clearinghouses about year 2000 processing of computers, systems, products, and services, including websites maintained by independent agencies and other departments.

(2) CONSULTATION.--In creating the national year 2000 website, the Administrator of General Services shall consult with--

- (A) the Director of the Office of Management and Budget;
- (B) the Administrator of the Small Business Administration;
- (C) the Consumer Product Safety Commission;
- (D) officials of State and local governments;
- (E) the Director of the National Institute of Standards and Technology;
- (F) representatives of consumer and industry groups; and
- (G) representatives of other entities, as determined appropriate.

(b) REPORT.--The Administrator of General Services shall submit a report to the Committees on the Judiciary of the Senate and the House of Representatives and the Committee on Governmental Affairs of the Senate and the Committee on Government Reform and Oversight of the House of Representatives not later than 60 days after the date of enactment of this Act regarding planning to comply with the requirements of this section.

SMALL BUSINESS YEAR 2000 READINESS ACT

S. 314 - ENACTED AND SIGNED INTO LAW

106th CONGRESS, 1st Session

S 314
Enrolled Bill
March 24, 1999

AN ACT
S 314

Begun and held at the City of Washington on Wednesday, the sixth day of January, one thousand nine hundred and ninety-nine

To provide for a loan guarantee program to address the Year 2000 computer problems of small business concerns, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the 'Small Business Year 2000 Readiness Act'.

SEC. 2. FINDINGS.

Congress finds that--

(1) the failure of many computer programs to recognize the Year 2000 may have extreme negative financial consequences in the Year 2000, and in subsequent years for both large and small businesses;

(2) small businesses are well behind larger businesses in implementing corrective changes to their automated systems;

(3) many small businesses do not have access to capital to fix mission critical automated systems, which could result in severe financial distress or failure for small businesses; and

(4) the failure of a large number of small businesses due to the Year 2000 computer problem would have a highly detrimental effect on the economy in the Year 2000 and in subsequent years.

SEC. 3. YEAR 2000 COMPUTER PROBLEM LOAN GUARANTEE PROGRAM.

(a) PROGRAM ESTABLISHED- Section 7(a) of the Small Business Act (> 15 U.S.C. 636(a)) is amended by adding at the end the following:

'(27) YEAR 2000 COMPUTER PROBLEM PROGRAM-

'(A) DEFINITIONS- In this paragraph--

'(i) the term 'eligible lender' means any lender designated by the Administration as eligible to participate in the general business loan program under this subsection; and

'(ii) the term 'Year 2000 computer problem' means, with respect to information technology, and embedded systems, any problem that adversely effects the processing (including calculating, comparing, sequencing, displaying, or storing), transmitting, or receiving of date-dependent data--

'(I) from, into, or between--

'(aa) the 20th or 21st centuries; or

'(bb) the years 1999 and 2000; or

'(II) with regard to leap year calculations.

'(B) ESTABLISHMENT OF PROGRAM- The Administration shall--

'(i) establish a loan guarantee program, under which the Administration may, during the period beginning on the date of enactment of this paragraph and ending on December 31, 2000, guarantee loans made by eligible lenders to small business concerns in accordance with this paragraph; and

'(ii) notify each eligible lender of the establishment of the program under this paragraph, and otherwise take such actions as may be necessary to aggressively market the program under this paragraph.

'(C) USE OF FUNDS- A small business concern that receives a loan guaranteed under this paragraph shall only use the proceeds of the loan to--

'(i) address the Year 2000 computer problems of that small business concern, including the repair and acquisition of information technology systems, the purchase and repair of software, the purchase of consulting and other third party services, and related expenses; and

'(ii) provide relief for a substantial economic injury incurred by the small business concern as a direct result of the Year 2000 computer problems of the small business concern or of any other entity (including any service provider or supplier of the small business concern), if such economic injury has not been compensated for by insurance or otherwise.

'(D) LOAN AMOUNTS-

'(i) IN GENERAL- Notwithstanding paragraph (3)(A) and subject to clause (ii) of this subparagraph, a loan may be made to a borrower under this paragraph even if the total amount outstanding and committed (by participation or otherwise) to the borrower from the business loan and investment fund, the business guaranty loan financing account, and the business direct loan financing account would thereby exceed \$750,000.

'(ii) EXCEPTION- A loan may not be made to a borrower under this paragraph if the total amount outstanding and committed (by participation or otherwise) to the borrower from the business loan and investment fund, the business guaranty loan financing account, and the business direct loan financing account would thereby exceed \$1,000,000.

'(E) ADMINISTRATION PARTICIPATION- Notwithstanding paragraph (2)(A), in an agreement to participate in a loan under this paragraph, participation by the Administration shall not exceed--

'(i) 85 percent of the balance of the financing outstanding at the time of disbursement of the loan, if the balance exceeds \$100,000;

'(ii) 90 percent of the balance of the financing outstanding at the time of disbursement of the loan, if the balance is less than or equal to \$100,000; and

'(iii) notwithstanding clauses (i) and (ii), in any case in which the subject loan is processed in accordance with the requirements applicable to the SBAExpress Pilot Program, 50 percent of the balance outstanding at the time of disbursement of the loan.

'(F) PERIODIC REVIEWS- The Inspector General of the Administration shall periodically review a representative sample of loans guaranteed under this paragraph to mitigate the risk of fraud and ensure the safety and soundness of the loan program.

'(G) ANNUAL REPORT- The Administration shall annually submit to the Committees on Small Business of the House of Representatives and the Senate a report on the results of the program carried out under this paragraph during the preceding 12-month period, which shall include information

relating to--

'(i) the total number of loans guaranteed under this paragraph;

'(ii) with respect to each loan guaranteed under this paragraph--

'(I) the amount of the loan;

'(II) the geographic location of the borrower; and

'(III) whether the loan was made to repair or replace information technology and other automated systems or to remedy an economic injury; and

'(iii) the total number of eligible lenders participating in the program.'

(b) GUIDELINES-

(1) **IN GENERAL-** Not later than 30 days after the date of enactment of this Act, the Administrator of the Small Business Administration shall issue guidelines to carry out the program under section 7(a)(27) of the Small Business Act, as added by this section.

(2) **REQUIREMENTS-** Except to the extent that it would be inconsistent with this section or section 7(a)(27) of the Small Business Act, as added by this section, the guidelines issued under this subsection shall, with respect to the loan program established under section 7(a)(27) of the Small Business Act, as added by this section--

(A) provide maximum flexibility in the establishment of terms and conditions of loans originated under the loan program so that such loans may be structured in a manner that enhances the ability of the applicant to repay the debt;

(B) if appropriate to facilitate repayment, establish a moratorium on principal payments under the loan program for up to 1 year beginning on the date of the origination of the loan;

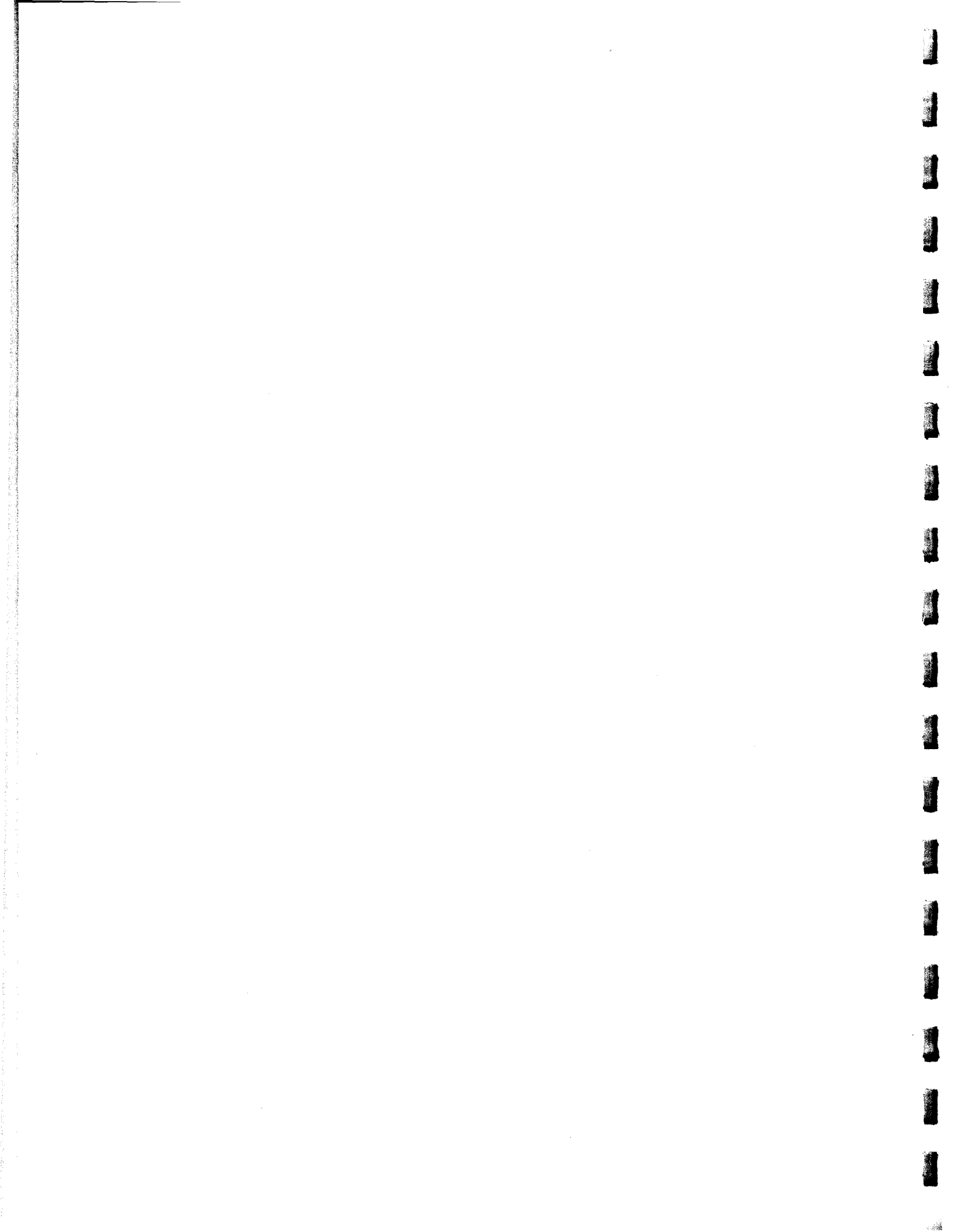
(C) provide that any reasonable doubts regarding a loan applicant's ability to service the debt be resolved in favor of the loan applicant; and

(D) authorize an eligible lender (as defined in section 7(a)(27)(A) of the Small Business Act, as added by this section) to process a loan under the loan program in accordance with the requirements applicable to loans originated under another loan program established pursuant to section 7(a) of the Small Business Act ((> 15 USCA 636)) (including the general business loan program, the Preferred Lender Program, the Certified Lender Program, the Low Documentation Loan Program, and the SBAExpress Pilot Program), if--

(i) the eligible lender is eligible to participate in such other loan program; and

(ii) the terms of the loan, including the principal amount of the loan, are consistent with the requirements applicable to loans originated under such other loan program.

(c) **REPEAL-** Effective on December 31, 2000, this section and the amendments made by this section are repealed.

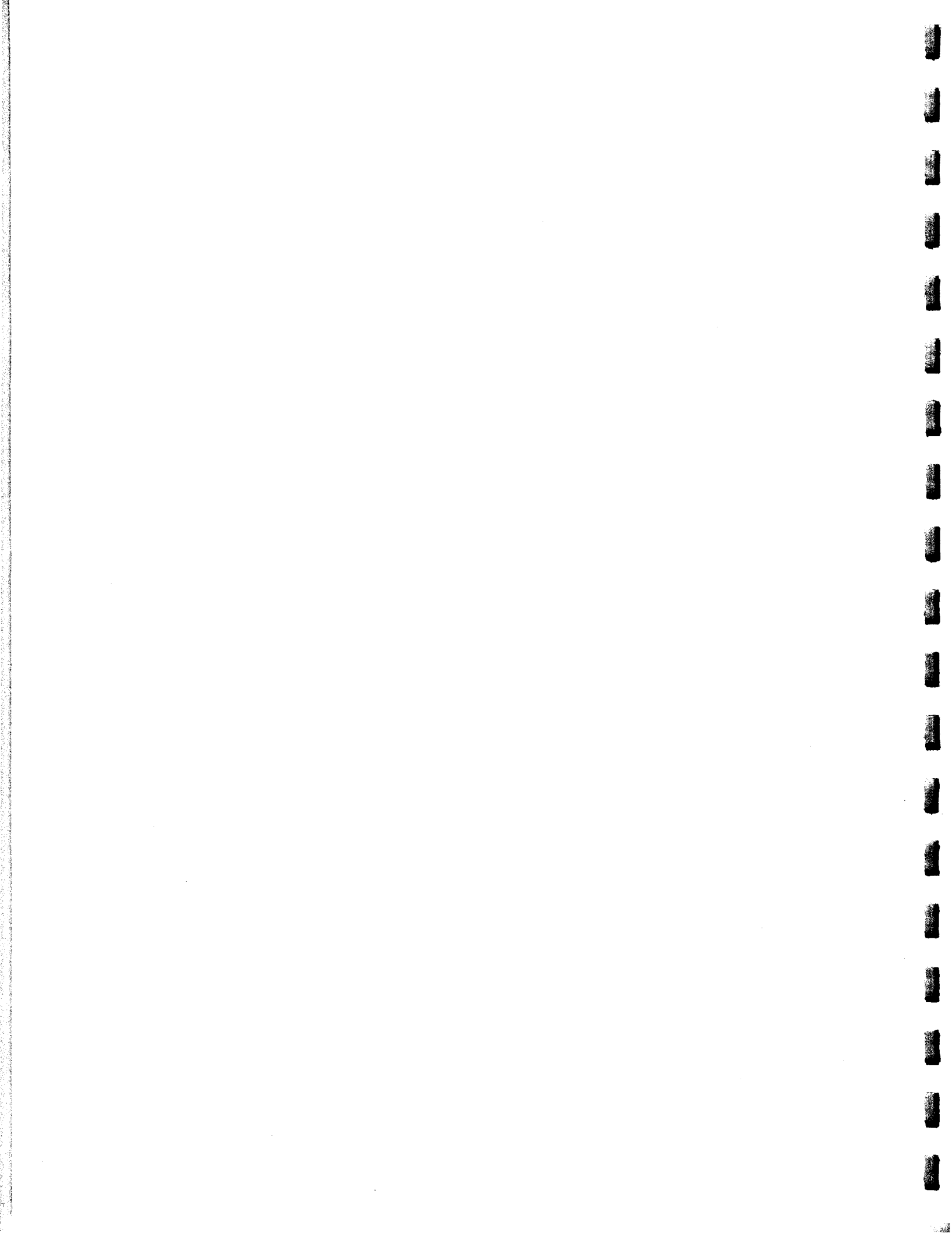


**YEAR 2000:
ASSESSMENT, READINESS & REMEDIATION**

J. Mark Grundy
Greenebaum Doll & McDonald PLLC
Louisville, Kentucky

Copyright 1999, J. Mark Grundy. All Rights Reserved.

SECTION C



YEAR 2000: ASSESSMENT, READINESS & REMEDIATION

TABLE OF CONTENTS

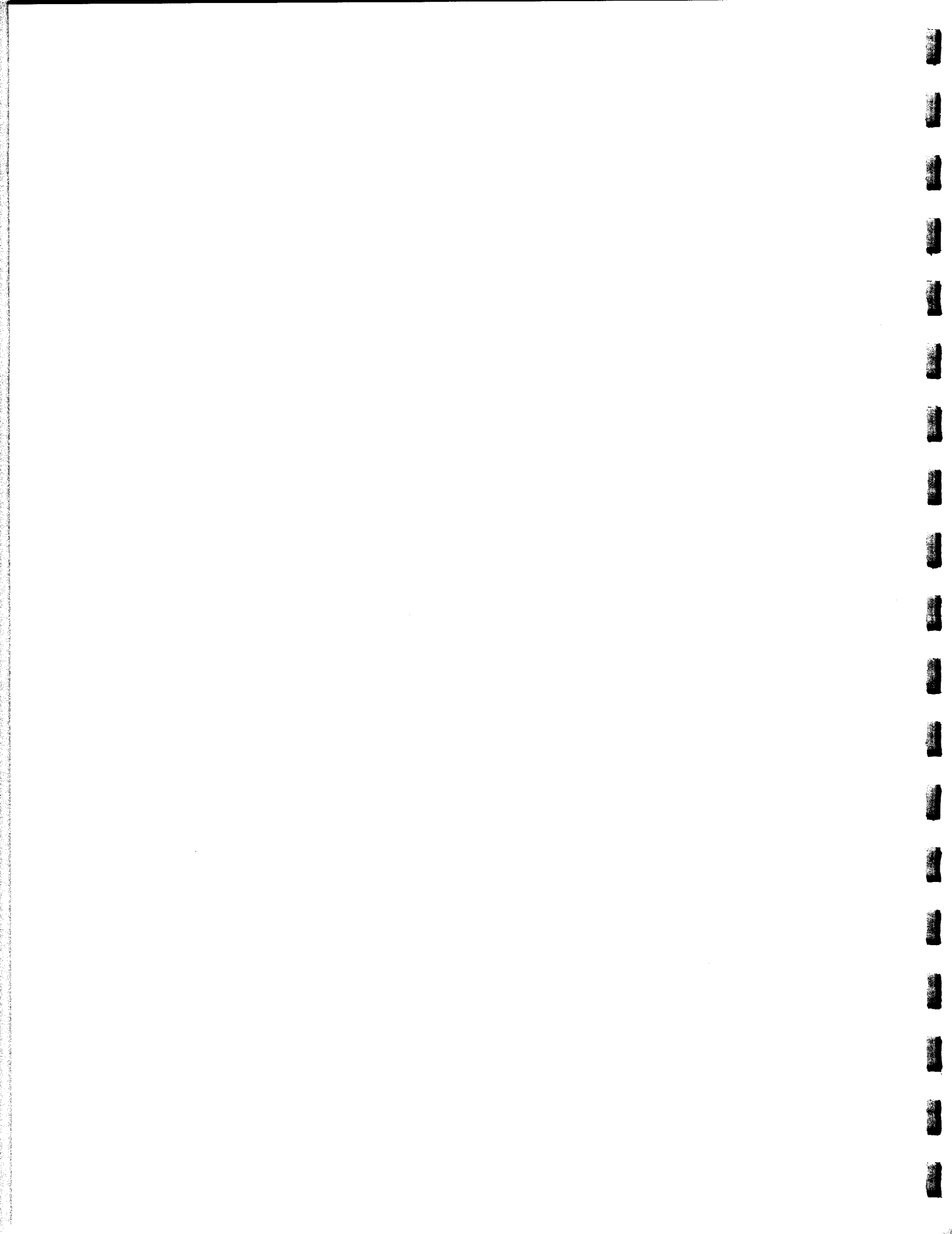
I. INTRODUCTION C-1

II. CLAIMS AND DEFENSES C-1

- A. Insurance C-1
- B. Directors And Officers Liability C-1
- C. Securities Claims C-2
- D. Intellectual Property And Consultant Claims C-2
- E. Compliance Letters C-3
- F. Contract Claims C-3
- G. Tort Claims C-4
- H. Statutory C-4

III. THE REALITY OF Y2K LITIGATION C-5

ADDENDUM: Business First Article, Grundy, "Are you ready for Y2K litigation?" C-6



I. INTRODUCTION

The Y2K problem, in some manner, has or will impact virtually every business enterprise. In order to identify and properly address the legal risks associated with Y2K, you should have an understanding of Y2K related claims and defenses. Armed with that understanding, you can take the steps that will help your company either avoid or prevail in Y2K litigation.

II. CLAIMS AND DEFENSES

A. Insurance

- ▶ Every company should check the status of their insurance coverage to make sure it has appropriate Y2K coverage. Insurance companies have responded to the potential Y2K litigation explosion in three different ways:
 1. A number of insurance companies have "added" exclusions to their policies in an effort to exclude coverage for Y2K problems. If a business receives an "endorsement" that purports to exclude Y2K coverage, common sense steps should be taken - depending on the applicable language - to make sure the business does not waive its rights. For example, if the business believes that the original policy should cover Y2K matters, then a letter to that extent may be of significant evidentiary value.
 2. Some insurance companies are offering riders or separate policies that expressly provide Y2K coverage. Each business should do a risk analysis and determine whether to purchase such coverage.
 3. Some insurance companies are doing nothing with their policies and are taking the position that Y2K is a foreseeable event that is implicitly excluded from business interruption coverage.
- ▶ In order to avoid any misunderstandings and coverage disputes, insureds should check with their insurers now to determine the status of coverage. Their respective positions should be documented in writing, with a view that those documents may be necessary court exhibits.

B. Directors and Officers Liability

- ▶ As a general rule, directors and officers are legally bound by the fiduciary duties of loyalty and due care to manage the corporation in the best interest of its shareholders. If a corporation fails to address Y2K

problems successfully, and the business is significantly impacted, shareholders may seek to hold the directors and officers liable.

- ▶ The general defense to such claims is the "business judgment rule," which provides that directors and officers are insulated from liability if they can make a showing that they acted in good faith, were reasonably diligent in informing themselves of the facts, and relied upon knowledgeable experts. The following basic steps should be taken and documented by the board:
 1. Designate a company Y2K committee that includes representatives from all management areas.
 2. Mandate and document a company Y2K compliance and contingency plan.
 3. Consult with knowledgeable experts and budget a realistic line item for Y2K expenditures.
 4. Require regular Y2K progress reports to the board.
- ▶ If a Y2K claim is brought, the entire process in which the company handled Y2K issues will be the subject of discovery in the litigation. Therefore, you should involve the proper technical and legal experts to make sure nothing is overlooked or can be misconstrued under the scrutiny of an opposing litigator.

C. Securities Claims

- ▶ Various federal and state securities statutes import a duty to public companies to disclose material facts. Counsel and company management should make sure that reasonable care is exercised in making appropriate Y2K disclosures.
- ▶ The general spectrum of common defenses to securities actions may apply, including: lack of materiality, Y2K exposure is common knowledge, and lack of intent to mislead.

D. Intellectual Property and Consultant Claims

- ▶ Numerous intellectual property and trade secret issues arise with respect to Y2K remediation measures. Commonly litigated issues are whether existing software can be accessed to outside remediation companies in violation of license agreements, and whether software can be reversed engineered for remediation purposes.

- ▶ Counsel should be fully aware of the company's rights and duties before enlisting outside assistance for preventative and remediation measures. It may be necessary to extend, modify, or renegotiate applicable agreements - or to obtain a Court approved protective order - in order to achieve the desired result of avoiding the often conflicting nature of intellectual property claims and Y2K claims.

E. Compliance Letters

- ▶ The economy has been flooded with compliance requests and response correspondence between vendors and purchasers. Purchasers send compliance requests in order to determine whether they are reliant on vendors who are not Y2K complaint. The end result is a massive paper trail of contractual rights, duties, warranties, representations and disclaimers.
- ▶ It is imperative that counsel thoroughly review the contents of compliance request and response letters. Many of these documents will become court exhibits and serve as the evidentiary cornerstone of the rights and duties between claimants.
- ▶ In the fall of 1998, the federal Y2K Readiness and Disclosure Act was signed into law. The Act significantly impacts the enforceability of compliance letters. The Act requires a company to include certain "magic language" in compliance letters in order to enjoy the protection of the Act.

F. Contract Claims

- ▶ Y2K contract claims usually arise when a business is unable to fulfill its obligations because of a computer failure somewhere in the supply chain. Each contract claim is governed by the terms of the particular contract, as reflected in written agreements, compliance letters, purchase orders and invoices.
- ▶ Typically these types of disputes are viewed as "sales of goods" which are governed by the UCC. (It should be noted that the courts are split on whether software sales or license agreements are governed by Article 2 of the UCC.)
- ▶ Within the normal business context, most companies have at some time had their contract forms reviewed by counsel so they are protected under the UCC. It is important to recognized that some vendors are expressly disclaiming Y2K liability in their purchase documents. Counsel should

review the status of the contract forms being received and generated by the company to make sure UCC protections remain in place.

- ▶ Particular attention should be paid to whether the writings are creating or disclaiming expressed or implied warranties, and whether the writings limit remedies by excluding indirect or consequential damages, or require only repair or replacement.

G. Tort Claims

- ▶ Depending of the particular fact situation, Y2K tort claims have or will run the gambit of tort claims ranging from fraud, misrepresentation, negligence, and strict liability.
- ▶ A tort claim requires more than "economic injury." There must be injury to property or to a person. Some courts have held that the requisite "property damage" must occur to the property of another, rather than to the property itself. Hence, the failure of computer software has not been viewed as "property damage" - even though the business lost valuable information as a result of the failure.
- ▶ It is believed that Y2K tort claims for personal injury will arise from the failure of imbedded chips in equipment such as medical devices, elevators, traffic control devices, motor vehicles, and environmental and electrical support systems. Such claims will follow the traditional analysis of negligence, and strict liability claims.
- ▶ In order to avoid such claims, each business should review its equipment and systems. It is noteworthy that the FDA has assembled a lengthy list of types of medical equipment that have embedded chip problems.
- ▶ Counsel and company management should realized that with the bombardment of Y2K publicity, the "foreseeability" of Y2K defects has been heightened and the applicable "standard of care" has risen.

H. Statutory

- ▶ Numerous federal acts are being considered by Congress to address what is perceived to be a flood of Y2K litigation that could seriously disrupt the global economy. The acts presently under consideration seek to curtail Y2K suits, require "cooling off periods", and limit punitive damages, attorneys' fees, and class actions.
- ▶ Some states (such as California) have consumer protection statutes under which Y2K actions have been brought.

III. THE REALITY OF Y2K LITIGATION

No one knows whether Y2K will lead to a litigation explosion. But one thing is certain - Y2K defects are real, and litigation has begun. Suits have already been filed in Michigan, California, and even in Kentucky over equipment that either is not Y2K compliant, or which has already failed. Computer failures have caused the temporary closure of an airport in the Orient, and of a manufacturing plant in Europe. Damages in those case have been calculated as running in the millions of dollars.

BUSINESS FIRST®

VOLUME 14, NUMBER 1

The Weekly Business Newspaper of Greater Louisville

WEEK OF AUGUST 10, 1998

Are you ready for Y2K litigation?

Year 2000 has yet to arrive, but the litigation has already begun over widespread defects in many computer programs that fail to process data related to the year 2000 and beyond.

The "Y2K" problem — and potential litigation — threatens virtually every business.

Either the business has a computer system that may be at risk or the business is faced with the potential failure of computer systems at the companies that it relies upon for materials, supplies, services or revenue.

Has your business adequately addressed the Y2K problem? Are you reliant on suppliers and customers who have not addressed the problem?

Word to the wise — in most instances, it is not enough to simply rely on an "opinion" that your system is Y2K "compliant."

For example, a Michigan grocery store chain bought computerized cash registers in 1995 based on assurances that the registers were "free of problems" and would enhance customer service and profitability.

After the registers were put into operation, the store learned that the registers do not process credit cards with expiration dates of the year 2000 or beyond. As a result, the system repeatedly fails, shuts down and needs to be "rebooted" at least once a day.

The grocery has filed suit against the register vendor seeking to recover its lost profits and remediation costs.

Many businesses have been somewhat "luckier" in that they have performed Y2K audits and have upgraded their systems to avoid any such business interruptions.

A large number of those businesses have discovered that their software vendors are charging substantial fees for the upgrade, however.

Irate over such practices, a group of businesses in California recently filed a class action suit seeking to recoup their upgrade costs. The lawsuit alleges that as recently as last year, the software companies sold systems that are not Y2K compliant and are improperly requiring the businesses to pay substantial fees to purchase upgrades.

As has been widely reported, the heart of the Y2K problem is a defect in software programs that express the year in two digits on the assumption that the first two digits of the year are always going to be "19."

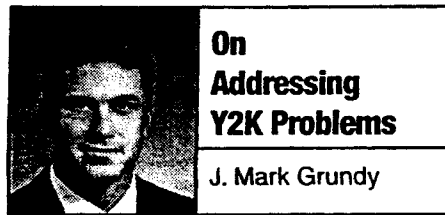
Therefore, those programs are not geared to address data that relate to the year 2000 and beyond. When data for that time period is entered, such computer programs either incorrectly roll back to the year 1900, shut down, or experience other technical difficulties.

The problem is so significant that the U.S. Securities and Exchange Commission has adopted strict disclosure requirements, and public corporations — including their management personally — can be subjected to liability if they fail to make the disclosures. Similarly, Congress is setting in motion

a task force in the event the Y2K problem leads to a severe disruption of our economy.

Accounting firms are now including Y2K audits as an exception in their audit reports. Law firms have begun to include Y2K audits as due diligence matters in acquisitions.

Many businesses are requiring that vendors and



suppliers provide certification that they are Y2K compliant.

Many business owners face a wide range of legal and business issues as a result of the Y2K problem.

As evident by the Michigan and California lawsuits, the initial round of litigation consists of two types of cases. Businesses are suing either to recoup their remediation costs, or in the worse case scenarios, an interruption of their businesses' operations has actually occurred, and they have sued to recover lost profits and other consequential damages.

By all accounts, a second round of lawsuits soon will be under way that will seek to spread the liability for the Y2K problem — and its "chain reaction" in the economic world.

Potential targets of such litigation include business advisers who failed to timely address the need for Y2K audits; accountants who failed to make adequate disclosures in audit reports; corporate officers and directors who failed to take reasonable and prudent measures to avoid or timely remedy Y2K problems; software consultants; and insurance companies.

Speculation suggests that the Y2K problem may even lead to personal injury or medical malpractice claims.

For example, it was recently reported that a hospital had to postpone an operation because a Y2K glitch in a hospital computer system incorrectly told the doctors that swabs needed during the surgery were out of stock.

The legal theories that most likely will be asserted to spread the Y2K liability range from basic contract and breach of warranty claims to negligent or fraudulent misrepresentation. Claims have also been filed under state and federal consumer protection statutes.

It is even contemplated that disgruntled shareholders will bring actions against corporate officers and directors in the event Y2K glitches cause a reduction in the value of the company stock.

If the Y2K problem is as extensive as has been initially predicted, the potential scenarios for litigation are numerous. For example, reports have been

made of predicted litigation in the following illustrative areas:

- Pension and fund computers that miscalculate or fail to process benefits for participants;
- Health care settings where drug inventory and distributions systems miscalculate the delivery and expiration dates of medicines and supplies;
- Banking systems that provide improper accountings and fail to allow the filing of timely regulatory reports;
- Companies that have interfaced their computer systems with defective systems from other companies;
- Insurance companies that reject claims because their systems inaccurately reflect that the time allowed for the claims has expired;
- Businesses and individuals who are at the mercy of computer systems that operate transits, traffic devices, environmental controls for buildings, elevators, telephone switches, and countless other industrial and commercial activities.

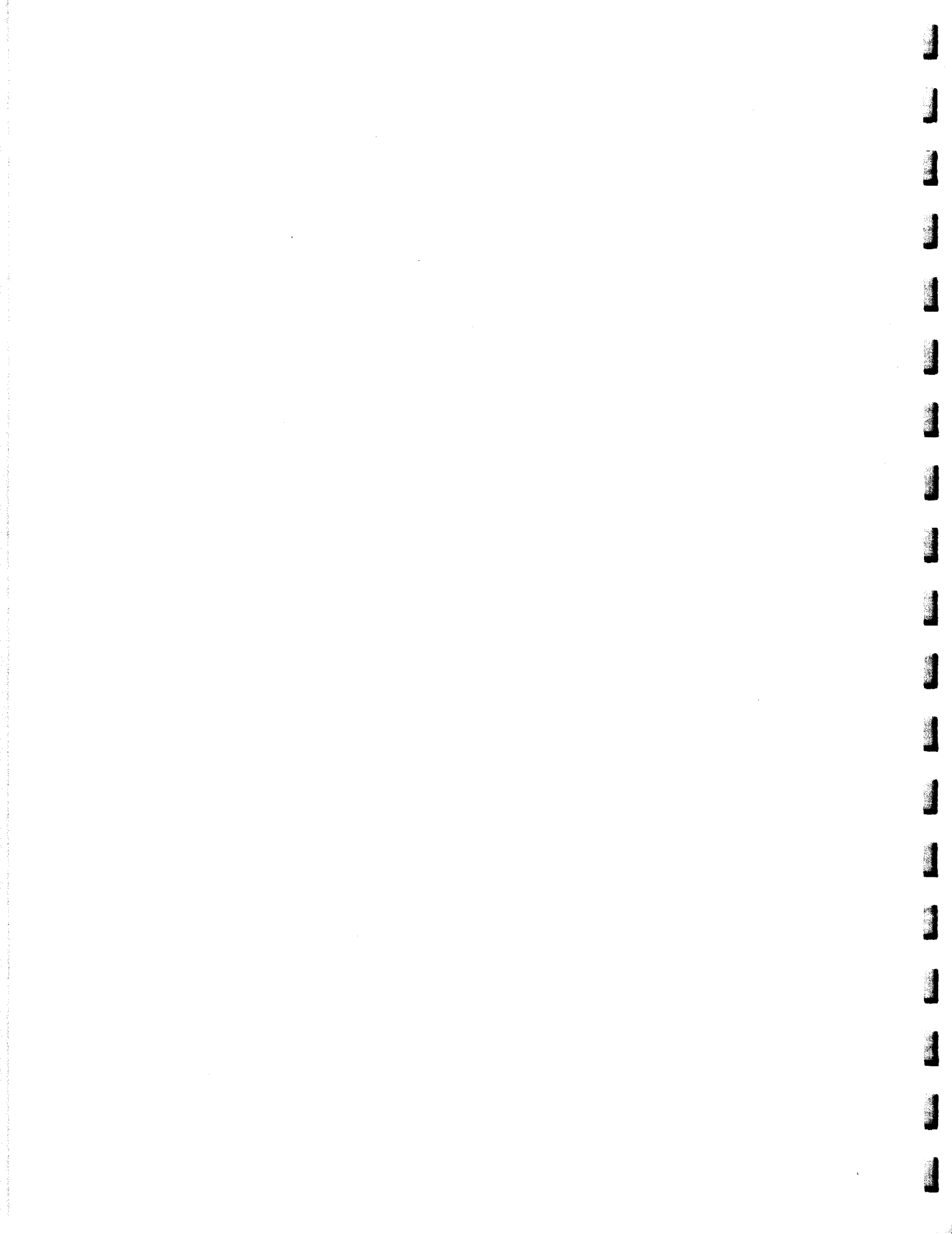
What can your company do to avoid or to prepare for Y2K litigation? Although not an exhaustive list, some basic steps to consider include the following:

- Put together a Y2K "team" and evaluate your exposure.
 - Prepare a contingency plan in the event a Y2K emergency arises.
 - Consider measures such as keeping hard copies of critical records.
 - Institute a Y2K compliance audit program.
 - Work with certified and bonded specialists to correct existing Y2K problems.
 - Review not only your company's systems, but also require your suppliers and vendors to certify that their systems are Y2K compliant and that they will reimburse or indemnify you for any related losses.
 - Educate your customers and revenue sources about Y2K issues so they do not experience business interruption.
 - Have an expert review your business forms and contracts to make sure you have protection in the event Y2K problems arise.
 - Check your insurance coverage. It has been widely reported that insurance companies may deny Y2K claims on the grounds that the problem should have been foreseen by the insured and timely remedied. Consider purchasing a separate rider for coverage of Y2K-related losses.
- Finally, if a Y2K problem requires you to upgrade your system or interrupts your business, immediately speak to a knowledgeable consultant or attorney who can advise you as to your rights and duties and assist you with mitigating your losses.

J. Mark Grundy is an attorney and member of the Y2K team with Greenebaum Doll & McDonald PLLC in Louisville.

**LITIGATION AND INSURANCE ISSUES IN
PREPARATION FOR YEAR 2000**

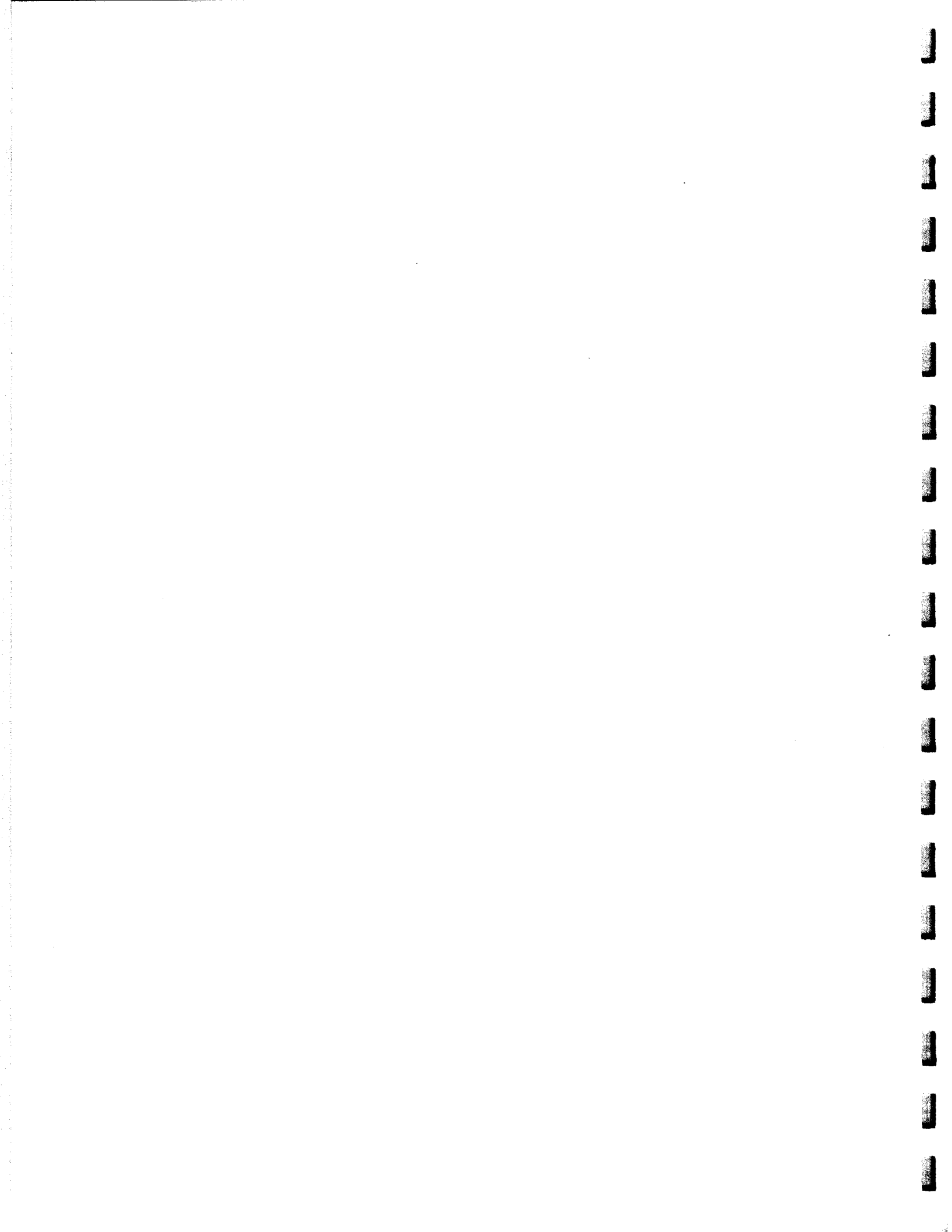
Robert F. Duncan
Jackson & Kelly
Lexington, Kentucky



**LITIGATION AND INSURANCE ISSUES IN
PREPARATION FOR YEAR 2000**

TABLE OF CONTENTS

LITIGATION	D-1
1. Breach Of Express Warranties	D-2
2. Breach Of Implied Warranties	D-3
(A) Implied warranty of merchantability	D-3
(B) Implied warranty of fitness for a particular purpose	D-3
(C) Limitations and disclaimers of warranties	D-4
3. Breach Of Contract	D-5
4. Product Liability / Strict Liability	D-5
5. Negligence / Professional Malpractice	D-6
6. Fraudulent Inducement / Unfair Trade Or Business Practices	D-7
7. Shareholder Derivative Suits / Directors' And Officers' Liability	D-7
8. Copyright Infringement And Breach Of Licensing Agreement	D-7
9. Miscellaneous	D-7
INSURANCE	D-8
1. First Party Claims	D-9
2. Third Party Claims	D-10
3. Errors And Omissions Claims	D-12
4. Directors And Officers Insurance	D-12
5. Y2K Exclusions And Y2K Policies	D-12



Y2K: LITIGATION AND INSURANCE

As we approach the year 2000, the mysteries surrounding the *Millennium Bug* are beginning to unfold. There are two issues that remain virtually unknown: (1) the economic costs, including the costs for remediation and economic damages resultant from failures, and (2) who will be responsible for these costs. The intent of this text is to generally discuss the theories of liability that may arise in the inevitable litigation that will seek to answer the Y2K issues and to discuss the relationship of insurance in the Y2K context.

LITIGATION

To date, there have been relatively few lawsuits filed (approximately 80 known to this author) and virtually no reported decisions to offer strong guidance on the issues. The best guidance comes from reported decisions in analogous situations such as environmental torts, asbestos cases, breast implant cases, matters involving intrauterine devices, fen-phen cases, and tobacco litigation. With the exception of the environmental claims and remediation claims pertaining to asbestos, these cases pertain to personal injury and therefore do not address some of the complex issues which will be faced in the anticipated Y2K litigation.

The present dearth of cases may be attributable to some or all of the following factors: resources are being prioritized for remediation and compliance; damages have not been incurred or have not been quantified; legislative matters pertaining to rights of recovery are still pending; and, potentially responsible parties and theories of recovery are still being identified and developed.

Although the absence of damages due to failure may presently preclude some actions, the failure to pursue prompt and timely litigation may prove detrimental or fatal to some actions. In many jurisdictions, actions such as negligence and product liability have short

statutes of limitations. Frequently, the statute of limitations begins to run when the cause of action was known or should have been known. The notoriety of the Y2K issues may therefore cause an early triggering of the limitations period. Additional problems may be caused by the potential insolvency of defendants, legislatively imposed limitations, aggregate insurance loss limits and decisions regarding insurance coverage. In short, although it is sometimes costly and risky to be the pioneer in new litigation issues, the early birds in the Y2K litigation may indeed be the only ones to get the worm.

In addition to the expected insurance litigation, the Y2K issues are expected to produce tort and contract litigation in two potential categories. If remediation efforts are successful and the Year 2000 computer "disaster" is avoided, there will be litigation seeking reimbursement for remediation costs and other consequential damages, such as business interruption. If there are computer failures, then there will likely be claims for any resultant losses, including lost data, business interruption, property damage, personal injury and other consequential damages. Under either scenario, the parties will need to consider the facts under the following legal theories:

(1) Breach of Express Warranties.

Claims for breaches of express warranties will most likely exist on the basis of the language contained in purchase and service contracts or license agreements; however, such warranties may also exist on the basis of advertising, trade publications, verbal representations, product specifications, and the parties' course of dealing.

Of course, the potential application of the Uniform Commercial Code may have a significant influence on the determination regarding express warranties in any particular case. According to the Uniform Commercial Code, the terms "guarantee" or "warranty" do not have to be used in order to create an express warranty. Likewise, it is not necessary that the

seller have the specific intent to create a warranty. In some situations, representations, whether oral or written, made prior to the written agreement, even in the presence of an integration clause, can create express warranties.

The express warranties governed by the Uniform Commercial Code pertain to the sales of "goods". There is still significant debate regarding the classification of computer software as "goods". Similar debates have previously occurred in the realm of the intellectual property issues surrounding computer software. The prevailing thought is that software is generally classified as "goods" rather than services. There may be special situations where a better argument exists that the product purchased is an intellectual application by the programmer rather than the software itself, and thus, a purchase of a service rather than "goods".

(2) Breach of Implied Warranties:

Implied warranties are created as a matter of law by the Uniform Commercial Code in sales of goods unless explicitly disclaimed.

(A) Implied Warranty of Merchantability.

In all sales of goods, there is an implied warranty that the goods will be fit for the ordinary purpose for which they are typically used. The sellers' implied warranty of merchantability extends to subsequent users and there is no requirement of privity of contract.

In the Y2K context, it is expected that users will assert that software which is not Y2K compliant cannot be used for its ordinary purposes. On the other hand, if the software is used for a period of time prior to any failure, the seller can argue that the goods were used for their ordinary purpose.

(B) Implied Warranty of Fitness for a Particular Purpose.

An implied warranty of fitness for a particular purpose arises when the seller has reason to know of the particular purpose for which the goods are required and the buyer is relying on the seller's skill or judgment to select or furnish suitable goods. This warranty obviously arises in situations where the software is customized to the needs of a particular client. This implied warranty is not likely to apply to general consumer software. Obviously, assurances that the product is Y2K compliant may create a potential claim for breach of implied warranty of fitness for a particular purpose if there is subsequent failure.

(C) Limitations and Disclaimers of Warranties.

Both express and implied warranties can be significantly limited or disclaimed by the seller. Historically, courts have construed disclaimers and limitations more strictly against the sellers and in favor of retail consumers but have been less forgiving to more sophisticated purchasers who may be on an equal or superior economic basis to the seller. Express warranties, stated in the contract, are enforced, even if there is disclaimer language also in the contract. For this reason, most express warranties are carefully worded and the scope, duration and available remedies to the purchaser are usually limited.

Implied warranties may be disclaimed with blanket disclaimers using common words such as "as is". Conspicuous language which informs the purchaser that the product is being sold with no implied warranty is sufficient to disclaim such warranties.

Rather than totally disclaiming any warranties, a seller may limit recovery to a specific liquidated amount. The seller may also provide a specific and exclusive limited remedy such as repair or replacement of the goods. The seller may also limit its liability to the buyer by excluding liability for incidental or consequential damages. The seller may also limit the time in which a remedy may be sought by the buyer. The limitation of liability and

more specifically, the limited and exclusive remedies contained in many computer agreements are expected to be topics of much debate and litigation.

(3) Breach of Contract.

The primary actions for breach of contract by the purchasers of computer goods will be the breaches of warranty provisions discussed above. It is expected that other breach of contract actions will arise out of the anticipated failures of non-compliant computer goods. Any provider of services or goods who relies upon a computer system for the provision of those services or goods may be subject to such a claim. If a Y2K failure occurs which prevents the provider from supplying the goods and services under the terms of a contract, a Y2K related breach will occur. Contract providers of goods and services are now frequently limiting liability for contract breaches due to Y2K problems. Contractual purchasers of goods and services, or their auditors, are well advised to pay close attention to such limitations of contractual liability.

(4) Product Liability/Strict Liability.

In situations where a Y2K failure results in property damage, personal injury, or death, there may be an action pursued for product liability. Such actions typically include claims for personal injury, death or property damage caused by or resulting from the manufacture, construction, design, formulation, development of standards, preparation, processing, assembly, testing, listing, certifying, warning, instructing, marketing, advertising, packaging or labeling of any "product". For product liability cases brought as a result of a Y2K failure, the courts must first grapple with the issue of whether the computer software or application constituted a "product". As noted above in the discussion of warranties, some situations may be more appropriately described as a provision of services rather than a "product".

In most jurisdictions, in order to establish that the produce is "defective" and to recover under strict liability, it must be established that the product was sold in a condition which constitutes an unreasonably dangerous threat of injury when the product is used in a manner intended. An important factor is how safe or dangerous the product is, when used as it was intended or should reasonably have been anticipated to be used. Additionally, liability depends on what a product manufacturer would have anticipated had the manufacturer been aware of the condition of the product and potential incidents which could occur when the product was placed on the market. These factors are of critical importance when considering the sale and use of software products which are not Y2K compliant after a point in time when the Y2K issues were known and generally understood by the industry. It is expected that issues pertaining to recalls, the provision of retrofit or remediation services, warnings, and failures to warn, will result in substantial litigation regarding product liability claims.

(5) Negligence/Professional Malpractice.

Persons or entities who design, manufacture or sell computer software, remediation services or computer consulting services are subject to claims for negligence or professional malpractice for Y2K failures. Additionally, persons or entities who utilize computer systems for the provision of services may be subjected to claims for negligence or professional malpractice if their services are affected by Y2K failures. Typically, such claims are expected to be asserted against professions which rely heavily on computer systems such as accountants, stockbrokers, attorneys, banks and so forth. Although these are perhaps the most obvious potential defendants, virtually any person or entity who relies on a computer for the provision of services is vulnerable to such claims.

Additionally, companies which depend on computers for the production of products or the management of inventory may be subjected to negligence claims if their systems fail and there are certain resultant damages.

(6) Fraudulent Inducement/Unfair Trade or Business Practices.

A party may obviously be accountable in fraud for knowing misrepresentations of Y2K compliance or similar matters. Many jurisdictions also have statutes which may create actions for unfair business practices. For example, in a California case against multiple retailers, the plaintiffs claim that the retailers are guilty of "unfair business practices" because they sold computer products without advising consumers as to whether the products were Y2K compliant.

(7) Shareholder Derivative Suits/Directors' and Officers' Liability.

This topic is discussed in a separate section of the seminar.

(8) Copyright Infringement and Breach of Licensing Agreement.

This topic will be discussed in a separate section of the seminar..

(9) Miscellaneous.

There are a number of issues which are applicable to several of the above theories or which may impact the Y2K litigation. For example, it is relatively unusual to have significant economic damages to multiple parties without personal injury or property damage. Typically, courts have limited tort actions for negligence and product liability to instances where the damaged parties have suffered personal injury, death or property damage. Likewise, many jurisdictions preclude punitive damages for claims related to breaches of contracts. Because of the unique nature of the Y2K claims, it is expected that litigants will attempt to create exceptions to these and other general conventions.

The potential insolvency or bankruptcy of many defendants is a matter that must be carefully considered by litigants and the courts. Such matters are likely to be considered in the certification of class actions and the establishment of multi-district litigation.

Statutes of limitation will present a particularly complex quagmire for litigants. Most theories of liability present different statutory limitations and may be triggered by different circumstances. For example, the same facts which might limit a primary cause of action for negligence or product liability because of a shortened statutory period may allow an indemnity action which has a longer statute of limitations.

Importantly, costs or damages incurred for remediation may trigger the running of the statutory period under the "discovery rule" and damages may be limited if the party waits to see if there is an eventual failure. Contributory negligence for failure to remediate and issues regarding disclosures of readiness and compliance are also likely to contribute to the litigation issues.

It is expected that many parties to litigation will be both plaintiffs and defendants. In situations involving Y2K failures, the person or entity suffering the failure is likely to be a defendant if the failure effects the provision of goods or services to others. Likewise, that same party is likely to be a plaintiff to recover damages against the manufacturer or seller of the software product. Additionally, that party is likely to be involved in litigation with one or more insurers regarding the coverage of claims against the party and losses incurred by the party. Multi-party actions are a certainty and litigators must be wary of compulsory claims which may need to be asserted against various parties.

INSURANCE

It is axiomatic that a claim under an insuring agreement must involve a fortuitous event. In other words, insurers do not provide insurance for intended or expected events.

Undoubtedly, as claims for Y2K losses are presented, insurers will argue that some of those claims were not the result of a fortuitous event. Because of the pervasive awareness of the Y2K problem and the anticipated failures, insurers will argue that the failures were expected and not fortuitous. Such arguments may be more credible where the products were manufactured after the acquired knowledge of potential Y2K problems or users fail to make efforts to obtain Y2K compliance.

Claims for losses under insuring agreements will be either first party claims or third party claims. First party claims involve damages to the insured. Third party claims involve claims against the insured by other damaged or injured parties.

1. First Party Claims

As a result of Y2K problems, an insured may have costs of repairing or replacing a defective computer system. Additionally, an insured may have costs or damages, such as lost inventory or equipment damage, due to a computer failure. The insured may have a first party claim against their insurer for either or both of these types of damages.

First party policies are usually either an "all risk" or a "named peril" policy. An "all risk" policy provides coverage for losses occurring as a result of any risk. A "named peril" policy provides coverage for losses occurring only as a result of specifically stated events. First party policies frequently contain significant exclusions pertaining to interruption of power or utility services, extreme temperature variations in controlled environments, and mechanical breakdowns. First party policies also usually exclude or offer very limited coverage for electronic data processing losses or losses related to the replacement and restoration of information stored electronically. These exclusions may significantly impair the ability of an insured to recover for Y2K failures.

Generally, first party policies also require direct physical loss or damage to covered property in order to invoke coverage. Insureds who incur costs for remediation but do not sustain any physical loss from a Y2K failure may incur substantial difficulties in recovering under a first party policy.

Typically, business interruption coverage is an endorsement to a property policy but may occasionally constitute a separate first party policy. Business interruption coverage is provided to protect the insured from losses incurred during an interruption of its business as a result of some fortuitous event. Once again, physical loss is usually required to invoke the coverage.

Ordinarily, the applicable policy for first party claims is the policy in effect at the time of the physical loss or damage. Because of the predicted Y2K problems, many insurers have included exclusions for Y2K losses in their first party policies. As a result, it is expected that insureds may attempt to "trigger" coverage in prior policies, similar to the tactics that have been used successfully in third party claims. Because of notice limitations contained in all policies, it is essential that the insured provide notice of the loss or claim to every possible or potential insurer as soon as possible.

2. Third Party Claims

As in the case of first party policies, most third party policies (usually a commercial general liability (CGL) policy) require physical damage to property or personal injury to invoke coverage. Claims related to economic losses without a concomitant physical damage may not constitute covered claims. Significant debate is expected over the issue of whether a physical loss or damage has occurred when a computer is rendered useless and of no value due to a Y2K problem or failure. The insurers of manufacturers and sellers of computers are certainly expected to argue that the claims made by purchasers and users cannot constitute

physical loss claims and thus do not constitute covered claims. It is important to note that there is a significant distinction in most third party policies between the insurers' duty to defend and the duty to indemnify for claimed losses. The duty to defend has been broadly construed and is frequently applicable even though there may be no duty to indemnify. Thus, many insureds may obtain the benefit of a defense while litigating the issues of the indemnity coverage.

Undoubtedly, insurers will argue that an occurrence has not taken place during the applicable coverage period and that some other insurer must provide the coverage. These issues have arisen in many other situations and the courts have developed multiple theories for determining the "trigger" of coverage. These theories include the following:

- A. Exposure Theory: Coverage is triggered by exposure to the injury causing product.
- B. Manifestation Theory: Coverage is triggered at the time of the manifestation of the injury or damage.
- C. Continuous Trigger: Coverage is triggered continuously from the time of the exposure to the manifestation of the damage or injury.
- D. Injury In Fact: Coverage is triggered by a showing of an actual injury producing or damaging event during the policy period.
- E. Double Trigger: Coverage is triggered at both the time of exposure and the time of manifestation of damages or injury but not in the interval between the exposure and manifestation.

These theories are not particularly applicable to the Y2K claims because continuous injury causing events are not likely. There could possibly be latent injuries that manifest at subsequent dates; however, it is anticipated that most damages and injuries will be readily

known. The triggering theories which have been developed are indicative of the willingness of courts to adopt new theories to invoke insurance coverage and may suggest appropriate triggering theories for Y2K coverage. In the Y2K litigation, it is not yet known whether coverage will be applied at the time of the sale of the product, the time of failure, the time of actual injury of damage, all of these times or some other time created by the courts. Without question, claimants will present creative and persuasive arguments to establish trigger dates that will invoke applicable coverage. As with first party claims, insureds must provide prompt notice of claims and should provide all possible insurers with notice since the triggering dates are not established.

3. Errors and Omissions Claims

Errors and omissions (E&O) policies apply to claims arising out of errors or omissions in the provision of professional services. As discussed above with respect to warranty claims in litigation, if the services involve the provision of software, a significant point of debate will be whether the professional was involved in providing services or selling goods. If the services are characterized as the sale of goods, warranty claims will apply; however, the E&O coverage will likely be avoided.

4. Directors and Officers Insurance

This topic is covered in a separate section of the seminar.

5. Y2K Exclusions and Y2K Policies

Exclusions for Y2K problems are rapidly being developed and incorporated into policies. The Insurance Services Office (ISO) has several standard exclusions which are now being utilized frequently within the industry. Additionally, some companies are now providing Y2K policies to insure against specific Y2K losses; however, because of the

uncertainty regarding the Y2 litigation and potential damages, there does not appear to be any consistency between the coverages provided or the premiums charged.



**YEAR 2000: DIRECTOR AND OFFICER LIABILITY
AND THE BUSINESS JUDGEMENT RULE**

Kenneth J. Tuggle
Brown, Todd & Heyburn PLLC
Louisville, Kentucky

Copyright 1999, Kenneth J. Tuggle. All Rights Reserved.

SECTION E

**YEAR 2000: DIRECTOR AND OFFICER LIABILITY
AND THE BUSINESS JUDGEMENT RULE**

TABLE OF CONTENTS

I.	SOURCES OF LITIGATION	E-1
II.	REDUCING DIRECTORS' AND OFFICERS' EXPOSURE	E-2
III.	REDUCING DIRECTORS' AND OFFICERS' POTENTIAL LIABILITY	E-3
IV.	CREATE A DUE DILIGENCE RECORD	E-5
V.	APPLY DUE DILIGENCE STANDARDS	E-5
VI.	MONITOR RESPONSES BY COMPETITION	E-6
VII.	INVESTIGATE CLAIMS AGAINST THIRD PARTIES	E-6
VIII.	IDENTIFY EXPOSURES TO THIRD PARTIES	E-7
IX.	THIRTEEN DATES TO CHECK FOR Y2K COMPLIANCE	E-8



Y2K

The Year 2000 Crisis

Management Liability and Protection

Sources of Litigation

- **Federal Securities and Anti-Fraud Laws**
- **Contract, Tort and Other State Law Claims**
- **Copyright Infringement Claims**
- **ERISA Claims**
- **Derivative Suits**
- **Breach of Duty Claims**

Reducing Directors & Officers Exposure

- **The Most Effective Defense to Most Y2K Claims Is Successful Remediation**
 - **Directors and Officers Must Be Able to Document**
 - **They Took All Reasonable Steps to Attempt Remediation and**
 - **They Made All Required Legal Disclosures**

Reducing Directors & Officers Exposure

- **Legal Defenses:**
 - Business Judgement Rule**
- **Be Disinterested**
- **Act In Good Faith**
- **Make Informed Decision Only After**
 - **Making a Reasonable Effort**
 - **To Ascertain and Consider**
 - **All Relevant Information**
 - **Reasonably Available**

Reducing Directors & Officers Exposure

- **Legal Defenses: Reliance**
- **Ability to Rely Upon Persons With Specific Expertise In the Subject Matter**
 - **Board Committees**
 - **Other Officers**
 - **In-House or Outside Experts**
 - **Counsel**

Reducing D&O's Potential Liability

- **Determine the Extent of the Issue**
 - **Examine the Company's Own Systems**
 - **For Y2K Compliance**
 - **For Leap-year Compliance**
 - **For Ability to Deal With "Magic Dates"**
- **Formulate, Implement, Track and Test a Remediation Plan**
- **Control Future Transactions**

Reducing D&O's Potential Liability

- **Get Representations of Y2K Compliance From Outside System Vendors**
- **Clarify Who Pays for Any Upgrade Necessary for Y2K Compliance**
- **Seek Y2K Compliance Certifications From Key Suppliers and Vendors**
- **Certify Key Suppliers', Vendors' and Customers' Systems**

Reducing D&O's Potential Liability

- **Consider Direct Testing and Evaluation for Truly Crucial Third-parties**
- **Identify Alternative Solutions, Respective Costs and Time Schedules**
- **Select and Promptly Implement the Most Favorable Alternative(s)**
- **Adopt Appropriate Time Schedule**
- **Adopt Contingency Plans**

Create A Due Diligence Record

- **To Document Your Successful Remediation Effort**
- **To Defend The Company In Litigation**
- **To Support A Business Judgement Defense For D & O's**
- **To Reassure Third Parties - e.g. Customers, CPAs and Regulators**
- **To Support A Due Diligence Defense Under Securities Laws**

Apply Due Diligence Standards

- **Act In Good Faith**
- **Act With Due Care**
- **Act In The Best Interests Of The Company**
- **Act Upon Due Inquiry**
- **Exercise Fiduciary Duties Properly**
- **Avoid Corporate Waste**

Monitor Responses By Competition

- To Be Aware of Emerging Best Practices**
- To Gain/Maintain Competitive Advantage**

Investigate Claims Against Third Parties

Identify Exposures to Third Parties

Questions?

Ken Tuggle
502-568-0269
ken@lou.bth-pllc.com

13 DATES TO CHECK FOR Y2K COMPLIANCE

DATE	REASON
April 9, 1999	9999 on the Julian calendar, incorporated into many computer programs. The 99th day of the Year 1999. 9999 denotes "end of input" in many computer programs.
September 9, 1999	9999 on the Gregorian calendar. 9999 denotes "end of input" in many computer programs.
December 31, 1999	Last day in year 1999.
January 1, 2000	Beginning of the Year 2000.
January 3, 2000	First business day in the Year 2000.
January 10, 2000	First date to require a 7-digit date field (1/10/2000).
January 31, 2000	End of the first month of 2000.
February 29, 2000	Leap year day.
March 31, 2000	End of first quarter of 2000.
October 10, 2000	First date to require an 8-digit date field (10/10/2000).
December 31, 2000	End of Year 2000.
January 1, 2001	Beginning of Year 2001
December 31, 2001	Check that year has 365 days.

**DOMAIN NAMES, TRADEMARKS &
COPYRIGHT ISSUES IN CYBERSPACE**

Joel T. Beres
Wheat, Camoriano, Smith & Beres, PLC
Louisville, Kentucky

Copyright 1999, Joel T. Beres. All Rights Reserved.

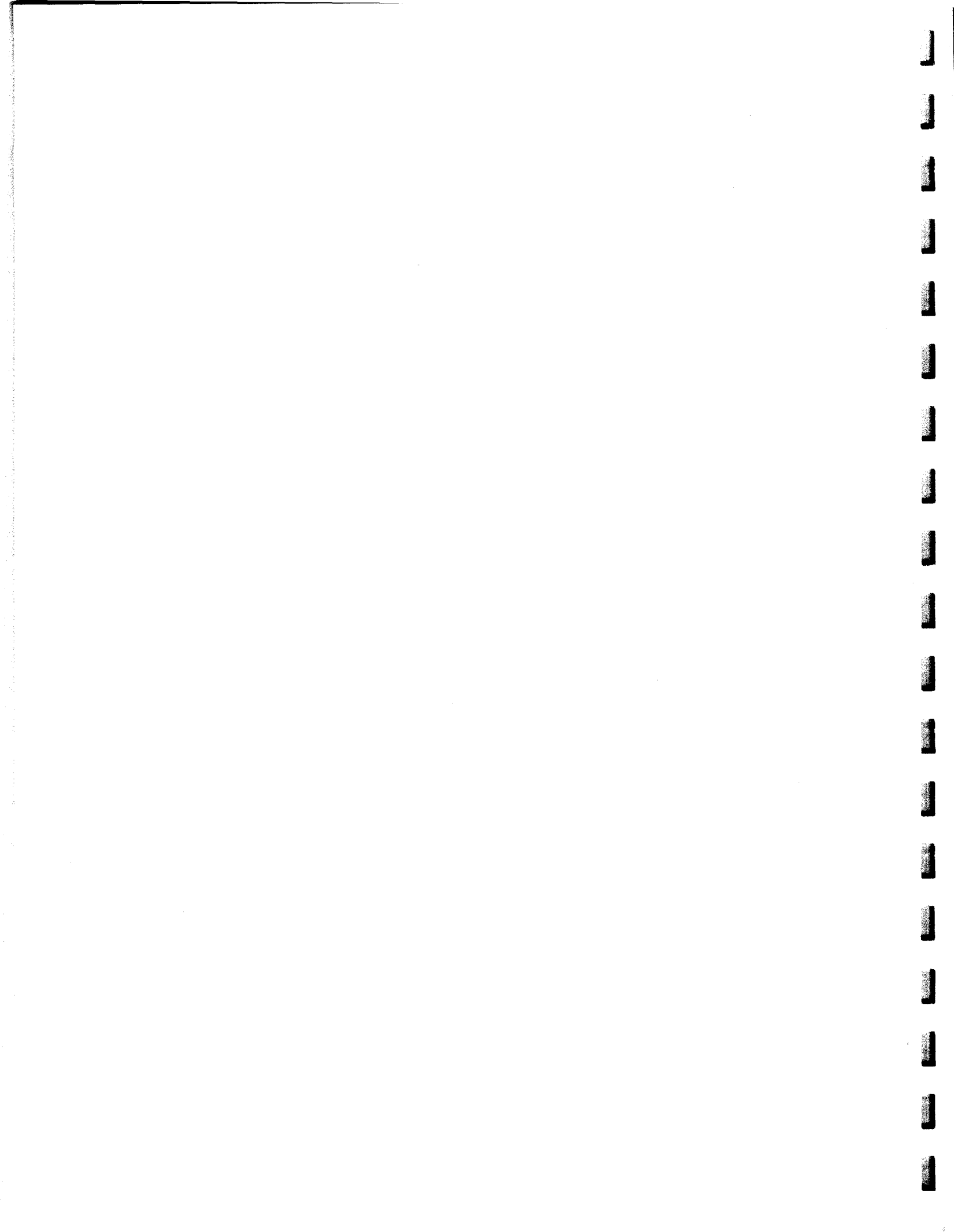
SECTION F



DOMAIN NAMES, TRADEMARKS & COPYRIGHT ISSUES IN CYBERSPACE

TABLE OF CONTENTS

- I. Dan L. Burk, *Trademarks Along the Infobahn: A First Look at the Emerging Law Of Cybermarks*, 1 Rich. J.L. & Tech. 1 (1995). This article may be found online at <http://www.richmond.edu/jolt/vlii/burk.html> and is reprinted with the permission of the author. F-1**
- II. John W. Scruton, *battle.com: Trademark Issues Relating To Domain Names* (1998). This article may be found online at <http://www.iplawky.com/wcsb/domain.htm> and is reprinted with the permission of the author. F-23**
- III. Network Solutions, Inc. currently effective domain name registration agreement. <http://www.networksolutions.com/legal/dispute-policy.html> F-35**
- IV. Network Solutions, Inc. currently effective Domain Name Dispute Policy (Rev. 03). <http://www.networksolutions.com/legal/dispute-policy.html> F-43**
- V. Network Solutions, Inc. help page regarding its Domain Name Dispute Policy. <http://www.networksolutions.com/help/general/dispute.html> F-49**
- VI. Ellen Rony (Stanford University, M.A. Communications) and Peter Rony (University of California, Berkley, Ph.D. Chemical Engineering), *The Domain Name Handbook: High Stakes and Strategies in Cyberspace* (1998). The table of contents of this work may be found online at <http://www.domainhandbook.com/toc.html> and is reprinted with the permission of the authors. F-57**
- VII. United States Patent & Trademark Office statement on examination of domain names for registration. <http://www.uspto.gov/web/offices/tac/domain/tmdomain.htm> F-67**
- VIII. United States Patent & Trademark Office statement on identification and classification of certain computer related goods and services. <http://www.uspto.gov/web/offices/tac/domain/domc.html> F-69**





**Trademarks Along the Infobahn:
A First Look at the Emerging Law of Cybermarks**

by Dan L. Burk

April 10, 1995

Cite As: Dan L. Burk, *Trademarks Along the Infobahn: A First Look at the Emerging Law of Cybermarks*, 1 RICH. J.L. & TECH. 1 (1995) <<http://www.richmond.edu/jolt/v1i1/burk.html>>.

Copyright © 1995 by Dan L. Burk. Portions of this paper were presented at the symposium on Community in Cyberspace: The Emerging Law of Technology," sponsored by the Richmond Law & Technology Association, University of Richmond, February 4, 1995.

Introduction

{1} Use of the global Internet computer network is rising exponentially.[1] As Internet subscription increases disagreements between users are expected to arise, just as where any sizeable number of human beings interact, disagreements may be expected to arise. To date, on-line disputes have been primarily dealt with via informal solutions, such as the polite conventions of "netiquette" shared by Internet users.[2] However, as the community of Internet users grows increasingly diverse, formal dispute resolution mechanisms, embodied as law and legal institutions, may be called upon by the parties to resolve disagreements. For example, several acrimonious disputes have already arisen over the use of particular "domain names" on the Internet. This paper discusses how established principles of trademark law may be applied to resolve such controversies. Such a discussion properly begins with a review of the nature and function of the global Internet.

The Internet Experience

{2} The Internet has been called a network of networks -- local computer systems hooked to regional systems hooked to national or international high-capacity "backbone" systems.[3] Each link or node in this web is a computer or computer site connected together by a variety of connections: fiber optic cable, twisted-pair copper wire, microwave transmission, or other communications media. Each computer in the network communicates with the others by employing machine-language conventions known as Internet Protocols ("IP").[4] Indeed, these protocols define the network; the Internet is the linked mass of machines which use IP to communicate.

{3} Smart Communications: Unlike other communications media that tie up the entire channel during transmission, the Internet breaks information into discrete packets that can be transmitted as capacity allows. The packets follow any of a number of different routes from computer to computer until they reach their destination, where they are reassembled by the recipient machine. Each computer in the network assesses whether to temporarily hold packets or send them on, so that maximum use is made of the available carrying capacity at any given time.[5]

{4} Decentralization: There is no centralized control of the Internet. From a technical standpoint, each computer acts autonomously, coordinating traffic with its nearest connected neighbors, and guided only by the "invisible hand" that arises from the sum of millions of such independent actions.[6] From a management standpoint, each node is similarly autonomous, answering only to its own systems administrator. This means that there is no central authority to govern Internet usage, no one to ask for permission to join the network, and no one to complain to when things go wrong.

{5} Telepresence: The Internet protocol provides geographically extended sharing of scattered resources. An Internet user may employ her Internet link to access computers, retrieve information, or control various types of apparatus from around the world. These electronic connections are entirely transparent to the user; the "virtual machine" created by the connection appears to be the one at the user's fingertips. Indeed, the user may be completely unaware of the geographic location of the resource being accessed.

{6} These features make available a vast array of interconnected information, including digitized text, graphics, and sound. The totality of this international information structure is commonly referred to as "cyberspace," a cognitive realm that is conceptually separate from the real space that we physically inhabit. "Cyberonauts" who traverse this digital landscape find that virtual relationships with other electronic pilgrims blossom into collaboration, friendship, and even romance. Virtual communities coalesce from all corners of the globe to exchange information and reinforce shared values. And, increasingly, the universal human proclivity toward arbitrage and commerce is becoming an important component of on-line interaction.

Virtual Commerce

{7} The Internet began as a product of Cold War military technology, linking together researchers involved in a research program sponsored by the U.S. Department of Defense.[7] This system for communicating and sharing computer resources became increasingly important to the scientific community; much of the funding, as well as management of the net's high speed backbone connection became the responsibility of the National Science Foundation ("NSF").[8] There was little opportunity for commercial Internet traffic in the days of government sponsored research usage. Indeed, the NSF promulgated an acceptable use policy ("AUP"), forbidding such use of the publicly-funded Internet backbone connections.[9]

{8} As the benefits of Internet access became better known, the usefulness of computer networking was not lost on business, or for that matter, on consumers. A crop of private Internet access providers developed, offering network access and facilities for customers outside the research community.[10] In order to route traffic around facilities restricted by the NSF's AUP, these providers formed the Commercial Internet Exchange ("CIX"), which sponsored high-speed links for commercial

traffic.[11] In the meantime, NSF slowly began to edge its way out of the Internet management business: first, by funding regional networks; then by contracting oversight duties out to private firms; and finally by encouraging the regional networks to find paying customers.[12] By early 1995, NSF's sole duty will be to fund a few Network Access Points, or NAP's, to act as data traffic exchanges.[13]

{9} Consequently, although the academic and scientific research communities remain an important part of the Internet community as a whole, private and commercial traffic is becoming a dominant force in the development and growth of the "electronic frontier." Businesses of all types routinely use the Internet for a variety of commercial transactions, and consumer services have begun to appear. It is presently possible to access a variety of mail-order catalogs on-line, and arrange for the purchase of music, books, fast food delivery, and even flowers. The variety and availability of similar consumer services is likely to grow. But in order for customers to order commodities, they must first be able to locate and recognize the commodities among the sprawling data connections of cyberspace.

Internet Locators

{10} In order for the Internet to function, there must be some manner of distinguishing and locating all the various computers, users, files, and other resources attached to the net. Host machines must know which information packets are intended for a particular machine; which packets must be passed on; and the ultimate destination of packets that are passed to the next machine. Machines must also be able to differentiate themselves from other machines. This is accomplished via Internetworking Protocol Addresses ("IP addresses").[14] Assignment of IP addresses to users is the responsibility of the Internet Assigned Numbers Authority ("IANA"), a private entity with ties to international standard-setting bodies such as ANSI. IANA delegates the administration of IP address applications and registrations via InterNIC Registration Service, operated by a private firm called Network Solutions.[15]

{11} At the time of this writing, IP addresses are divided into classes A, B, and C; this system may change somewhat with the introduction of the next anticipated version of the Internetworking Protocols. Classes A and B are, much like certain frequencies of the electromagnetic spectrum, reserved for special uses. Class C addresses are assigned to network access providers in blocks of numbers; these blocks may then be divided and subdivided among that provider's users. Each address within a block is potentially a unique designator for some entity on the network.

{12} IP addresses are represented as strings of digits divided into parts, or fields. By convention, the fields in the IP address are separated by periods. For example:

124.33.45.112

might be a typical Internet address. Each address contains a network portion, the IP network address, and a local portion, called the local address. The network portion begins on the left, the local portion ends on the right; the exact division between these portions is determined by the class of the address.[16] The combination of these local and network portions uniquely identifies and specifies the location of some interface on the Internet. Unfortunately, using these numerical strings is somewhat inconvenient and cumbersome; Internet users may find it difficult to routinely remember and use such addresses. Consequently, the IP Address system has been overlaid with a more "user-

friendly" system of domain names.[17] This overlay allows Internet resources to be assigned a mnemonic designation that is more easily remembered. Internet applications have been designed to automatically look up the IP Address corresponding to mnemonic designations; this is done through a facility called the Domain Name Service ("DNS") which operates invisibly to the Internet user.[18]

{13} Like IP addresses, domain names are divided into fields separated by periods. An example would be:

dickens.oliver.twist.com

Read from right to left, fields designate the computer, subdomains, and domains of the address in proximity to the user. The rightmost field is the top-level domain, a standardized designation showing the type of organization or the country to which the address belongs.[19] There are a variety of such top-level designators. For example, the designation ".com" indicates a commercial organization, ".gov" indicates a governmental organization; ".net" indicates an organization running a computer site or network; and ".org" is a classifier for miscellaneous organizations. Country designators include ".uk" for the United Kingdom; ".nl" for the Netherlands; and ".ca" for Canada.[20]

{14} As with IP addresses, IANA is responsible for assigning domain names, and has delegated the operation of a name registry to the InterNIC.[21] InterNIC acts merely as a recorder; domain names may be requested by electronic mail and are assigned on a first-come, first-served basis.[22] Once an organization or a person has registered a domain name, it may do as it wishes with that name: they can use it, reassign it, or simply hold it unused. Because domain names are simply mnemonics, and because there is no logical connection between them and the IP address that in fact locates an Internet resource, domain names are fully portable, and can be transferred to a new machine or site if the name holder moves.

{15} Given that domain names were instituted as mnemonics to aid recollection of Internet resource locations, one might expect that the use of such names will become critical where remembering a resource is critical -- as for example, where money is at stake in Internet commerce. The importance of such names for commerce on the Internet has been demonstrated most recently by a series of legal and quasi-legal disputes over possession and use of certain domain designations. For example, in one early scuffle, Wired magazine, which maintains the Internet site "wired.com," objected to the use of the domain name "wire.net" by an organization called "Women's Wire." That dispute was quickly settled when Women's Wire changed its domain name to "wwire.net" in order to avoid a legal confrontation.[23] However, subsequent disputes such as those discussed below have been more protracted.

MTV v. Curry

{16} Perhaps the most notorious Internet trademark dispute to date is that involving Adam Curry and the MTV cable television channel. [24] Curry was formerly employed as a video jockey, or "VJ" host on MTV. Curry organized an Internet site registered as "mtv.com" during his employment period, apparently with the knowledge and approval of MTV. The site was devoted to discussion of topics related to Curry's vocation, including popular culture, entertainment, and celebrities.[25] He also established a considerable net presence by writing and circulating the "Cybersleaze Report," an

electronic newsletter devoted to celebrity gossip.[26] Curry's fame both on and off the Internet generated a high volume of traffic at the mtv.com site.[27]

{17} In 1993, Curry and MTV parted ways, apparently with some rancor. Among other items of dispute, MTV demanded that Curry surrender or disable the mtv.com site because it carried the designation "mtv." [28] Curry, who had registered the site's domain name under his own name, refused to do so. The parties moved their dispute to court. Pending trial, Curry suspended his operations at mtv.com and moved to a new and equally chic site registered as "metaverse.com." [29] The parties quietly settled the dispute on March 24, 1995, [30] and it appears that MTV is now in control of the mtv.com domain.

Kaplan v. Princeton Review

{18} Another Internet trademark dispute involved the Princeton Review, a purveyor of courses and materials to prepare students for standardized aptitude tests such as the SAT, LSAT, and GRE. In 1994, Princeton Review determined that its business could benefit from establishing Internet services where students could discuss test-taking strategies, acquire information and materials concerning aptitude tests, and most importantly, obtain promotional literature about Princeton Review's services. [31] The company subsequently established such an Internet site, and registered several domain names with the InterNIC, including "princeton.com" and "review.com."

{19} Princeton Review also registered the domain name "kaplan.com," and established an Internet site under that name. [32] Not surprisingly, the "Stanley Kaplan Review" is Princeton Review's chief competitor in the market for standardized test preparatory courses. The chief executive of the Princeton Review cheerfully admitted that his company registered its chief rival's name in order to mock and annoy the other company. [33] Additionally, Princeton Review hoped that cybersnobs hoping to contact the Kaplan Review company would sign on to the kaplan.com site. Individuals who mistakenly did so were offered electronic materials disparaging the quality of Kaplan Review's services and extolling the comparative advantages of the Princeton Review courses. [34]

{20} The Kaplan Review had no on-line presence but became aware of the rogue Internet site in relatively short order. Kaplan Review demanded that Princeton Review cease using the Kaplan name in conjunction with the site. Princeton Review offered to surrender the domain name in exchange for a case of beer -- either domestic or imported. Kaplan Review declined the settlement, opting instead to pursue a legal remedy. The President of Princeton Review quipped in response that his rivals had "no sense of humor, no vision, and no beer." [35] A lawsuit was initially filed but the dispute was subsequently removed to binding arbitration. The arbitrators determined that Princeton Review should surrender the site to Kaplan Review. [36] Princeton Review did so, but vowed to register instead the domain name "kraplan.com," which, like the kaplan.com during Princeton Review's control, would be devoted to comparative advertising disparaging Princeton's competitor. [37]

McDonald's v. Quittner

{21} The most recent Internet trademark dispute was created by a magazine writer attempting to generate material for his column on the Internet. In the course of writing about businesses that fail to

register their names as Internet domains, writer Joshua Quittner reviewed the list of registered domain names and noted that no one had registered the name of "McDonald's," the renowned fast food chain. Quittner then contacted McDonald's corporation to get a statement regarding their failure to protect their famous name. No statement appeared forthcoming, so Quittner generated the story by registering "McDonalds.com" himself, activating the site, and circulating his new e-mail address as "ronald@mcdonalds.com." Some messages urged him to use the site to promote vegetarianism, other messages urged him to offer the domain name back to McDonalds in return for an exorbitant price.[38]

{22} Quittner did indeed offer the name back to McDonald's in one of his magazine columns, but not in exchange for money. In a manner reminiscent of the Princeton Review, he instead offered to surrender the domain name if McDonald's corporation would underwrite some Internet equipment for a grade school.[39] This and other provoking articles caught the corporation's attention; they responded not by funding grade school computer access, but by pressuring the InterNIC to revoke Quittner's registration of the name. Although the registry had stayed out of previous disputes such as the Adam Curry litigation, sticking tenaciously to its "first-come, first-served" policy, it wavered before this new corporate threat. InterNIC first resisted McDonalds' demands, then eventually agreed to revoke the registration, then changed its mind again, leaving the registration with Quittner.[40] McDonald's ultimately agreed to donate \$3,500 to purchase the equipment.[41]

Trademark Law

{23} The disputes described above all involve some disagreement over the use of a distinguishing business name. This type of disagreement is by no means limited to the Internet, and in real space has generated a substantial body of law regarding the use, ownership, and infringement of trademarks. Trademarks comprise a type of intellectual property used to identify the source of goods or services.[42] Technically, marks used to identify goods are referred to as "trademarks," and marks used to identify services are referred to as "servicemarks." Generally, however, trademarks and servicemarks are treated as equivalent under federal trademark law.[43] Such rights serve both to protect the public by preventing fraud and confusion regarding the origin of goods, and also to protect the goodwill and name recognition of businesses that have invested in improving and distinguishing their products.[44]

{24} Trademark rights exist at common law, and most states recognize and enforce such rights. The United States Congress has also recognized and extended these rights via federal statute, and this source of trademark rights has become paramount in the United States.[45] The federal trademark statute, or Lanham Act, provides a national registry for trademarks, generating nationwide protection for registered marks. The statute also provides for enforcement of either registered or unregistered marks.[46] Trademark owners who wish to sue for trademark infringement under the statute must first show that they have a protectable mark. Protectability is largely a function of the strength of the mark; some marks are highly distinctive, or "strong" marks, others are less distinctive or "weak." Some marks may be accorded no protection at all.

{25} Trademark strength is usually assessed by reference to five categories: arbitrary, fanciful, suggestive, descriptive, and generic. As listed here, they range in descending order of strength, with arbitrary or fanciful marks receiving the greatest protection. Arbitrary marks are well-known words that are used to identify goods or services to which they have no relation -- "Apple" computers, for

example.[47] Fanciful marks are invented words, such as "Exxon," applied to goods or services.[48] Each of these types of marks is considered inherently distinctive because their only association with the marked goods or services is the association gained in the marketplace.

{26} Suggestive marks are also inherently distinctive, but are weaker than an arbitrary or fanciful mark because a consumer with some thought or imagination could discern the nature of the goods from the suggestive mark.[49] Descriptive marks require little imagination to discern the nature of their associated goods, and are not considered inherently distinctive.[50] As such, descriptive marks are not protectable unless the holder can show "secondary meaning," that is, an association in the minds of consumers between the mark and that particular source of the product or service. Where secondary meaning can be shown, the law declines to allow competitors to "free ride" off of a business' goodwill and recognition by using an otherwise descriptive mark.[51]

{27} Generic terms are terms commonly descriptive of a class of goods or services, and are unprotectable.[52] They simply name the good or product. Generic terms are not recognized as protectable marks because they are terms that all competitors in that market require in order to describe their products. Allowing one business to monopolize the term would hamstring the competitive efforts of all other such businesses.[53] Some terms, such as "toothpaste" are born generic; others such as "escalator," have genericness thrust upon them by becoming a common descriptive name in the mind of the public.

{28} If the plaintiff in a trademark suit can show that she has a protectable mark, she must then demonstrate that the use of an infringing mark is likely to result in consumer confusion as to the source of the marked goods. Courts evaluating the likelihood of confusion may review a variety of factors, none of which are dispositive. Factors that a court may review include the similarity between the marks, the strength of the plaintiff's mark, the defendant's intent or bad faith in adopting a similar mark, the "proximity" of the goods in advertisement, marketing and distribution, instances of actual confusion, and the sophistication of consumers of the goods.[54] Remedies that may be awarded to a plaintiff who successfully demonstrates trademark infringement include injunctive relief, recovery of unjust profits, damages and costs.[55]

Names and Addresses

{29} The fit between trademark law as developed in real space and domain names used in cyberspace may to some extent depend on the ability to classify domain names as either names or addresses. In general, names are thought of as discrete emblems used to establish or designate identity; addresses are thought of as emblems designating location. Trademarks and servicemarks are clearly names; they designate or identify goods and services. They are not used to locate a good or service, or even to indicate the producer's place of origin -- they indicate the source or affiliation of the item. Trademarks also have the portability associated with an individual designator or name -- when a business moves, the trademark goes with it; the mark is not tied to the particular location.[56]

{30} Domain names might seem to be unusual because they appear to be *both* names and addresses; they both locate and identify Internet resources.[57] Yet even in real space, this division is not pristine. People's personal names, for example, establish identity, and such identifiers travel with the individual rather than changing when the person changes location. Street addresses or geographic names, by contrast, are more static in order to establish location. Yet such addresses and geographic

names also serve to identify the physical place, differentiating it from other places.

{31} Geographic names and street addresses also change; indeed, there is no particular reason why a person who moves from one house to another could not take his street address with him -- this might be undesirable in cities, where the address scheme frequently follows some order. But in rural settings, where the address may simply be "Chatham Farm," the name/address could certainly move with its user. Geographic names of all kinds -- street addresses, zip codes, counties -- are in fact overlays on an unchanging numerical system of longitude and latitude, which is a universally recognized designator and locator for a particular place on the earth's surface. In this sense, geographic names are much like Internet domain names, which are an overlay on the "real" IP number designations.

{32} Telephone numbers share the same dual nature. At one time, telephone numbers were "hard-wired" and a particular number was associated solely with a particular telephone line. However, as switching technology advanced, numbers became more portable. Telephone numbers are no longer necessarily tied to one place -- it is common for a person or business to take their telephone number with them when they move, especially within the same area code. In this respect, the number seems more like a name. Yet, a telephone set, fax machine or modem that is plugged into a new telephone line changes "address," that is, a different number must be dialed to establish a connection to the instrument. Thus the number establishes the location of a particular endpoint on the telephone network.

{33} If trademark law contemplates only the use of a designator as a name, then application of trademark law to domain names, with their dual nature, might be problematic. However, it appears that a fair number of designators in "real space" share this dual nature of acting as both a name and an address. Domain names may be analogous to real space designators such as geographic names or telephone numbers. To the extent that trademark law recognizes such real space designators as trademarks, it may be readily applicable to domain names as well.

Geographic Names

{34} One real space analogy to domain names might be geographic place name; trademark law relating to names such as street addresses might be instructive in determining the proper legal treatment for domain names. As the discussion above suggests, domain names and geographic names share an amenability to be used as either names or addresses. However, trademark law generally seems to assume that geographic names are in fact addresses, and so, like generic terms, are unprotectable because everyone needs them to locate the place in question.[58] Geographic names may be entitled to legal protection if they attain secondary meaning as to the source of goods, but not if they are merely descriptive of the goods' place of origin.[59] As a consequence, under the Lanham Act, geographic place names as such cannot be registered as trademarks, and this has led some experts to opine that street addresses could not be registered as trademarks.[60]

{35} However, this rule assumes that the good or service takes its name from the place or address. This is not the case in the Internet trademark disputes encountered so far. To the contrary, the cyberspace "address," the Internet domain, has been named after goods or services that are well-known in real space. This phenomenon of using an established trademark to name a location is not entirely unknown off-line. Consider the following addresses taken from *Standard & Poor's*

Registry :

McDonald's Corp.
One McDonald Plaza
Oak Brook, IL 60521-1900

Coca-Cola Corp.
One Coca-Cola Plaza
Atlanta, GA 30313

Mohawk Tools Co.
One Precision Plaza
Crystal Lake, IL 60014-8263

Wolfemann's
One Muffin Lane
P.O. Box 15913
Shawnee Mission, KS 66285

{36} In each of these examples, the geographic address of the business has incorporated some distinctive name or mark associated with the business located at that address. Thus, the mark appears to have preceded the address. This is quite the inverse of the law cited above -- far from the mark containing a geographic name indicating the source of the goods or services, the geographic name instead contains an indicator of goods or services located there! This seems closely analogous to naming an Internet domain after the business that locates itself at that site.

{37} The marks in the addresses above run the gamut from arbitrary or fanciful to generic. The name "McDonald's" in no way suggests or describes food services, except that it has gained that association in commerce. In the case of Mohawk tools, the address name is significant only if one knows the firm's motto, "A Precision Twist Drill Company," in which case the term "precision," found in the address, appears to be descriptive and protectable if it has secondary meaning with regard to Mohawk tools. Finally, the address for Wolfemann, a purveyor of baked goods well known for their english muffins, carries the term "muffin," which would probably be considered generic. Interestingly enough, this address appears to be a pure mnemonic for Wolfemann's mail order catalogs, and the P.O. Box is the true postal address.

{38} The protectability of such addresses will likely be dependant on the strength of the mark given being employed as a postal or physical locator. But it is not hard to envision situations in which adoption of a similar address would constitute unfair competition. For example, if Pepsi-Cola were to set up an office in the same zip code as the Coca-Cola headquarters, and designate the address as "10 Coca-Cola Plaza," Coca-Cola might well have cause for complaint. This would especially be true if, much like Princeton Review on the Internet, Pepsi-Cola did so in the hopes of intercepting misrouted mail intended for Coca-Cola's headquarters, or perhaps even intercepting confused Coca-Cola clients or customers who had intended to visit "1 Coca-Cola Plaza."

{39} In such an instance, the factors indicating the likelihood of confusion would seem to translate well into an analysis indicating infringement by Pepsi: the name adopted as a postal address is a strong mark associated with a competitor's product, and the addresses differ by only a zero. The locations are in close physical proximity, and more importantly, in close *logical* proximity. Pepsi's motivation for adopting the address, to capture its rival's mail or clients, seems to be in bad faith, and

any misrouted mail or mistaken individuals would supply evidence of actual confusion. This analysis seems equally applicable to confusingly similar designators in cyberspace, particularly where the designation appears to have been adopted to specifically capitalize on anticipated confusion.

Broadcast Designators

{40} Trademark parallels to Internet designators are also found in the identifying names or addresses for broadcast services, albeit subject to the peculiarities of the broadcast medium. Two broad classes of disputes emerge in the area of broadcasting identification marks: those involving call letters, and those involving frequency designations. Each broadcaster carries a designator, similar to the IP addresses and domain names of the Internet. An additional similarity is that domain names and IP addresses are assigned by a central authority, the InterNIC, much like the way the Federal Communications Commission ("FCC") assigns call letters and frequencies to broadcasters. However, unlike the designators on the Internet, the two types of broadcast designators are somewhat uncoupled: there is no equivalent to the Domain Name Service utility for radio or television. If there were, listeners or viewers could enter a station's call letters and have the receiver automatically tune to that station's frequency.

{41} As a consequence of this separation, the naming and locating functions of broadcast designators have become somewhat discrete, unlike Internet domain name functions. Call letters in broadcasting tend to function as names rather than as addresses. Radio and television station call letters are assigned by the FCC, with each station receiving a distinctive set of letters.[61] However, broadcasters are able to request particular call letters, subject to the constraint that call letters of stations east of the Mississippi must begin with a "W" and call letters of stations west of the Mississippi must begin with a "K." [62] Much like the assignment of domain names by the InterNIC, call letters are assigned by the FCC on a "first-come-first-served" basis.[63] Stations frequently employ homonyms to identify their call letters, such as "Kiss" for a soft-music station bearing the letters WKSS,[64] or "Warm" for a soft-music station bearing the letters WRMM.[65] Acronyms such as WBCS for "We're Boston's Country Station"[66] are also sought. This is somewhat similar to the way Internet domain names may indicate the domain site operator, but lacks a similar locating function.

{42} Call letters have been treated for the most part as arbitrary marks. The letters chosen tend not to describe or even suggest the nature of the service designated. Instead, they indicate only broadcast music of one sort or another. This tends to put the junior user of a similar call letter set at a severe disadvantage when a court assesses the likelihood of confusion. For example, where a new radio station adopts the letters "WMEE" and an existing station already uses "WMCZ,"[67] or where an established television station uses the letters "WBOC" and a new station attempts to use "WBOT,"[68] the factor of trademark strength has tended to favor the prior user.[69]

{43} However, this factor is not necessarily determinative. In addition to the strength of the mark, courts deciding these cases apply the other likelihood of confusion factors. Depending on the particular facts, these factors may either aid or hinder the junior user.

{44} **Similarity of marks:** Opinions analyzing the likelihood of confusion between call letters have devoted considerable space to evidence on the phonetic and visual similarity of letter combinations. Much of this evidence comes from a particular expert witness who appears to specialize in testifying

for plaintiffs in such trials.[70] Some courts find an analysis of call letter similarity persuasive, while others discount it entirely.[71] Courts discounting similarity studies rely on the fact that call letters are frequently used in the context of slogans, phrases, or logos that would distinguish them, and because stations in a given region frequently share two or more of their call letters, listeners are accustomed to distinguishing stations with such overlapping letters.[72]

{45} **Similarity of product:** In call letter cases, courts have also looked to the similarity of broadcast format when assessing the likelihood of confusion in call letter cases. Stations with similar formats are more likely to be confused with one another, such as the case of two radio stations that each broadcast a "top-forty" music format.[73] Where one station broadcasts a family-oriented country-western music format, and another broadcasts a "bad-boy, iconoclastic" rock n' roll format, listeners are unlikely to confuse the two.[74] Certainly a listener who mistakenly tuned to one of the stations would soon realize her mistake.[75] Medium, too, tends to prevent listeners from confusing stations: one court has held that a television and radio station with almost identical call letters are unlikely to be confused in part because of the clear differences between radio and television.[76]

{46} **Area of use:** Generally, conflicts between stations with similar call letters only occur when the territories reached by their broadcast signals overlap.[77] However, there seems to be no reason that stations with similar call letters but separate geographic territories might come into conflict. Such a case would present great difficulties for a plaintiff attempting to show a likelihood of confusion: the plaintiff would presumably need to show consumer recognition of his call letters outside his broadcast area.

{47} **Sophistication of consumers:** The nature of broadcasting has produced an odd twist in analyzing the factor of consumer sophistication: courts have recognized advertisers, rather than listeners, to be the true consumers of broadcast services.[78] Indeed, it has been suggested that consumers are in some sense the "product" of broadcast, by which the courts appear to mean that delivery of messages to a certain audience is the product.[79] Radio broadcasters in fact target their programming to appeal to particular niche populations.[80] The cases discussing call letter disputes suggest that advertisers are very sophisticated in selecting broadcast services that are oriented toward the particular demographic market that the advertiser wishes to reach.[81] Consequently, this factor tends to favor defendants, since it seems unlikely that advertisers will mistakenly recruit the wrong station to deliver their messages, even if one station's call letters closely resemble those of another station.

{48} **Degree of Care:** Given the analysis of consumer sophistication above, it stands to reason that the degree of care exercised by advertisers, the true consumers of broadcast services, is very high. However, in contrast to the "sophistication of consumers" factor, courts assessing the "degree of care" factor tend to apply it to the audience rather than to the advertisers.[82] In general, the courts have postulated that the degree of discrimination between radio stations with similar broadcast formats is not high because, first, the consumer has no direct financial stake in the choice of stations, and second, listeners often play the radio as "background" while engaged in other activities.[83] One court has extended this analysis from the "purely aural"[84] medium of radio to the audiovisual medium of television.[85] This extension is somewhat questionable. Even though television consumers also have no real financial stake in tuning to a particular channel, television clearly requires a greater investment of attention than does radio.

{49} **Intent in adopting mark:** The existence of "bad faith" or an intent by the junior user to "free ride" off of mistaken association with the prior user's mark is not ostensibly determinative of the outcome of a trademark infringement suit, but courts seem to weigh the question of scienter heavily.

Infringers are usually not foolish enough to admit or leave evidence of an intent to appropriate a prior user's reputation, but in instances where the junior user knew of the prior user and showed an awareness of the possibility of confusion, the court was willing to infer an intent to trade on the prior user's goodwill.[86]

Frequency Identifiers

{50} A second type of dispute over broadcast identifiers involves frequency designations, which carry the location function for broadcast services. It may seem surprising that the latter disputes could arise: each broadcaster is assigned a particular frequency within a geographic area by the Federal Communications Commission; otherwise, stations would interfere with one another by broadcasting over each other's signals.[87] However, because FM tuners were analog until recently, radio stations developed the habit of rounding their designators to the nearest whole number on the FM dial in advertisements or for identification purposes.[88] FM frequency assignments lie between 88.1 and 107.9 Megahertz; the FCC has divided this portion of the spectrum into 100 channels 0.2 Megahertz apart -- since the channels begin at 88.1, no station could be assigned to a whole number frequency.[89] Given that only 21 whole numbers are available on the FM spectrum, and since stations can elect to round up or down, several conflicts developed between stations that rounded to the same number.

{51} In deciding these disputes, the courts tend to treat frequency designators as addresses -- that is, as a term describing the approximate location of the broadcast service on the FM dial.[90] This utilitarian function of facilitating frequency location throws the designator into the category of descriptive terms.[91] As such, the designators have been treated much like geographic terms in other trademarks: they lack inherent distinctiveness, and are protectable only upon a showing of secondary meaning.[92] The rounded frequency designator therefore might be distinctive if a plaintiff could show that it was associated in the minds of consumers with the source of a particular broadcast service, rather than as an aid to locating the broadcast frequency. However, as a practical matter, plaintiffs in reported cases have shown a marked inability to offer such proof, perhaps because of the uncoupling of call letters and frequency numbers: distinctiveness is easily shown for call letters because they act almost exclusively as a name, whereas distinctiveness is difficult to show for frequency numbers, because they act almost exclusively as an address.

Telephone Mnemonics

{52} A third real space analogy to cyberspace domain names might be that of telephone numbers, which act both as names and logical addresses. Several trademark cases have recently been decided involving the use of "vanity" telephone numbers, which correspond to alphanumeric designators that are easy for consumers to remember and associate with the business at that number. For example, "L-A-W-Y-E-R-S" serves as a mnemonic for 529-9377, the number of a law firm.[93] Such telephone mnemonics bear a close resemblance to the mnemonic domain names associated with IP addresses, and legal decisions regarding their status as trademarks suggest that domain names may be protectable.

{53} Courts have almost unanimously held that telephone mnemonics may be protectable as

trademarks, and have readily applied the law regarding the likelihood of confusion to such marks.[94] In *Dranoff-Perlstein Assocs. v. Sklar* ,[95] plaintiffs who used the telephone mnemonic "INJURY-1" to advertise their personal injury legal services sought an injunction against defendants who used the mnemonic "INJURY-9" to advertise their legal services. The trial court denied the motion, holding that the plaintiff's marks was generic or at best descriptive without having been shown to have secondary meaning.[96] The appellate court partially agreed, reasoning that the term "INJURY" was so commonly descriptive of personal injury representation that it must be generic.[97]

{54} However, the appellate court in *Dranoff-Perlstein* noted that marks must be assessed "as a whole," and the marks in question differed in their numerical suffixes.[98] It further noted that where two marks share generic portions but differ in non-generic portions, it is presumed that the public tends to distinguish the marks on the basis of the non-generic portions.[99] Thus, any confusing similarity between the marks "INJURY-1" and "INJURY-9" would depend on the likelihood of confusion between the marks, taking each as a whole, with particular emphasis on the likelihood of confusing the suffix "1" with "9." The case was remanded for findings on the likelihood of such confusion, taking into account the familiar factors of confusion analysis.[100]

{55} In some instances, however, there may be no question that a single digit difference will be confusing. In *Holiday Inns v. 800 Reservations* ,[101] plaintiff sought to enjoin defendant's use of a telephone mnemonic that differed from plaintiff's "1-800-HOLIDAY INN" mnemonic by one critical digit. The defendant was aware that telephone users routinely confuse the letter "O" with the numeral "zero" when dialing mnemonic telephone designators. The defendant therefore secured the "complementary" number, 1-800-H-[zero]-LIDAY, that is 1-800-405-4329, expecting that some number of callers intending to contact Holiday Inn reservations would instead dial his number.[102] Callers who did so would be connected to defendant's hotel travel agency, which offered booking for not only Holiday Inn, but other hotel chains. The defendant's business received a fee for placement of reservations.[103]

{56} The court held that this use of a similar telephone mnemonic was "parasitic." [104] The defendant admittedly attempted to avoid passing his service off as that of Holiday Inns', and arranged to have the "complementary" number answered with a recording stating that the caller had not reached Holiday Inns, but a reservation service that would assist in finding the lowest hotel rate at Holiday Inns or elsewhere. This was not persuasive to the court, which found that the recording was in fact likely to increase customer confusion by offering new options at the moment the customer is most confused, having attempted to contact one service and mistakenly contacted another.[105] The court noted further that, "Defendant's use of plaintiff's [1-800-HOLIDAY INN] mark involves more than the likelihood of confusion -- our present technology allows defendants to use plaintiff's mark in such a way that they can anticipate actual confusion with absolute accuracy and can profit accordingly." [106] The injunction was issued against 800 Reservations.[107]

Generic Mnemonics

{57} As might be supposed from the analysis in *Dranoff-Perlstein* , the problem of generic terms runs throughout the telephone mnemonic cases. The fear that a common term might be monopolized by granting it trademark status is in fact exacerbated by the fixed correspondence between numerals and letters on the telephone keypad.[108] There is some redundancy in this code since there is a three to one correspondence between letters and digits. For example, the letters A, B, and C are all assigned

to the numeral 2. Thus, although there is redundancy in the code, it is with regard to words, not numbers. Within a given area code, there is only one telephone number that corresponds to a given mnemonic word. Control of that telephone number is tantamount to control of the word as a mnemonic device.

{58} The exception to this exclusivity is, of course, the availability of toll-free "800" numbers, which transcend area codes since they are accessible nationwide. Thus, in the telephone cases, the clash between mnemonics is frequently between a local number and an "800" number with the same or similar mnemonic. In *Dial-a-Mattress Franchise Corp. v. Page*, [109] the plaintiff held a local exchange number corresponding to the mnemonic "mattres"; the plaintiff successfully enjoined a competitor's use of the analog "800" number within that area code. The trial court's finding that the competing "800" mnemonic could be confusingly similar was upheld on appeal.[110]

{59} In contrast, the case of *Bell v. Kidan* [111] involved the use of a similar "800" number. This was found unlikely to confuse consumers, in part because it was *not* a toll call.[112] Plaintiff used the mnemonic "CALL-LAW" in advertising their legal services; they sought to enjoin use of defendant's mnemonic "1-800-LAW-CALL" in the same area.[113] In assessing plaintiff's likelihood of success on the merits, the trial court reviewed the factors indicating likelihood of confusion, and noted that the difference between a toll call and an "800" call was likely to be of significance to consumers, who would expect even a slight difference in numbers to yield a different connection.[114] This analysis similarly weighed the consumer sophistication factor against the plaintiff; the court reasoned that consumers are familiar with the difference between local toll calls and "800" calls.[115] The court denied injunctive relief.[116]

Transplanted Marks

{60} The emergence of Internet trademarks offers a clear opportunity to come to grips with the issue of names and addresses inherent in the use of designators as trademarks. The real space examples reviewed here show that cyberspace is not unique in harboring designators that function as both names and addresses, and these designators will frequently be employed as trademarks or servicemarks. In the case of geographic place names, the distinction between naming and addressing appears to have gone entirely unrecognized. In the case of broadcast designators, where the two functions have come almost completely uncoupled, the failure to recognize the distinction between naming and addressing has generated a highly idiosyncratic and somewhat confused body of cases. In neither instance have the courts considering these real world designators articulated broad principles that might be readily transferred to new fact patterns, such as those arising on the Internet.

{61} Neither has the distinction between naming and addressing been expressly articulated in the cases considering telephone mnemonics. However, in these cases, factual and technological similarities to the Internet domain name incidents offer a ready comparison from which some general principles may be drawn. As the telephone mnemonic cases reviewed above indicate, the dual nature of a designator such as a telephone number or domain name is no bar to rational application of established trademark law. Such cases are exceptionally helpful in charting the likely progression of trademark law on the Internet. The telephone cases suggest: first, that domain names, like telephone mnemonics, are potentially protectable as trademarks; and second, that domain names, like telephone mnemonics, should be susceptible to the accepted infringement analysis applied to other types of trademarks.

{62} However, this is not to say that consideration of domain names as trademarks will not entail its own idiosyncracies. The calculus of mark strength in the kind of Internet dispute encountered thus far may not be as straightforward as one might initially assume. To date, the domain names in dispute have drawn much of their recognition and goodwill from their use as trade or service marks in real space. This may in some instances turn the usual classification of marks on its head, as they are in essence being applied to a new service. Considered in the abstract, there is no particular reason to suppose that cyberspace happening upon a domain designated "McDonalds.com" or "Kaplan.com" would associate those sites with a source of hamburgers or testing services in real space -- the world is full of individuals named McDonald and Kaplan, any of whom might have registered such domain names with the InterNIC. This seems to weaken the presumption of distinctiveness for arbitrary marks transported to the new medium. By contrast, a site designated with a fanciful name such as "Exxon.com" seems inherently distinctive whether in real space or cyberspace. And a generic mark from real space may become arbitrary when used to designate a domain name such as "muffin.com."

{63} This carry over from real space to cyberspace suggests that a key factor in analyzing the likelihood of consumer confusion will be the "proximity" of the marks. Use of the name "McDonald's" to peddle hamburgers in real space may not necessarily overlap with the use of the same name for a resource locator in cyberspace; the two uses may be in distinctly different markets. They may also involve very different services, as the major commodity on the Internet is information, rather than hamburgers. This is beginning to change, however, as companies begin to use their net presence to allow customers to order products including fast food delivery of pizzas.^[117] Consequently, the real and virtual markets may eventually converge.

{64} By contrast, the use of marks like "MTV" or "Kaplan" on the Internet may already entail a high likelihood of confusion, as they are associated with entertainment or information in both real space and cyberspace. In such instances, the use of the Internet becomes a natural extension of the service offered in real space. This increases not only the prospect that the marks overlap in proximity but also the occasion for parasitic or bad faith use of the mark. It seems relatively clear, for example, that at least some of the notoriety of the "mtv.com" site was generated by Curry's real space association with the MTV broadcast channel. Similarly, there is no question, indeed the Princeton Review openly admits, that their use of "kaplan" in their domain name was designed to capture potential rivals of their customer. Additionally, such cases appear to use the technology to anticipate actual confusion, as in the *Holiday Inns* case.

Emerging Cybermarks

{65} Although the Internet's present trademark disputes appear imported from real space, this will not always be the case; eventually the disputes will be home-grown. The dispute between Wired and Women's Wire is an early precursor to such conflicts: the heart of the dispute was not the appropriation of a well-known mark from real space, but the confusing similarity between two marks in cyberspace. As Internet commerce becomes more common, we may expect that certain domains will acquire a reputation based entirely on their Internet activities -- as Adam Curry's "metaverse.com" site seems to be doing. Development of a competing site with a similar mnemonic, such as "metaverse.net" or "multiverse.com" would raise the possibility of confusing similarity between two cyberspace-based marks -- "cybermarks" if you will.

{66} Such disputes need not be divorced from the law of real space, however, and precedent such as the telephone mnemonic cases will continue to be helpful, so long as it is realized that, at some points, the correspondence between telephone numbers and IP addresses will break down. For example, although the strength of the cybermark will likely be assessed as much as any trademark, the problem of generic terms may be of lesser concern than in the telephone mnemonic cases. Generics in general go unprotected because they are words necessary to all competitors in a given market. At least part of the rationale underlying the policy toward generic telephone mnemonics is the static correspondence between telephone numbers and their associated letters on the telephone key pad -- only one telephone number in an area will correspond to the term. However, unlike telephone mnemonics, domain name mnemonics are entirely separable from their underlying IP addresses, and completely portable to a new Internet resource site. Thus, there is no necessary monopoly of a mnemonic when an IP address is assigned; any alphanumeric string may be chosen as the corresponding domain name.

{67} The problem of confusion between domain names may also be lessened if, as in *Dranoff-Perlstein*, the domain name must be taken as a whole when assessing the likelihood of confusion. Imagine for example competing computer program vendors who have registered, respectively, "software.net" and "software.com" as their domain sites. Under the analysis of *Dranoff-Perlstein*, the word "software" must surely be generic as it is a common descriptive term, and likely essential to the advertising and business operations of any purveyor of computer programs. This does not necessarily render the competing domain names unprotectable, however; the analysis will simply shift to whether or not there is a likelihood of confusion between the top-level domain designations ".com" and ".net" when used as part of the full domain names.

{68} Such an analysis suggests that the factor of consumer sophistication may also prove important: a result that is problematic, as the computer literacy of cybernauts is currently in flux. Until very recently, the majority of Internet users were relatively experienced in the use of the medium; like consumers who can readily distinguish an "800" telephone number from a toll call, Internet users would likely distinguish a "wired.com" from "wire.net" simply by recognizing the top-level domain designation. However, the recent and burgeoning influx of computer neophytes or "newbies," onto the Internet may have drastically altered the likelihood of domain name discrimination. Ironically, this flood of new net citizens, which appears to have greatly diluted the mean level of user sophistication, is also driving the movement toward commercialization. A large pool of such cyberspace consumers is critical to the viability of any electronic business venture, and in time they will likely become discriminating cybermarket patrons. In the interim, however, their appearance on-line may increase the chances that a court will find a likelihood of confusion between similar domain designations.

Conclusion

{69} As commercial use of the Internet becomes increasingly common, designation of goods and services by on-line trademarks, or "cybermarks" will gain in significance. Businesses that are willing to venture out into cyberspace will wish to advertise and differentiate their services; lack of settled trademark rights may deter them from investing in such ventures. However, the established law of trademarks appears admirably suited to providing such surety. Although cybermarks may in some cases function as both names and addresses, established trademark doctrines are well able to accommodate such designators. As a consequence, doctrines applied to decide disputes in real space over marks such as telephone number mnemonics will be extended to resolve disputes over

trademarks in cyberspace.

{{END}}

↪ See the related readings

Journal staff members have compiled a list of hypertext links of information contained on the Internet that may be of interest to you.

Footnotes

- [1] *See* M. Mitchell Waldrop, *Culture Shock on the Networks* , 265 SCIENCE 879, 880 (1994).
- [2] *See* DANIEL P. DERN, THE INTERNET GUIDE FOR NEW USERS 364-66, 388-91 (1994) (discussing Internet etiquette, or "netiquette").
- [3] *See* Vinton G. Cerf, *Networks* , SCI. AM., Sept. 1991, at 72.
- [4] *See A Close-up of Transmission Control Protocol/Internet Protocol (TCP/IP)* , DATAMATION, Aug. 1, 1988, at 72; DERN, *supra* note 2, at 10-11.
- [5] DERN, *supra* note 2, at 7-8.
- [6] *See id* . at 16.
- [7] *Id* . at 8-11.
- [8] Waldrop, *supra* note 1, at 879.
- [9] DERN, *supra* note 2, at 369-70.
- [10] *See* Waldrop, *supra* note 1, at 881.
- [11] *See* DERN, *supra* note 2, at 15 (discussing the CIX).
- [12] *See id* . at 12-13.
- [13] *See* Waldrop, *supra* note 1, at 880.
- [14] *See* DERN, *supra* note 2, at 69-70.
- [15] *Id* . at 71.
- [16] *Id* . at 69-70.
- [17] *See* DERN, *supra* note 2, at 71-72.
- [18] *Id* . at 75-76.

[19] *Id.* at 73-74.

[20] *Id.* at 74.

[21] *Id.* at 71.

[22] Anthony Lazarus, *Trademark Laws Clash With First-come, First-served Domain Registration*, DIGITAL MEDIA, June 8, 1994, at 37.

[23] *Id.*

[24] See Rosalind Resnik, *Cybertort: The New Era*, THE NAT'L L.J., July 18, 1994, at A1.

[25] *Video Jockey Butts Heads With MTV Over Internet*, THE PLAIN DEALER, May 25, 1994, at 6C.

[26] *Id.*

[27] See Resnik, *supra* note 24, at A1.

[28] See Stewart Ugelow, *Address for Success: Internet Name Game*, WASH. POST, August 11, 1994, at A1.

[29] See Chris Gulker, *Firm Must Alter Name on Internet*, S.F. EXAMINER, Oct. 6, 1994, at E1.

[30] *MTV, Curry Settle*, INFO. L. ALERT, Mar. 24, 1995, available in WESTLAW, INFLA database (1995 WL 2399911).

[31] See Ugelow, *supra* note 28, at A1.

[32] *Id.*

[33] See Gulker, *supra* note 29, at E1.

[34] *Video Jockey Butts Head with MTV over Internet*, *supra* note 25, at 6C.

[35] Joshua Quittner, *You Deserve a Break Today*, NEWSDAY, Oct. 7, 1994, at A05.

[36] See Gulker, *supra* note 29, at E1.

[37] Ugelow, *supra* note 28, at A1.

[38] Quittner, *supra* note 35, at A05.

[39] *Id.*

[40] Harley Jebens, *Exploring All Things High Tech in the World of Entertainment*, AUSTIN AM.-STATESMAN, Oct. 27, 1994, at 26.

- [41] *McDonald's Gives \$3,500 to Get Name Back on Net* , ARIZ. REPUBLIC, Feb. 6, 1995, at E1.
- [42] 1 J. THOMAS MCCARTHY, TRADEMARKS AND UNFAIR COMPETITION § 3.01[2] (3d ed. 1994).
- [43] 1 JEROME GILSON, TRADEMARK PROTECTION AND PRACTICE § 1.02[1][b] (1994).
- [44] See *Two Pesos, Inc. v. Taco Cabana, Inc.*, 112 S.Ct. 2753, 2760 (1992) (discussing purposes of trademark law).
- [45] See 15 U.S.C. §§ 1051-1127 (1988 & Supp. IV 1992).
- [46] See 15 U.S.C. §§ 1114(1), 1125(a) (1988 & Supp. IV 1992).
- [47] See 1 MCCARTHY, *supra* note 42, § 11.4.
- [48] See *id.* § 11.3; see also *Exxon Corp. v. Xoil Energy Resources*, 552 F. Supp. 1008, 1014 (S.D.N.Y. 1981) ("Exxon" mark is arbitrary and accorded greatest possible degree of protection).
- [49] See 1 MCCARTHY, *supra* note 42, § 11.2.
- [50] See 3 LOUIS ALTMAN, CALLMAN ON UNFAIR COMPETITION, TRADEMARKS AND MONOPOLIES § 18.03 (4th ed. 1994).
- [51] 1 MCCARTHY, *supra* note 42, § 11.9.
- [52] 1 *Id.* . § 12.1[1].
- [53] 1 GILSON, *supra* note 43, § 12.01[1].
- [54] See, e.g. , *Ford Motor Co. v. Summit Motor Prods.*, 930 F.2d 277, 293 (3d Cir. 1991) (listing factors); *Polaroid Corp. v. Polarad Elecs. Corp.*, 287 F.2d 492, 495 (2d Cir. 1961) (listing factors).
- [55] See 15 U.S.C. §§ 1116, 1117 (1988 & Supp. V 1993).
- [56] 3 ALTMAN, *supra* note 50, § 19.43 (explaining the proposition and citing contrary authority as exceptions).
- [57] *Cf.* DERN, *supra* note 2, at 67-68.
- [58] See generally 3 ALTMAN, *supra* note 50, § 19.43 (discussing geographic names as trademarks).
- [59] 3 *Id.* .
- [60] See Ugelow, *supra* note 28, at A1 (quoting Lynne Beresford, United States Patent and Trademark Office).
- [61] 47 U.S.C. § 303(o) (1988); see also *Allen B. Dumont Lab. v. Carroll*, 184 F.2d 153, 155 (3d

Cir. 1950) (interpreting the term "radio broadcasting" within the statute to include all forms of television transmission).

[62] *See* Infinity Broadcasting Corp. v. Greater Boston Radio II, No. CIV.A.93-11161-WF, 1993 WL 343679, at *6 (D. Mass., Aug. 18, 1993).

[63] 47 C.F.R. § 73.3550(h)(1994).

[64] *See* Covenant Radio Corp. v. Ten Eighty Corp., 390 A.2d 949, 952 (Conn. Sup. Ct. 1977).

[65] Cox Communications v. Susquehanna Broadcasting Co., 620 F. Supp. 143, 145 (N.D. Ga. 1985).

[66] *See* Infinity Broadcasting, 1993 WL 343679, at *6.

[67] *See* Pathfinder Communications v. Midwest Communications Co., 593 F.Supp. 281, 286 (N.D. Ind. 1984).

[68] *See* Draper Communications v. Delaware Valley Broadcasters, 505 A.2d 1283, 1295 (Del. Ch. 1985).

[69] *But see* Virginia Tech Foundation v. Family Group Limited V, 666 F. Supp. 856, 858 (W.D. Va. 1987) (suggesting that call letters assigned by the FCC are not a "strong mark").

[70] *See, e.g.*, *Draper Communications*, 505 A.2d at 1290-91 (testimony of Daniel A. Dinnsen, Professor of Linguistics, University of Indiana); *Pathfinder Communications*, 593 F. Supp. at 283-84 (testimony of Professor Dinnsen); *Infinity Broadcasting*, 1993 WL 343679, at *6 (testimony of Professor Dinnsen).

[71] *See, e.g.*, *Virginia Tech Foundation*, 666 F. Supp. at 858 ("The experts, in my opinion, did more to obfuscate the problem than they did to clarify it. . . . In my judgment, this is a classic misuse of expert testimony, and I give very little weight to any of it.") (Kiser, J.).

[72] *See Infinity Broadcasting*, 1993 WL 343679, at *5-6.

[73] *See Pathfinder Communications*, 593 F. Supp at 285.

[74] *See Infinity Broadcasting*, 1993 WL 343679, at *3.

[75] *Id.*

[76] *See* Virginia Tech Foundation v. Family Group Limited V, 666 F. Supp. 856, 859 (W.D. Va. 1987).

[77] *See, e.g.*, *Draper Communications v. Delaware Valley Broadcasters*, 505 A.2d 1283, 1294 (Del. Ch. 1985); *Pathfinder Communications*, 593 F. Supp at 285.

[78] *Pathfinder Communications*, 593 F. Supp. at 283.

[79] *Infinity Broadcasting* , 1993 WL 343679, at *10.

[80] *Id* . at *3.

[81] *Id* . at *4.

[82] *See Pathfinder Communications* , 593 F. Supp at 286.

[83] *Id* .

[84] *Id* .

[85] *See Draper Communications v. Delaware Valley Broadcasters*, 505 A.2d 1283, 1294 (Del. Ch. 1985) (citing *Pathfinder Communications* , 593 F. Supp. at 286).

[86] *See Draper Communications* , 505 A.2d at 1295-96; *Pathfinder Communications* , 593 F. Supp. at 286.

[87] 47 C.F.R. §§ 73.201-203 (1994).

[88] *See Walt-West Enters. v. Gannett Co.*, 695 F.2d 1050, 1052 (7th Cir. 1982); *Covenant Radio Corp. v. Ten Eighty Corp.*, 390 A.2d 949, 952 (Conn. Sup. Ct. 1977).

[89] *Walt-West Enters.* , 695 F.2d at 1052 n.1.

[90] *Id* . at 1059; *Cox Communications v. Susquehannah Broadcasting Co.*, 620 F. Supp. 143, 146 (N.D. Ga. 1985); *Covenant Radio* , 390 A.2d at 952.

[91] *See Cox Communications* , 620 F. Supp. at 146 (noting that numerical identifiers indicating frequency location act like geographical identifiers).

[92] *Walt-West Enters.* , 695 F.2d at 1059; *Covenant Radio* , 390 A.2d at 953-54.

[93] *See, e.g.* , *Murrin v. Midco Communications*, 726 F. Supp. 1195 (D. Minn. 1989) (trademark suit to enjoin allegedly infringing use of telephone mnemonic "Dial L-A-W-Y-E-R-S"); *see generally* , Terry Ann Swift, Comment, *Telephone Numbers That Spell Generic Terms: A Protectable Trademark or An Invitation to Monopolize a Market?* , 28 U.S.F. L. REV. 1079 (1994) (discussing trademark protection of telephone mnemonics).

[94] *See* 3 ALTMAN, *supra* note 50, § 18.23. *But see* *Cytanovich Reading Ctr. v. Reading Games*, 208 Cal. Rptr. 412 (1984) (declining to recognize telephone mnemonic as a trademark).

[95] 967 F.2d 852 (3d Cir. 1992); *see also* Jaqueline Pasquarella, Note, *Trademark Law - Confusion Over the Likelihood of Confusion?* *Dranoff-Perlstein Associates v. Sklar (1993)* , 38 VILL. L. REV. 137 (1993).

[96] *Dranoff-Perlstein* , 967 F.2d at 853.

[97] *Id* . at 860.

[98] *Id* .

[99] *Id* . at 861.

[100] *Id* . at 862.

[101] 838 F. Supp. 1247 (E.D. Tenn. 1993).

[102] *Id* . at 1250-51.

[103] *Id* . at 1251, 1253.

[104] *Id* . at 1255.

[105] *Id* . at 1253, 1255.

[106] *Id* . at 1255.

[107] *Id* .

[108] *See* *Dranoff-Perlstein v. Sklar*, 967 F.2d 852, 859 (3d Cir. 1992).

[109] 880 F.2d 675 (2d Cir. 1989).

[110] *Id* . at 678.

[111] 836 F. Supp. 125 (S.D.N.Y. 1993).

[112] *Id* . at 127.

[113] *Id* . at 126.

[114] *Id* . at 127.

[115] *Id* .

[116] *Id* . at 128.

[117] *Pizza Hut Testing Internet Delivery* , UPI, Aug. 22, 1994, available in LEXIS, Nexis Library, Cmpcom.

[Return to this Issue's Index](#)
[Return to *The Journal's* Home Page](#)

Copyright 1999 Richmond Journal of Law & Technology

battle.com

TRADEMARK ISSUES RELATING TO INTERNET DOMAIN NAMES

by

John W. Scruton
of
WHEAT, CAMORIANO, SMITH & BERES, PLC
Suite 1515 Citizens Plaza
500 West Jefferson Street
Louisville, Kentucky 40202
(502) 585-2040

Prepared for Louisville Bar Association
Center for Continuing Legal Education

Annual Seminar on Intellectual Property

May 22, 1998

As a new medium of communication and commerce, the Internet has become a battleground for a variety of trademark issues. The importance of those issues has increased with the rapidly increasing volume of commerce on the Internet. One particularly fertile area of dispute has concerned the use of Internet domain names where two or more parties seek to use the same domain name, and at least one of them claims trademark rights in the name.

WHAT IS A DOMAIN NAME?

Domain names are the now-familiar devices typically ending in ".com," ".org," and a handful of other suffixes. In combination with other elements (typically http://www), they create the uniform resource locator (URL) that serves as an Internet address. The domain name is linked with a numerical Internet address known as the Internet Protocol (IP) address.

The domain name consists of two parts: the "top level domain" (TLD) and the "second level domain" (SLD).¹ There are currently three so-called generic TLD's (gTLD's), which are available to entities in any country throughout the world. They are .com, .org, and .net. Other TLD's include .gov for governmental entities and .edu for educational entities, and identifiers for individual countries such .ca (Canada), .fr (France), and .de (Germany).

There is currently a plan, known as the Generic Top Level Domain Memorandum of Understanding (gTLD-MoU) that calls for creation of seven new gTLD's, each of which would be dedicated to a specific type of website. They are: .firm (businesses), .shop (businesses selling goods), .web (entities whose activities emphasize use of the world wide web), .arts (entities emphasizing cultural/entertainment activities), .rec (entities emphasizing recreational activities), .info (sites offering information services), and .nom (individuals' sites). The gTLD-MoU is currently scheduled to take effect later this year, although its effective date has already been postponed once.

The SLD is the part of the domain name preceding the TLD. It may consist of up to 24 alphanumeric characters. SLD's often consist of words that indicate either the operator of the website or the type of content to be found at that site.

Like a physical address or a telephone number, each Internet address must be unique. A difference of one character in the SLD is enough to make the technical distinction. Further, two entities could have identical SLD's as long as they are in different TLD's. Thus the Yale Equipment company can maintain a website at <yale.com> while Yale University maintains one at <yale.edu> without causing any technical problems.

DOMAIN NAME REGISTRATION

To operate a website at a particular domain name, you must first register that name. The entity that currently registers names in the .com, .org, and .net TLD's is Network Solutions, Inc. (NSI) (corporate slogan: "We're the dot com people™"). NSI registers names on a first-come, first-served basis. Only one entity may be registered for any particular combination of letters in

¹ Copyright 1998, John Scruton

In the world of the Internet, no term is worth having if it cannot be reduced to a confusing abbreviation.

any given TLD. NSI will not register essentially identical domain names to different users, so, for example, if Disney had already registered <disneyworld.com>, NSI probably would not allow another entity to register <disney_world.com>. NSI considers such matters on a case-by-case basis.

Domain name registration is normally (if not exclusively) done on-line. The person seeking to register the domain name goes to the NSI website at <www.netsol.com> and types in the desired domain name. NSI's computer will compare that name with its database of existing names. If the desired name is available, the registrant clicks through various other screens. If the requested name is not available, the would-be registrant is asked to choose another. According to information brought out in published cases, NSI registers a new domain name about every 20 seconds (on average), for a total of about 100,000 new registrations each month. About 90 percent of those registrations are done without any human intervention.

Registration with NSI requires the registrant to verify that "the registration of the selected domain name, to the best of the registrant's knowledge, does not interfere with or infringe upon the rights of any third party. The registrant also represents that the domain name is not being registered for any unlawful purpose."

The registration of a domain name gets you nothing more than the ability to use that domain name. It does not, by itself, provide access to the Internet. To actually create a website using the domain name, the registrant must contract with an Internet service provider.

DOMAIN NAME DISPUTES

Domain name disputes occur when somebody has registered a domain name that another company thinks it has a superior right to use. That typically happens when the owner of a trademark seeks to register a domain name including the mark and learns that that name is taken.

The battleground for trademark purposes is the SLD. Most businesses on the Internet are found in the .com TLD, and it has become the most familiar to consumers. Consequently, a business establishing a new Internet presence typically wants its domain name to be in the .com TLD. To allow customers and potential customers to easily remember its domain name, the business normally wants its SLD to be its mark. A single company may have multiple sites devoted to its different products, each at a domain name designated by the product's mark with the .com suffix. For example, the toy and game maker Hasbro has a general site at <hasbro.com>, and game-specific sites at <monopoly.com>, <risk.com>, <battleship.com>, and others (but not, as we shall see, <clue.com>).

Domain name disputes differ from typical trademark disputes in at least one fundamental way. In a standard trademark case, two entities are using the same name, or similar names, and the issue is whether that concurrent use creates a likelihood of confusion. The court will assess a number of factors to determine whether confusion is likely, and it is entirely possible that the combatants will both be able to use the identical mark because differences in the types of goods, the marketing channels, and other particulars prevent confusion. Nobody buys a Delta faucet because they think it was made by Delta Airlines.

Domain name disputes arise, at least in part, because the concurrent use of identical domain names by two parties is not possible. Once one entity gets <delta.com>, the next one wanting the same domain name must either wrest it from the first, or choose another. It remains to be seen whether the introduction of new TLD's will diminish the perceived importance of the .com suffix.

Parties: Cybersquatters and Other Malefactors

One person may begin using another's trademark as a domain name for various reasons. The registrant and the complainant may be legally using the same trademark for different goods, and the registrant may simply have gotten there first. Or the registrant may have chosen a domain name that it liked with no knowledge that it was being used as a trademark at all.

Many disputes have arisen from baser motives: Perhaps the most egregious cases are those involving so-called "cybersquatters," who register domain names including famous trademarks with the specific intent of reselling them to the trademark owners. To date, cybersquatters have invariably lost in litigation, so it is likely that this tactic will become less popular as time goes by.

Other disputes have arisen where a competitor or other antagonist has registered a domain name consisting of the "enemy's" trademark. For example, the Princeton Review registered the domain name <kaplan.com> to use as a site dedicated to complaints about Stanley Kaplan's review courses. Similarly, an antiabortion activist registered <plannedparenthood.com> and used it with a site promoting antiabortion literature.

Procedures for Addressing Domain Name Disputes

An entity wishing to institute a challenge to an existing domain name has two options.² It may initiate a dispute under the NSI policy or it may file a lawsuit.

NSI's Dispute Resolution Policy

NSI is on the third revision of its dispute resolution policy. The following is an outline of the current NSI policy, which became effective February 25, 1998 (a copy of which is attached). In general, the policy allows, but does not require, NSI to follow the outlined procedures.

Dispute initiation: A challenger initiates a dispute by providing NSI with (1) an original, *certified copy of a certificate of registration* on any country's principal register (or equivalent) of a *word mark* which is identical to a second-level domain name; and (2) a *copy of written notice sent to the domain name registrant* stating the claim of violation of trademark rights and the legal and factual bases for that claim.

Dispute procedures: NSI will review the materials submitted by the complainant. If the domain name was registered *before* the complainant's trademark registration, NSI will take no further action. If the domain name was registered *after* the complainant's trademark registration, NSI will ask the domain name registrant to submit proof that it had a trademark registration before the date of the complainant's notice of dispute. If so, NSI will take no further action. If no such proof is provided within thirty days, and the domain name registrant cooperates by asking for a new domain name, NSI will help register a new name and give up to ninety days of simultaneous use of the old and new names for a transition period. After 90 days the old name will be put on hold and unavailable until resolution of the dispute. If the domain name registrant fails to cooperate within 30 days of notification of a dispute, NSI will put the domain name on hold pending resolution of the dispute. When the name is in hold status, neither the domain name registrant nor the complainant can use it. NSI will not place the name on hold, or will

² Of course, before a dispute is initiated, the potential challenger has the options of asking nicely to have the domain name assigned, offering to pay money for the domain name, threatening, wheedling, cajoling, etc.

reinstate the name, upon satisfactory evidence of resolution of the dispute.

Litigation: If either party initiates a lawsuit against the other relating to the domain name, NSI will maintain the status quo pending the court's decision: if the name is on hold, it will stay on hold; if not, it will not be put on hold. NSI will deposit "control of the domain name" into the court's registry by giving the plaintiff the registry certificate for deposit.

NSI reserves the right, "in its sole discretion to revoke, suspend, transfer or otherwise modify a domain name registration" upon thirty days' written notice or upon court order or arbitration award requiring such action.

NSI's dispute resolution procedure does not correspond to U.S. trademark law. The NSI policy specifically provides that NSI does not resolve domain name disputes. NSI's policy is heavily based on *priority* and *registration*, and -- perhaps understandably -- pays little heed to the likelihood of confusion analysis that is standard in trademark disputes. NSI's policy has the virtue of simplicity: if you had a registration of a mark that is identical to your domain name before you got notice of a dispute about your domain name, you win under NSI's system.

Options Other Than NSI Dispute

A trademark owner who finds that its mark is being used as somebody else's domain name is likely to have two objectives: to stop the other person's use and to obtain control of the domain name. The NSI policy only addresses the first of those objectives: NSI will put an "improper" domain name on hold. However, a successful complaint under the NSI policy will not result in the domain name being transferred to the trademark owner. Transfer of the domain name will require either negotiation with the domain name registrant or filing a lawsuit.

Negotiation

Like any other, a dispute concerning a domain name can be settled, and many have been. Indeed, the business of the cybersquatter is based on transfer of domain names for a ransom payment in lieu of litigation. A trademark owner considering negotiating a settlement should consider whether to institute an NSI dispute or lawsuit before beginning negotiations. A lawsuit will cause NSI to maintain the status quo, which the trademark owner may not want. If the trademark owner wants to shut down the website, it should avoid making threats of litigation that would provide the domain name registrant a basis for filing a declaratory relief action. It is not clear whether an NSI dispute is by itself enough to satisfy the "actual dispute" requirement of the declaratory relief statute.

Litigation

Many lawsuits have been filed as a result of domain name disputes. As is typical, they have resulted in many settlements and a few reported decisions. I have found no appellate decisions to date, so it is hard to say how good the law is, but the basic thrust of the trial court decisions seems to be correct. Because they are normally based in trademark law, domain name lawsuits are normally filed in, or removed to, federal court. Most lawsuits have involved the adverse domain name claimant, and many have also involved NSI.

The fact that a domain name registrant has prevailed in a challenge under NSI's dispute policy does not mean that it will be able to continue using the domain name indefinitely. As the court held in Cardservice Int'l, Inc. v. McGee, 950 F.Supp. 737, 42 USPQ2d 1850 (E.D. Va. 1997),

[NSI's policy] cannot trump federal law. Holders of valid trademarks under

federal law are not subject to company policy, nor can the rights of those trademark holders be changed without congressional actions. If trademark laws apply to domain names, anyone who obtains a domain name under [NSI's] policy must do so subject to whatever liability is provided for by federal law.

The following is an analysis of many of the reported cases dealing with domain name disputes.

Lawsuit Against NSI

Lawsuits against NSI have rarely been successful. Based on the caselaw to date, the trademark owner who finds that its trademark is someone else's domain name has little to gain by suing NSI. NSI's policy provides that NSI will abide by court decisions, so there is no apparent need to involve NSI. The reported actions against NSI have been brought under the following theories:

Direct Trademark Infringement

Infringement claims against NSI have not fared well because of the plaintiffs' inability to show that NSI was using the disputed mark "in commerce" as required for liability under the Lanham Act. In Academy of Motion Picture Arts and Sciences v. Network Solutions, Inc., 45 USPQ2d 1463 (C.D. Cal. 1997), the Academy contended that NSI unlawfully registered to others the domain names <academyaward.com>, <academyawards.net>, <theoscars.net>, and <oscar.net> and moved for a preliminary injunction to preclude NSI from registering domain names that are similar to the Academy's registered marks OSCAR and ACADEMY AWARDS. The court held that NSI's registration of the domain names was not a use of the marks "in commerce," precluding a likelihood of success on the merits on the infringement claims. Similarly, in Lockheed Martin Corp. v. Network Solutions, Inc., 44 USPQ2d 1865 (C.D. Cal. 1997) the court held that NSI's "use" of the disputed mark was limited to a pure machine-linking "address" function, which is not a trademark use and hence cannot be a trademark infringement.

Dilution

The court in Lockheed Martin rejected Lockheed's dilution claim, holding that NSI's acceptance of domain name registrations is not a "commercial use." Although NSI makes money by registering domain names, unlike a cybersquatter who trades on the value of the domain name *as a trademark* by trying to sell it to the trademark owner, NSI's money comes from the technical function of registering the domain names. NSI makes no more from a domain name that is also a trademark than from one that is a random string of letters.

Contributory Infringement/Dilution

NSI's passive role in the registration process has typically doomed any attempts to hold NSI liable under theories of contributory infringement or contributory dilution. The court in Academy of Motion Picture Arts and Sciences held that NSI lacked the "knowledge of infringement" necessary to support a claim of contributory infringement. In Lockheed Martin, the court held that NSI's activity was too remote to support contributory infringement liability because of NSI's passive role in the registration and lack of involvement with the actual use of the domain name.

The court in Academy of Motion Picture Arts and Sciences held that the absence of any authority supporting a contributory dilution claim precluded a likelihood of success on that claim. The court in Lockheed Martin Corp. v. Network Solutions, Inc., 44 USPQ2d 1521 (C.D. Cal. 1997)³ allowed the possibility of a contributory dilution claim, but rejected Lockheed's

³ There are three published decisions in the Lockheed-Martin v. NSI action.

claim. It held that, like contributory infringement, contributory dilution requires that the defendant have "either induced another's conduct or continued to supply a product after the defendant knew or should have known that it was being used to dilute the plaintiff's trademark." The court found it unlikely that Lockheed could meet the "narrow standard" required to prove such a claim.

Other Theories

The only litigant that has achieved a modicum of success against NSI is Clue Computing, a small Colorado company that is battling Hasbro for the right to use the <clue.com> domain name. Hasbro filed a challenge under the NSI dispute policy. Within its thirty-day period to respond, NSI filed a breach of contract action against NSI in Colorado state court. The court granted an injunction precluding NSI from changing the status of the <clue.com> domain name, thereby precluding NSI from putting it on hold.

In an attempt to extricate itself from the dispute, NSI filed a federal interpleader action. The court dismissed that action on the ground that the state court injunction prevented NSI from depositing control of the *res* as required by the interpleader statute. Network Solutions, Inc. v. Clue Computing, Inc., 946 F.Supp. 858, 41 USPQ2d 1062 (D. Colo. 1996). Meanwhile, Hasbro has filed an infringement action against Clue Computing in Massachusetts district court. *See Hasbro, Inc. v. Clue Computing, Inc.*, 45 USPQ2d 1170 (D. Mass. 1997). At least under the current NSI policy, Clue Computing might have been able to achieve the same result -- maintenance of its domain name until resolution of its dispute with Hasbro -- and litigate the trademark action in its "home court" by filing a declaratory relief action against Hasbro in federal court in Colorado.

The court in Panavision International v. Toeppen, 41 USPQ2d 1310 (C.D. Cal. 1996) granted summary judgment on Panavision's claim against NSI for negligent interference with prospective economic advantage. Although the claim survived a motion to dismiss, Panavision failed to create a factual issue because it establish that NSI owed it a duty of care under California negligence law.

Lawsuit Against Domain Name Registrant

Many trademark owners have successfully sued domain name registrants to obtain the right to use the domain name. Although the best theory will differ from case to case, courts have accepted both trademark infringement and trademark dilution arguments.

Trademark Infringement

In analyzing a claim that use of a domain name is a trademark infringement or unfair competition, the courts have used the standard test to determine whether use of the domain name creates a "likelihood of confusion" with a prior mark. *See, e.g., Cardservice Int'l, Inc. v. McGee*, 950 F.Supp. 737, 42 USPQ2d 1850 (E.D. Va. 1997). Under this test, the court must analyze a number of factors. Although the factors vary somewhat between the federal circuits, the following list used in the Sixth Circuit is typical: 1) the strength of the plaintiff's mark; 2) the relatedness of the goods; 3) the similarity of the marks; 4) any evidence of actual confusion; 5) the marketing channels used; 6) the likely degree of purchaser care; 7) the defendant's intent in selecting the mark; and 8) the likelihood of expansion of the product lines. Frisch's Restaurants v. Elby's Big Boy, 670 F.2d 642, 648, 214 USPQ 15, 20 (6th Cir. 1982).

Because of the unique nature of the Internet, the analysis of the factors tends to differ somewhat from the standard analysis. For example, the "similarity of the marks" factor looms especially large in the analysis. *See, e.g., Cardservice* (finding a likelihood of confusion based

primarily on the similarity of <cardservice.com> domain name to the registered CARDSERVICE INTERNATIONAL mark); Planned Parenthood Federation of America, Inc. v. Bucci, 42 USPQ2d 1430 (S.D.N.Y. 1997) (finding that an antiabortion activist's use of <plannedparenthood.com> created a likelihood of confusion, based on various factors including actual confusion). But use of a registered mark as a domain name does not guarantee that an infringement claim will be successful. In Intermatic, Inc. v. Toeppen, 947 F.Supp. 1227, 40 USPQ2d 1412 (N.D. Ill. 1996), the court refused to grant summary judgment on the claim that defendant's use of the <intermatic.com> domain name infringed plaintiff's registered INTERMATIC mark because of the dissimilarity of the products and the lack of evidence on various other factors. Although the defendant's intent is often an important factor, the court in Intermatic found that defendant's bad faith was not established because there was no law indicating that cybersquatting, by itself, was illegal.

The courts seem to be struggling somewhat with precisely how to analyze some of the factors in the context of domain names and websites. In some cases, the analysis of some factors seems to be skewed in an attempt to find liability where a domain name registrant is intentionally misusing the plaintiff's mark. In Planned Parenthood, for example, the court found that the "competitive proximity of the services" was close, because the parties compete for the same audience, i.e. "Internet users searching for a web site that uses plaintiff's mark as its address."

To prevail on an infringement claim, the plaintiff must show that the defendant "used" the disputed mark "in commerce." In Planned Parenthood, the court held that the use of the <plannedparenthood.com> domain name as a site promoting antiabortion literature and viewpoints was a "commercial use" for Lanham Act purposes. In Juno Online Services L.P. v. Juno Lighting, Inc., 44 USPQ2d 1913 (N.D. Ill. 1997), the court held that the mere "warehousing" of a domain name -- registering the name without actually using it in connection with a website -- is not a "use" of the mark. There, the defendant had reserved the <juno-online.com> name, apparently with the intent of ensuring its availability to swap for the <juno.com> name that it desired. Had the defendant been a cybersquatter, the holding of a domain name for ransom might well have been found to be a sufficient "use in commerce." See Panavision International v. Toeppen, 945 F.Supp. 1296, 40 USPQ2d 1908 (C.D. Cal. 1996) (holding that registration, without more, is not commercial use, but holding marks for sale is), cf. Intermatic (holding that the mere registration of a domain name incorporating a famous mark, without actual use on the Internet, causes dilution in that it precludes the mark's owner from using its mark as a domain name).

Trademark Dilution

To date, plaintiffs in reported cases have had the greatest success with dilution claims. Such a claim requires the plaintiff to prove that it has a "famous mark" and that the defendant is making "commercial use in commerce" of a mark that "causes dilution of the distinctive quality of the [plaintiff's] mark." Lanham Act §43(c). The general purpose of dilution law is to protect the trademark owner's rights in a famous mark by preventing others from using similar marks even when such uses would not be likely to cause confusion, and even in the absence of competition between the parties. A "Xerox Donut Shop" would violate section 43(c).

Dilution is the theory that most closely fits domain name disputes. In Panavision, the court held that a cybersquatter, by preventing Panavision from using its mark as a domain name, not only diluted the mark but *eliminated* the marks' capacity to identify and distinguish Panavision's goods on the Internet, in violation of federal and state anti-dilution law. See also Hasbro, Inc. v. Internet Entertainment Group, Ltd., 40 USPQ2d 1479 (W.D. Wash. 1996)

(plaintiff showed likelihood of success on claim that defendant's use of <candyland.com> for explicit sex site diluted the registered CANDYLAND mark for children's game), Intermatic (cybersquatter's use of <intermatic.com> diluted INTERMATIC mark).

The defendant in TeleTech Customer Care Mgmt. v. Tele-Tech Co., 1997 WL 405898, 42 USPQ2d 1913 (C.D. Cal. 1997) began using the TELE-TECH mark before the plaintiff began using the TELETECH mark, but the plaintiff had obtained a federal registration of its mark before the defendant registered the <teletech.com> domain name. The court granted a preliminary injunction on TeleTech's dilution claim, finding that plaintiff had shown at least "serious questions which go to the merits" plus a balance of hardships favoring plaintiff because defendant could use <tele-tech.com> as its domain name but absent an injunction, plaintiff could not use its mark in its domain name. Had the case gone to a trial on the merits, TeleTech might have had serious problems showing dilution given the defendant's prior use of an almost identical mark.

The courts have had no trouble finding that use by a cybersquatter -- obtaining a domain name registration with the intent of selling it to the owner of the mark -- is a "commercial use in commerce." See, e.g., Intermatic, Panavision. The Intermatic court found that the use of a mark on the Internet automatically constitutes use "in commerce."

Other Theories

Plaintiffs have tried theories other than infringement and dilution, so far without success in the reported cases.

Trademark Misuse: In Juno Online, to avoid being placed on hold status, the registrant of a challenged domain name brought a declaratory relief action based in part on a theory of trademark misuse. The court rejected this as an affirmative claim, holding that it is recognized as a defense only.

Intentional Interference with Prospective Business Advantage: The court in Panavision granted summary judgment on plaintiff's intentional interference claim. The owner of the mark will not normally be able to identify with specificity the prospective relationship that was not consummated because of the domain name registrant's actions, precluding liability on this or similar theories.

Contract: The Panavision court also granted summary judgment on the plaintiff's claim that it was a third-party beneficiary of the contract between the domain name registrant and NSI. Although the registrant represents in that agreement that it is not knowingly violating any third-party rights, the court held that those terms were for NSI's protection, not for the benefit of third-party trademark owners.

Problems

The difficulty with existing theories is that there are many potential cases that they do not reach. Currently, the owner of a non-famous mark may be unable to avoid the need to pay off a cybersquatter, because a successful dilution claim requires the mark to be famous, and courts may be unwilling to find a likelihood of confusion arising solely from registration (or even use) of a domain name. Either the courts or the legislatures may have to invent a new claim to deal with this gap in existing law.

Relief Available Through Litigation

Injunctive Relief

Courts commonly grant injunctive relief in domain name cases. Typically, a prevailing plaintiff will obtain an injunction precluding the defendant from making further use of the

disputed domain name or a confusingly similar name (sometimes after a brief transition period) and requiring the defendant to transfer the domain name to the plaintiff. Preliminary injunctions are common.

The Cardservice case probably represents the outer boundary of plaintiff success in an injunction action. Because the defendant appeared *in pro per*, the case also stands as a monument to the importance of obtaining competent trademark counsel in these disputes. Despite potential for legitimate descriptive uses in connection with defendant's merchant credit card service business, the court there entered an injunction essentially precluding the defendant from using the words "card" and "service" together in any way on the Internet.

Monetary Relief

Damages, Profits, Costs: Although I have found no reported domain name case granting a damage award, there is a good possibility that such an award will eventually be granted. The Lanham Act authorizes courts to award profits, damages, and costs. *See* Lanham Act, §35. A domain name registrant who has obtained the name in an attempt to trade off the value of the mark contained in the name, or to dilute the value of that mark, would be a likely candidate for a monetary award.

Attorneys' Fees: The Lanham Act authorizes courts to award attorneys' fees to the prevailing party in "exceptional" cases. The court in Cardservice granted attorneys' fees where the defendant was aware of Cardservice International before registering the disputed domain name. The defendant made that award more likely by posting statements at <cardservice.com> vilifying Cardservice International and threatening to use the website to divert potential business away from Cardservice International. The court understandably saw this as an attempt to use Cardservice International's mark to harm the company's reputation. Other plaintiffs have been unsuccessful in their attempts to recover fees, largely because of the novelty of the issue. *See Panavision*. As the law becomes better established, attorneys' fee awards are increasingly likely.

REGISTRATION OF DOMAIN NAMES AS TRADEMARKS

Many companies have taken to registering their domain names as trademarks or service marks. Like any other word, phrase, or symbol, a domain name can function as a mark. The mere fact that a company is using a particular domain name, however, does not make it registrable as a mark.

The U.S. Patent and Trademark Office will require an applicant for trademark registration to submit specimens of use of the claimed mark. Those specimens must show that the domain name is being used *as a mark* -- that is, as an identifier of the source of goods or services -- in commerce.

The PTO has stated that "use of an Internet domain name as a mere directional reference, similar to use of a telephone number or business address on stationery, business cards, or advertisements, is not use of the name as a source identifier." The PTO will examine the specimen to see whether the domain name is presented in a distinctive manner and removed from other informational material in determining whether the domain name is being used as a mark.

The advantage of a trademark registration for a domain name is debatable and will depend upon the circumstances. If the applicant already owns a domain name using its mark, and the mark itself is registered, it will be a rare case where the registration of the domain name itself adds anything.



Agreement

[Use your browser's back button (if available) or close this window to return to the previous screen.]

A. AGREEMENT. In this Service Agreement ("Agreement") "you" and "your" refer to each customer and "we", "us" and "our" refer to Network Solutions, Inc. ("NSI"). This Agreement explains our obligations to you, and explains your obligations to us for various Network Solutions services. By selecting our Network Solutions service(s) you have agreed to establish an account with us for such services. When you use your account or permit someone else to use it to purchase or otherwise acquire access to additional Network Solutions service(s) or to cancel your Network Solutions service(s) (even if we were not notified of such authorization), this Agreement covers such service or actions. By using the service(s) provided by NSI under this Agreement, you acknowledge that you have read and agree to be bound by all terms and conditions of this Agreement and any pertinent rules or policies that are or may be published by NSI. The terms and conditions marked with an (*) apply to customers of the Network Solutions E-mail Service only. The terms and conditions marked with an (**) apply only to the Network Solutions dot com biz card™ service. The terms and conditions marked with an (***) apply only to the Network Solutions dot com forwarding™ service.

B. FEES, PAYMENT AND TERM. As consideration for the services you have selected, you agree to pay Network Solutions the applicable service(s) fees. All fees payable hereunder are non-refundable. As further consideration for the Network Solutions service(s), you agree to: (1) provide certain current, complete and accurate information about you as required by the registration process and (2) maintain and update this information as needed to keep it current, complete and accurate. All such information shall be referred to as account information ("Account Information"). You hereby grant NSI the right to disclose to third parties such Account Information.

***C. DESCRIPTION OF E-MAIL SERVICE.** NSI is providing you with a capability to send and receive electronic mail ("Network Solutions E-mail Service") via the World Wide Web ("Web") and on NSI's system. You must: (1) provide all equipment, including a computer and modem, necessary to establish a connection to the Web; and (2) provide for your own connection to the Web and pay any telephone service fees associated with such connection. NSI has set no fixed upper limit on the number of messages you may send or receive through the Network Solutions E-mail Service; however, NSI retains the right, at NSI's sole discretion, to determine whether or not your conduct is consistent with this Agreement and NSI's operating rules or policies and may terminate the Network Solutions E-mail Service if your conduct is found to be inconsistent with this Agreement, such rules or policies. Your right to use the Network Solutions E-mail Service is personal to you. You agree not to resell the E-mail Service, without the prior express written consent of NSI.

***D. PRIVACY POLICY.** E-mail is private correspondence between the sender and the recipient. It is NSI's policy to respect the privacy of its customers. Therefore, NSI will not monitor, edit or disclose the contents of your private communications unless required to do so by law or in the good faith belief that such action is necessary to; (1) conform to the law or comply with legal process served on NSI; (2) protect and defend the rights or property of NSI; or (3) act under exigent circumstances to protect the personal safety of its customers or the public.

You acknowledge and agree that NSI neither endorses the contents of any of your communications nor assumes responsibility for any threatening, libelous, obscene, harassing or offensive material contained therein, any infringement of third party intellectual property rights arising therefrom or any crime facilitated thereby. You acknowledge and agree that certain technical processing of e-mail messages and their content may be required to: (1) send and receive messages; (2) conform to connecting networks' technical requirements; (3) conform to the limitations of the Network Solutions E-mail Service; or (4) conform to other similar requirements.

***E. CUSTOMER CONDUCT.** You are solely responsible for the content of your transmissions through the Network Solutions E-mail Service. Your use of the Network Solutions E-mail Service is subject to all applicable local, state, national and international laws and regulations. You agree: (1) to comply with U.S. law regarding the transmission of technical data exported from the United States through the Network Solutions E-mail Service; (2) not to use the Network Solutions E-mail Service for illegal purposes; (3) not to interfere with or disrupt networks connected to the Network Solutions E-mail Service; and (4) to comply with all regulations, policies and procedures of networks connected to the Network Solutions E-mail Service.

The Network Solutions E-mail Service makes use of the Internet to send and receive certain messages. Your conduct is therefore subject to applicable Internet regulations, policies and procedures.

You agree not to use the Network Solutions E-mail Service for chain letters, junk mail, spamming or any use of distribution lists to any person who has not given specific permission to be included in such a process. You agree not to transmit through the Network Solutions E-mail Service any unlawful, harassing, libelous, abusive, threatening, harmful, vulgar, obscene or otherwise objectionable material of any kind or nature. You further agree not to transmit any material that encourages conduct that could constitute a criminal offense, give rise to civil liability or otherwise violate any applicable local, state, national or international law or regulation. Attempts to gain unauthorized access to other computer systems are prohibited. You agree not to interfere with another customer's use and enjoyment of the Network Solutions E-mail Service or another entity's use and enjoyment of similar services. NSI's contractor, Critical Path, Inc. shall be an intended third party beneficiary of the Network Solutions E-mail Service customers' obligations under this Agreement and thus shall be entitled to enforce those obligations against such customers as if a party to this Agreement. NSI

may, at its sole discretion, immediately terminate Network Solutions E-mail Service if your conduct fails to conform with these terms and conditions. You agree that NSI shall under no circumstances be held liable on account of any action it takes, in good faith, to restrict access to or availability of material that it or any user of the Network Solutions E-mail Service considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected.

***F. PROPRIETARY RIGHTS TO CONTENT.** You acknowledge that content, including but not limited to text, software, music, sound, photographs, video, graphics or other material contained in either advertisements or e-mail-distributed, or other commercially produced information presented to you by the Network Solutions E-mail Service ("Content") by NSI or NSI's advertisers, is protected by copyrights, trademarks, service marks, patents or other proprietary rights and laws. You therefore agree to use this content as expressly authorized by the Network Solutions E-mail Service or the advertiser. You agree not to copy, reproduce, distribute or create derivative works from this content without express authorization to do so by NSI or the advertiser.

G. MODIFICATIONS TO AGREEMENT. You agree, during the period of this Agreement, that we may: (1) revise the terms and conditions of this Agreement; and (2) change the services provided under this Agreement at any time. Any such revision or change will be binding and effective immediately on posting of the revised Agreement or change to the service(s) on NSI's homepages, or on notification to you by e-mail or United States mail. You agree to review NSI's homepages, including the Agreement, periodically to be aware of any such revisions. If you do not agree with any revision to the Agreement, you may terminate this Agreement at any time by providing us with notice by e-mail or United States mail at the addresses listed on the cover page of this Agreement. Notice of your termination will be effective on receipt and processing by us. You agree that, by continuing to use the Network Solutions services following notice of any revision to this Agreement or change in service(s), you agree to abide by any such revisions or changes.

H. MODIFICATIONS TO YOUR ACCOUNT. In order to change any of your account information with us, you must use your Account Number and Password that you selected when you opened your account with us. Please safeguard your Account Number and Password from any unauthorized use. In no event will we be liable for the unauthorized use or misuse of your Account Number or Password.

I. DOMAIN NAME DISPUTE POLICY. If you reserved or registered a domain name through us you agree to be bound by our current Domain Name Dispute Policy ("Dispute Policy") which is incorporated herein and made a part of this Agreement by reference. The current version of the Dispute Policy may be found at our web site: <http://www.networksolutions.com/legal/dispute-policy.html>. Please take the time to familiarize yourself with such policy.

J. DOMAIN NAME DISPUTE POLICY MODIFICATIONS. You agree that we, in our sole discretion, may modify our Dispute Policy at any time. You agree

that, by maintaining the reservation or registration of your domain name after modifications to the Dispute Policy become effective, you have agreed to these modifications. You acknowledge that if you do not agree to any such modifications, you may request that your domain name be deleted from the domain name database.

K. DOMAIN NAME DISPUTES. You agree that, if the registration or reservation of your domain name is challenged by a third party, you will be subject to the provisions specified in the Dispute Policy in effect at the time of the dispute. You agree that in the event a domain name dispute arises with any third party, you will indemnify and hold us harmless pursuant to the terms and conditions contained in the Dispute Policy.

L. AGENTS. You agree that, if an agent for you (i.e., an Internet Service Provider, employee, etc.) purchased our Network Solutions service(s) on your behalf, you are nonetheless bound as a principal by all terms and conditions herein, including the Dispute Policy.

M. ANNOUNCEMENTS. We reserve the right to distribute information to you that is pertinent to the quality or operation of our services and those of our service partners. These announcements will be predominately informative in nature and may include notices describing changes, upgrades, new products or other information to add security or to enhance your identity on the Internet.

N. LIMITATION OF LIABILITY. You agree that our entire liability, and your exclusive remedy, with respect to any Network Solutions services(s) provided under this Agreement and any breach of this Agreement is solely limited to the amount you paid for such service(s). NSI and its contractors shall not be liable for any direct, indirect, incidental, special or consequential damages resulting from the use or inability to use any of the Network Solutions services or for the cost of procurement of substitute services. Because some states do not allow the exclusion or limitation of liability for consequential or incidental damages, in such states, our liability is limited to the extent permitted by law. We disclaim any and all loss or liability resulting from, but not limited to: (1) loss or liability resulting from access delays or access interruptions; (2) loss or liability resulting from data non-delivery or data mis-delivery; (3) loss or liability resulting from acts of God; (4) loss or liability resulting from the unauthorized use or misuse of your Account Number or Password; (5) loss or liability resulting from errors, omissions, or misstatements in any and all information or services(s) provided under this Agreement; (6) loss or liability relating to the deletion of or failure to store e-mail messages; and (7) loss or liability resulting from the development or interruption of your Web site.

O. INDEMNITY. You agree to release, indemnify, and hold NSI, its contractors, agents, employees, officers, directors and affiliates harmless from all liabilities, claims and expenses, including attorney's fees, of third parties relating to or arising under this Agreement, the Network Solutions services provided hereunder or your use of the Network Solutions services, including without limitation infringement by you, or someone else using the Network Solutions E-mail Service with your computer, of any intellectual property or other proprietary

right of any person or entity, or from the violation of any NSI operating rule or policy relating to the service(s) provided. You also agree to release, indemnify and hold us harmless pursuant to the terms and conditions contained in the Dispute Policy. When NSI is threatened with suit by a third party, NSI may seek written assurances from you concerning your promise to indemnify NSI; your failure to provide those assurances may be considered by NSI to be a breach of your Agreement.

P. BREACH. You agree that failure to abide by any provision of this Agreement, any NSI operating rule or policy or the Dispute Policy, may be considered by us to be a material breach and that we may provide a written notice, describing the breach, to you. If within thirty (30) calendar days of the date of such notice, you fail to provide evidence, which is reasonably satisfactory to us, that you have not breached your obligations under the Agreement, then we may delete the registration or reservation of your domain name or terminate your e-mail account without further notice. Any such breach by you shall not be deemed to be excused simply because we did not act earlier in response to that, or any other breach by you.

Q. NO GUARANTY. You agree that, by registration or reservation of your chosen domain name, such registration or reservation does not confer immunity from objection to either the registration, reservation, or use of the domain name.

R. DISCLAIMER OF WARRANTIES. You agree and warrant that the information that you provide to us to register or reserve your domain name or register for other Network Solutions service(s) is, to the best of your knowledge and belief, accurate and complete, and that any future changes to this information will be provided to us in a timely manner according to the modification procedures in place at that time. You agree that your use of our Network Solutions service(s) is solely at your own risk. You agree that such service(s) is provided on an "as is," "as available" basis. NSI EXPRESSLY DISCLAIMS ALL WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. NSI MAKES NO WARRANTY THAT THE NETWORK SOLUTIONS SERVICE(S) WILL MEET YOUR REQUIREMENTS, OR THAT THE SERVICE(S) WILL BE UNINTERRUPTED, TIMELY, SECURE, OR ERROR FREE; NOR DOES NSI MAKE ANY WARRANTY AS TO THE RESULTS THAT MAY BE OBTAINED FROM THE USE OF THE SERVICE(S) OR AS TO THE ACCURACY OR RELIABILITY OF ANY INFORMATION OBTAINED THROUGH THE NETWORK SOLUTIONS E-MAIL SERVICE OR THAT DEFECTS IN THE NETWORK SOLUTIONS SERVICE(S) SOFTWARE WILL BE CORRECTED. YOU UNDERSTAND AND AGREE THAT ANY MATERIAL AND/OR DATA DOWNLOADED OR OTHERWISE OBTAINED THROUGH THE USE OF THE NETWORK SOLUTIONS E-MAIL SERVICE IS DONE AT YOUR OWN DISCRETION AND RISK AND THAT YOU WILL BE SOLELY RESPONSIBLE FOR ANY DAMAGE TO YOUR COMPUTER SYSTEM OR LOSS OF DATA THAT RESULTS FROM THE DOWNLOAD OF SUCH MATERIAL AND/OR DATA. NSI MAKES NO

WARRANTY REGARDING ANY GOODS OR SERVICES PURCHASED OR OBTAINED THROUGH THE E-MAIL SERVICE OR ANY TRANSACTIONS ENTERED INTO THROUGH THE E-MAIL SERVICE. NO ADVICE OR INFORMATION, WHETHER ORAL OR WRITTEN, OBTAINED BY YOU FROM NSI OR THROUGH THE E-MAIL SERVICE SHALL CREATE ANY WARRANTY NOT EXPRESSLY MADE HEREIN. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF CERTAIN WARRANTIES, SO SOME OF THE ABOVE EXCLUSIONS MAY NOT APPLY TO YOU.

S. REVOCATION. You agree that we may delete your domain name or terminate your right to use other Network Solutions service(s) if the information that you provided to register or reserve your domain name or register for other Network Solutions service(s), or subsequently to modify it, contains false or misleading information, or conceals or omits any information we would likely consider material to our decision to register or reserve your domain name.

T. RIGHT OF REFUSAL. We, in our sole discretion, reserve the right to refuse to register or reserve your chosen domain name or register you for other Network Solution service(s), or to delete your domain name within thirty (30) calendar days from receipt of your payment for such services. In the event we do not register or reserve your domain name or register you for other Network Solution service(s), or we delete your domain name or other Network Solution service(s) within such thirty (30) calendar day period, we agree to refund your applicable fee(s). You agree that we shall not be liable to you for loss or damages that may result from our refusal to register or reserve, or delete your domain name or register you for other Network Solution service(s).

U. SEVERABILITY. You agree that the terms of this Agreement are severable. If any term or provision is declared invalid or unenforceable, that term or provision will be construed consistent with applicable law as nearly as possible to reflect the original intentions of the parties, and the remaining terms and provisions will remain in full force and effect.

V. ENTIRETY. You agree that this Agreement, the rules and policies published by NSI and the Dispute Policy are the complete and exclusive agreement between you and us regarding our Network Solutions services. This Agreement and the Dispute Policy supersede all prior agreements and understandings, whether established by custom, practice, policy or precedent.

W. GOVERNING LAW. You agree that this Agreement shall be governed in all respects by and construed in accordance with the laws of the Commonwealth of Virginia, United States of America, excluding its conflict of laws rules. You and we each submit to exclusive subject matter jurisdiction, personal jurisdiction and venue of the United States District Court for the Eastern District of Virginia, Alexandria Division. If there is no jurisdiction in the United States District Court for the Eastern District of Virginia, Alexandria Division, then jurisdiction shall be in the Circuit Court of Fairfax County, Fairfax, Virginia.

****X. dot com biz card Content.** You are solely responsible for the content you furnish for inclusion in your dot com biz card. NSI cannot and does not design,

review or screen content provided in dot com biz cards by you and does not assume any obligation to monitor such content. HOWEVER, YOU AGREE THAT WE MAY REVIEW YOUR DOT COM BUSINESS CARD IN RESPONDING TO A THIRD PARTY COMPLAINT, AND NSI RESERVES THE RIGHT AT ITS SOLE DISCRETION TO REMOVE ANY DOT COM BUSINESS CARD, WITHOUT NOTICE AND WITH NO OBLIGATION TO REFUND FEES PAID, WHICH IN OUR JUDGMENT WE DETERMINE TO BE UNSUITABLE OR OTHERWISE UNLAWFUL OR HARMFUL. The content in your dot com biz card may be deemed by us to be unsuitable if, in our view, it:

- a. contains, promotes or links to sexually explicit or violent material;
- b. promotes, depicts or links to material that promotes or depicts discrimination based on race, gender, religion, national origin, physical or mental disability, sexual orientation, or age;
- c. contains unlawful material, including but not limited to materials that may violate another's intellectual property rights, or links to a site that contains such material;
- d. contains information regarding, promotes or links to a site that provides information or promotes illegal activity;
- e. is considered by us or any person with access to such content to be obscene, lewd, lascivious, filthy, excessively violent, harassing or otherwise objectionable, whether or not such material is constitutionally protected; or
- f. is deemed by us to be unsuitable for any other reason.

You understand that we reserve the right to conclude that your dot com biz card has content that is unsuitable in accordance with our standards, and we may come to such a conclusion even if it is based upon our opinion or mere suspicion or belief, without any duty to prove that our opinion or suspicion is well-founded and even if our opinion or suspicion is proven not to be well-founded or if we provide other customers dot com biz cards despite such web pages having the same or similar characteristics as your dot com biz card. You also understand that by providing you the Network Solutions service for the dot com biz card, NSI in no way endorses your dot com biz card or deems your content to be suitable under the terms of this Agreement.

*****Y. dot com forwarding.** You represent and warrant that you have the necessary rights to use the dot com forwarding service to forward, point, alias or resolve your domain name(s) to the other domain name designated by you in ordering such services.

Z. Infancy. You attest that you are of legal age to enter into this Agreement.

This is NSI Service Agreement Version Number 3.0. This Service Agreement is for all Network Solutions services offered by NSI.

[Use your browser's back button (if available) or close this window to return to the previous screen.]



Legal Information

[Close this window or use your browser's back button to return to the previous screen.]

NETWORK SOLUTIONS' DOMAIN NAME DISPUTE POLICY

Revision 03
Effective February 25, 1998

1. Network Solutions, Inc. ("Network Solutions") is responsible for the registration of second-level Internet domain names in the top level COM, ORG, NET, and EDU domains. Network Solutions registers these second-level domain names on a "first come, first served" basis. By registering a domain name, Network Solutions does not determine the legality of the domain name registration, or otherwise evaluate whether that registration or use may infringe upon the rights of a third party.

2. The entity applying for a domain name ("registrant") is solely responsible for selecting its own domain name ("domain name") and maintaining for the continued accuracy of the registration record. The registrant, by completing and submitting the Domain Name Registration Agreement ("Registration Agreement"), represents that the statements in its application are true and that the registration of the selected domain name, to the best of the registrant's knowledge, does not interfere with or infringe upon the rights of any third party. The registrant also represents that the domain name is not being registered for any unlawful purpose.

3. Network Solutions neither acts as arbiter nor provides resolution of disputes between registrants and third party complainants arising out of the registration or use of a domain name. This Domain Name Dispute Policy ("Policy") does not confer any rights, procedural or substantive, upon third party complainants. Likewise, complainants are not obligated to use this Policy.

4. This Policy does not limit the administrative or legal procedures Network Solutions may use when third party conflicts arise, or when Network Solutions is presented with information that a domain name violates the legal rights of a third party, including, but not limited to, information that the display or use of the domain name is expressly prohibited by a United States federal statute or regulation.

5. **Modifications.** The registrant acknowledges and agrees that Network Solutions may modify or amend this Policy from time to time, and that such changes are binding upon the registrant. Network Solutions will post the revised Policy at <http://www.netsol.com/rs/dispute-policy.html> at least thirty (30) calendar days before it becomes effective.

6. **Indemnity.** The registrant hereby agrees to defend, indemnify and hold harmless (i) Network Solutions, its officers, directors, employees and agents, and (ii) the National Science Foundation ("NSF"), its officers, directors, and employees (collectively, the "Indemnified Parties"), for any loss or damages

awarded by a court of competent jurisdiction resulting from any claim, action, or demand arising out of or related to the registration or use of the domain name. Such claims shall include, without limitation, those based upon trademark or service mark infringement, tradename infringement, dilution, tortious interference with contract or prospective business advantage, unfair competition, defamation or injury to business reputation. Each Indemnified Party shall send written notice to the registrant of any such claim, action, or demand against that party within a reasonable time. The failure of any Indemnified Party to give the appropriate notice shall not affect the rights of the other Indemnified Party. Network Solutions recognizes that certain educational and governmental entities may not be able to provide complete indemnification. If the registrant is (i) a governmental or non-profit educational entity, and (ii) not permitted by law or under its organizational documents to provide indemnification, the registrant must notify Network Solutions in writing and, upon receiving appropriate proof of such restriction, Network Solutions may provide an alternative provision for such a registrant.

7. Revocation. The registrant agrees that Network Solutions shall have the right in its sole discretion to revoke, suspend, transfer or otherwise modify a domain name registration upon thirty (30) calendar days prior written notice, or at such time as Network Solutions receives a properly authenticated order from a court of competent jurisdiction, or arbitration award, requiring the revocation, suspension, transfer or modification of the domain name registration.

8. Dispute Initiation. Registrant agrees that while Network Solutions can neither act as an arbiter nor provide resolution of disputes arising out of the registration and use of a domain name, Network Solutions may be presented with information that a domain name possibly violates the trademark rights of a trademark owner. Network Solutions may apply the procedures described in Section 9 when a third party complainant ("complainant") presents Network Solutions with satisfactory evidence of both trademark ownership and written notice to the domain name registrant describing the legal harm the trademark owner is incurring. The documents required in support of a complainant's written request that Network Solutions invoke Section 9, Dispute Procedures, must include:

(a) An original, certified copy, not more than six (6) months old, of a trademark registration ("certified registration"), which is in full force and effect and is identical to a second-level domain name (i.e., not including COM, NET, ORG, or EDU) on the principal or equivalent registry of any country (copies certified in accordance with 37 CFR 2.33(a)(1)(viii) or its successor will meet this standard for registrations in jurisdictions other than the United States). Trademark or service mark registrations from the supplemental or equivalent registry of any country, or from individual states or provinces of a nation, will not be accepted. Trademarks incorporating a design will not be accepted; and

(b) A copy of the written prior notice sent to the domain name registrant by the complainant, and a representation by the complainant indicating the mode of delivery of the notice (e.g., first class mail, overnight delivery) and the factual basis for believing that the domain name registrant received the notice. Notices must be sent to the mailing address of the domain name registrant as provided in Network Solutions' WHOIS database. The notice to the domain name registrant must clearly state that the complainant believes the registration and use of the disputed domain name violates the trademark rights of the complainant; the notice must also clearly allege the factual and legal bases for the belief. Network Solutions will not undertake any separate investigation of

the statements in such notice.

9. Dispute Procedures. In those instances where a third party claim is based upon and complies with Section 8(a and b), Network Solutions may apply the following procedures, which recognize that trademark ownership does not automatically extend to the right to register a domain name and which reflect no opinion on the part of Network Solutions concerning the ultimate determination of the claim:

(a) Network Solutions shall determine the creation date of the registrant's domain name registration ("domain name creation date").

(b) If the registrant's domain name creation date precedes the effective date of the valid and subsisting certified registration owned by the complainant, Network Solutions will take no action on the complainant's request.

(c) If the domain name creation date is after the effective date of the valid and subsisting certified registration owned by the complainant, then Network Solutions shall request from the registrant proof of ownership of registrant's own registered trademark or service mark by submission of a certified registration, of the type and nature specified in Section 8(a) above. The certified registration must be owned by the registrant and the effective date must be prior to the date of any third party's notice of a dispute to the registrant. If the registrant satisfies the requirements of this Section 9(c), Network Solutions will take no further action on the complainant's request.

(d) If the domain name creation date is after the effective date of the valid and subsisting certified registration owned by the complainant, and the registrant fails to provide a certified registration as specified in Section 8 (a) to Network Solutions within thirty (30) calendar days of receipt of Network Solutions' dispute notification letter, Network Solutions will assist the registrant with registration of a new domain name, and will allow the registrant to maintain both names simultaneously for up to ninety (90) calendar days to allow an orderly transition to the new domain name. Network Solutions will provide such assistance to a registrant if and only if, within thirty (30) calendar days of receipt of Network Solutions' dispute notification letter, the registrant (1) submits a Registration Agreement requesting the registration of a new domain name; and (2) submits an explicit written request to Network Solutions' Business Affairs Office, including an identification of the registrant's desired new domain name and the NIC tracking number (for example, NIC-981125.1234) assigned by Network Solutions in response to the new Registration Agreement. At the end of the ninety (90) calendar day period of simultaneous use, Network Solutions will place the disputed domain name on "Hold" status, pending resolution of the dispute. As long as a domain name is on "Hold" status, that domain name registered to the registrant shall not be available for use by any party.

(e) In the event the registrant fails to select one of the following options by a written response, received by Network Solutions' Business Affairs Office within thirty (30) calendar days of receipt of Network Solutions' dispute notification letter, Network Solutions will place the domain name on "Hold" (wherein the domain name will not be available for use by any party) pending resolution of the dispute:

(1) Provide the documentation required by Section 9(c) of this

Policy,

(2) Relinquish the domain name and transfer it to the complainant,

(3) Register a new and different domain name pursuant to Section 9(d) of this Policy,

or

(4) File a civil action and provide a copy of a file-stamped complaint pursuant to Section 10 of this Policy.

(f) Network Solutions will reinstate the domain name placed in "Hold" status, or will not place it in "Hold" status, (i) upon receiving a properly authenticated temporary or final order by a court of competent jurisdiction, or arbitration award, stating which party to the dispute is entitled to the domain name, (ii) if Network Solutions receives other satisfactory evidence from the parties of the resolution of the dispute, or (iii) the complainant requests that the domain name not be placed on "Hold.

(g) A domain name registrant involved in Dispute Procedures remains subject to the terms and conditions of the Registration Agreement, including fees.

10. **Litigation.** Independent of the provisions of Section 9 of the Policy, in the event that:

(a) The registrant files a civil action related to the registration and use of the domain name against the complainant in a court of competent jurisdiction, and provides Network Solutions with a copy of the file-stamped complaint, Network Solutions will maintain the status quo ante of the domain name record pending a temporary or final decision of the court. For example, if the domain name is not on "Hold," it will not be placed on "Hold;" if the domain name is already on "Hold," it will remain on "Hold." In such cases, Network Solutions will deposit control of the domain name into the registry of the court by supplying the registrant with the registry certificate for deposit. While the domain name is in the registry of the court, Network Solutions will not make any changes to the domain name record unless ordered by the court. The registrant also shall promptly provide copies of any and all pleadings filed in the action to Network Solutions upon Network Solutions' request.

(b) The complainant files a civil action related to the registration and use of the domain name against the registrant in a court of competent jurisdiction, and provides Network Solutions with a copy of the file-stamped complaint, Network Solutions will maintain the status quo ante of the domain name record pending a temporary or final decision of the court. For example, if the domain name is not on "Hold," it will not be placed on "Hold;" if the domain name is already on "Hold," it will remain on "Hold." Network Solutions will deposit control of the domain name into the registry of the court by supplying the complainant with the registry certificate for deposit. While the domain name is in the registry of the court, Network Solutions will not make any changes to the domain name record unless ordered by the court.

(c) In both instances, under Section 10(a and b), Network Solutions will abide by those provisions of temporary or final court orders, or arbitration

awards, directing the disposition of the domain name, without being named as a party to the civil action. The civil action must include the domain name registrant as a party. If named as a party to a civil action, Network Solutions shall not be limited to the above actions, but reserves the right to raise any and all defenses deemed appropriate, and to take any other action necessary to defend itself.

(d) A domain name registrant involved in Litigation remains subject to the terms and conditions of the Registration Agreement, including fees.

11. **DISCLAIMER.** THE REGISTRANT AGREES THAT NETWORK SOLUTIONS WILL NOT BE LIABLE FOR ANY LOSS OF REGISTRATION AND USE OF REGISTRANT'S DOMAIN NAME, OR FOR INTERRUPTION OF BUSINESS, OR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY KIND (INCLUDING LOST PROFITS) REGARDLESS OF THE FORM OF ACTION WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), OR OTHERWISE, EVEN IF NETWORK SOLUTIONS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL NETWORK SOLUTIONS' MAXIMUM LIABILITY EXCEED FIVE HUNDRED (\$500.00) DOLLARS.

12. **Notices.** All notices between Network Solutions and its registrants permitted or required under this Policy shall be in writing and shall be delivered by personal delivery, courier delivery, facsimile transmission, and/or by first class mail, and shall be deemed given upon delivery, transmission, or seven (7) calendar days after deposit in the mail, whichever occurs first. Initial notices shall be sent to the domain name registrant at the address of the domain name registrant listed in Network Solutions' WHOIS database.

13. **Non-Agency.** Nothing contained in this Policy shall be construed as creating any agency, partnership, or other form of joint enterprise between the parties.

14. **Non-Waiver.** The failure of Network Solutions to require performance by the registrant of any provision hereof shall not affect the full right to require such performance at any time thereafter; nor shall the waiver by Network Solutions of a breach of any provision hereof be taken or held to be a waiver of the provision itself.

15. **Breach.** The registrant's failure to abide by any provision under this Policy may be considered by Network Solutions to be a material breach and Network Solutions may provide a written notice, describing the breach, to the registrant. If, within thirty (30) calendar days of the date of such notice, the registrant fails to provide evidence, which is reasonably satisfactory to Network Solutions, that it has not breached its obligations, then Network Solutions may revoke registrant's registration of the domain name. Any such breach by a registrant shall not be deemed to have been excused simply because Network Solutions did not act earlier in response to that, or any other, breach by the registrant.

16. **Invalidity.** In the event that any provision of this Policy shall be unenforceable or invalid under any applicable law or be so held by applicable court decision, such unenforceability or invalidity shall not render this Policy unenforceable or invalid as a whole. Network Solutions will amend or replace such provision with one that is valid and enforceable and which achieves, to the extent possible, the original objectives and intent of Network Solutions as reflected in the original provision.

17. **Entirety.** This Policy, as amended, and the current Registration Agreement together constitute the complete and exclusive agreement between Network Solutions and the registrant, and supersede and govern all prior proposals, agreements, or other communications. The registrant agrees that registration of a domain name constitutes an agreement to be bound by this Policy, as amended from time to time.

This file last modified 2/25/98.

[Close this window to return to the previous screen.]

Questions? Please email help@networksolutions.com
© Copyright 1999 Network Solutions, Inc. All rights reserved.

Please read our [Disclaimer](#).

HELP

[General](#) | [Reservation](#) | [Registration](#) | [Make Changes](#)

Network Solutions' Domain Name Dispute Policy (Rev. 03)

The Domain Name Dispute Policy is incorporated by reference into the Domain Name Registration Agreement. Section 8 of the Policy describes what documents Network Solutions requires from a trademark owner complainant, while Section 9 outlines the actions we would take upon receipt of the complaint. Section 10 covers Network Solutions' procedures when we receive notice of litigation. All other Sections are not subject to review and/or enforcement by third parties. In other words, we decline all third party requests to apply any Section other than 8, 9 or 10 of the Domain Name Dispute Policy.

As a private company, Network Solutions cannot provide legal advice. We suggest that you contact an attorney if you:

Object to a domain name that is the same or similar to your company name or copyright

Object to a domain name that is the same or similar to an individual's name

Object to a domain name that is the same or similar to a phone number

Object to a domain name that is similar to your domain name

Object to the use of your copyright or trademark on a web site

Object to the content of a web site

Object to the use of a domain name

Have questions about what are legal or illegal activities

Have received a cease and desist letter or a letter of complaint

Have any questions related to your legal rights or your trademark rights

Have a dispute between the Internet Service Provider and the domain name registrant

Require information on case law, i.e. related court cases and relevant court orders

1. If the registrant isn't using the domain name registration, shouldn't it be made available to someone who wants to use it?
2. The contact information in WHOIS isn't valid. Do you have any additional information?

3. Can you let me know when a domain name will be deleted for non-payment?
4. Can I be next in line if the domain name registration is deleted?
5. A vendor registered my domain name in its own name, then promised to transfer it back to me. That hasn't happened yet. Can you help?
6. How do I dispute a domain name registered under a top-level country code?
7. I want to change my domain name registration to another one. Can you switch my payment?
8. Has anyone else complained about this domain name registration?
Would you give me the historical information on a domain name registration?
9. What is an original certified copy?
10. What's the effective date of a trademark?
11. Explain what you mean by "representation regarding delivery."
12. What does "identical" mean?
13. Who can submit a complaint?
14. What should the complainant do if its notice letter was returned by the postal service?
15. Where should I send my documents in support of my complaint?
16. If a domain name registrant has a trademark that is identical to the whole domain name, including the top-level, will they be allowed continued use of the domain name?
17. When can a domain name registrant get a free name?
18. Will Network Solutions take away the domain name registration and give it to the trademark owner?
19. When will the domain name registration be placed on "Hold"?
20. What happens after the domain name registration is placed on "Hold"? When will the "Hold" be removed? How are disputes resolved?
21. If my domain name registration is on "Hold," do I still have to pay the registration and re-registration fees?
22. What happens if a disputed domain name registration is deleted?
23. Is Section 10 contingent upon Sections 8 and 9?
24. Does Network Solutions abide by foreign court orders?
25. What kind of court order would Network Solutions comply with?
26. If a lawsuit is filed, will the domain name registration be placed on "Hold" immediately?

General

1. **If the registrant isn't using the domain name registration, shouldn't it be made available to someone who wants to use it?**

There is no "use" requirement for domain names. We suggest you contact the domain name registrant to discuss the disposition of a domain name registration.

2. **The contact information in WHOIS isn't valid. Do you have any additional information?**

The domain name registrant provides the information in the WHOIS database, and is

responsible for its accuracy. We do not have any additional information.



3. Can you let me know when a domain name will be deleted for non-payment?

Payment information is confidential. We suggest that you check Network Solutions' database frequently if you are waiting for a domain name to become available.



4. Can I be next in line if the domain name registration is deleted?

No. Registrations are accepted on a "first come, first served" basis. Once the domain name is available, you may submit a Domain Name Registration Agreement for it.



5. A vendor registered my domain name in its own name, then promised to transfer it back to me. That hasn't happened yet. Can you help?

We cannot enforce third party agreements, and suggest that you consult with an attorney.



6. How do I dispute a domain name registered under a top-level country code?

Network Solutions only administers its Dispute Policy for domain names in the COM, NET, ORG and EDU top-level domains. You should contact the administrator of the specific country code top-level domain for information. The Internet Assigned Numbers Authority maintains a list of contact information for each country code top-level domain. We recommend you visit this site to obtain contact information specific to your dispute.



7. I want to change my domain name registration to another one. Can you switch my payment?

Each domain name registration is unique. The registration fee cannot be transferred from one domain name registration to another. If you would like to register another domain name, you will be invoiced for the registration fee.



**8. Has anyone else complained about this domain name registration?
Would you give me the historical information on a domain name registration?**

Registration information is confidential, and will be supplied only to the domain name registrant or its attorney.

Section 8

9. What is an original certified copy?

An original certified copy is a special type of copy available from the government agency that issued the trademark. It is not your original trademark registration.

10. What's the effective date of a trademark?

The Policy refers to a trademark's "effective date" because of the varied nature of effective dates for trademark registrations. When Network Solutions receives a trademark in support of a complaint, we research to determine the effective date of a trademark based on the accepted practices of the trademark's country of origin. For example, the effective date of a United States trademark registration is the earlier of the filing date or the first use date.

11. Explain what you mean by "representation regarding delivery."

We require the complainant to tell us how the notice was delivered to the mailing address, and why he thinks it was received. We do not accept notices delivered via facsimile or email.

12. What does "identical" mean?

We compare the trademark to the second-level domain name, in other words, not including the .COM, .NET or .ORG. We do not accept trademarks incorporating any design elements. If you would like us to compare a specific trademark to a domain name, you may fax the trademark registration with your request to the Business Affairs Office at (703) 742-8706.

13. Who can submit a complaint?

The trademark owner, its attorney, or its sole, exclusive licensee or its attorney, must write the notice letter to the domain name registrant and the cover letter to Network Solutions. We cannot accept complaints from Internet Service Providers or other agents of the trademark owner.



14. What should the complainant do if its notice letter was returned by the postal service?

The complainant should send its documents and a photocopy of the returned envelope to Network Solutions, Inc.



15. Where should I send my documents in support of my complaint?

You may submit your documents to Network Solutions, Inc., Attn: Business Affairs Office, 505 Huntmar Park Drive, Herndon, VA 20170-5139.



Section 9

16. If a domain name registrant has a trademark that is identical to the whole domain name, including the top-level, will they be allowed continued use of the domain name?

No. If Section 9 is applied, the domain name registrant must supply a trademark that is identical to the second-level domain name, just as the complainant did. If the disputed domain name registration is EXAMPLE.COM, the complainant's trademark must be for the word "EXAMPLE." The domain name registrant must also supply a trademark for "EXAMPLE" for continued use of the domain name registration; we would not accept the registrant's trademark for "EXAMPLE.COM."



17. When can a domain name registrant get a free name?

If and when we do decide to apply Section 9, we will not take action without giving the domain name registrant written notice, and providing him with thirty-seven days from the date of the letter to respond. If the domain name registrant chooses another domain name registration in response to our letter, and has paid the registration fee for the disputed domain name, we will waive the registration fee for the new domain name.

18. Will Network Solutions take away the domain name registration and give it to the trademark owner?

If Section 9 is applied, we will not take action without giving the domain name registrant written notice, and providing him with thirty-seven days from the date of the letter to respond. This may lead to the domain name being placed on "Hold," but it does not provide for an automatic transfer of the domain name registrant to the complainant.

19. When will the domain name registration be placed on "Hold"?

The domain name registration can be placed on "Hold" if the registrant doesn't respond to our dispute notification letter, if the registrant chooses the "Hold" option of our letter, or at the end of the simultaneous use period.

20. What happens after the domain name registration is placed on "Hold"? When will the "Hold" be removed? How are disputes resolved?

The domain name will remain on "Hold" until Network Solutions receives a resolution to the dispute, in the form of one of the following:

- 1) a bilateral agreement signed by both parties to the dispute,
- 2) an order from a court of competent jurisdiction, or an arbiter,
- 3) a written request from the trademark owner withdrawing the complaint,
- 4) a transfer of the domain name from the registrant to the trademark owner,
- 5) a deletion request from the domain name registrant, or
- 6) deletion of the domain name for non-payment of the registration fee.

21. If my domain name registration is on "Hold," do I still have to pay the registration and re-registration fees?

Yes.

22. What happens if a disputed domain name registration is deleted?

Network Solutions will give the complainant an opportunity to register the domain name

only if Section 9 has been applied.

Section 10

23. Is Section 10 contingent upon Sections 8 and 9?

No.

24. Does Network Solutions abide by foreign court orders?

Section 10 of the Policy applies to any court of competent jurisdiction in the United States or abroad.

25. What kind of court order would Network Solutions comply with?

We will abide by temporary or final court orders directing the disposition of the domain name registration if the registrant is a party to the suit. The order must specify the action to be taken regarding a specific domain name registration. The domain name specified in the court order must include the top-level COM, NET or ORG. We cannot enforce any other terms of a court order.

26. If a lawsuit is filed, will the domain name registration be placed on "Hold" immediately?

Network Solutions maintains the status quo ante of the domain name registration when we receive notice of litigation. If the domain name is active, it will remain active. If the domain name is on "Hold," it will remain on "Hold."

The Domain Name Handbook

CONTACT US | ORDER BOOK | SITE INDEX

CONTENTS

CONTENTS / CD-ROM / TABLES / FIGURES

SPECIAL FEATURES

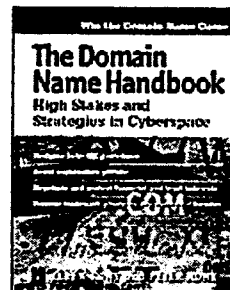
DNS NEWS

OPINIONS

GLOSSARY

ACKNOWLEDGMENTS

Ellen Rony and Peter Rony,
The Domain Name Handbook: High Stakes and Strategies in Cyberspace
(R&D Books: Lawrence, Kansas) 1998. 645 pp. *plus* CD-ROM. ISBN 0879305150



The Domain Name Handbook provides a comprehensive and lively discussion of the policies, protocols, procedures, principles, controversies, and initiatives associated with the domain name system. See Press Release: "[Internet Domain Names Are Focus of Hefty New Handbook.](#)"

TABLE OF CONTENTS

BOOK
Errata

Preface

Acknowledgements

Chapter 1. Introduction

Chapter 2. What's In a Name?

2.1 The Memory Palace of the Online Age

2.2 Meta Symbols

2.3 Alphanumeric IDs

2.3.1 Vanity Plates

2.3.2 Novelty Telephone Numbers

2.3.3 Ticker Symbols

2.4 Namesmithing

2.5 New Identities

2.6 Generic Domain Names

2.7 WYSIWYE: What You See Isn't What You Expected

2.8 Late to the Party

2.9 Not About Elvis

Chapter 3. How Does the Domain Name System Work?

3.1 Here Come the Acronyms: IP, TLD, DNS, and URL

3.2 Background on Hierarchies and the International Telephone, Postal, and Networked Computer Addressing Systems

3.2.1 What is a Hierarchy?

3.2.2 The International Postal System

3.2.3 The International Telephone System

3.3 The International Networked Computer System

3.3.1 International Top-Level Domains (iTLDs)

3.3.2 United-States-Only .US Top-Level Domain (TLD)

3.3.3 ISO 3166 Country-Specific Top-Level Domains (TLDs)

3.3.4 32-Bit Internet Protocol (IP) Addresses

3.3.5 Class A, Class B, and Class C Networks on the Internet

3.3.6 URLs are an Extension of the DNS

3.3.7 "Virtual Hosting"

3.4 How Do Domain Name Servers Work?

3.4.1 Is the DNS Important? An Example of DNS Corruption

3.4.2 The Domain Name System is Hierarchical

3.4.3 The Domain Name System is Distributed

3.4.4 The Domain Name System is Interdependent

3.4.5 The Domain Name System Requires Unique Addresses

3.4.6 The Objective of a Domain Name Server

3.4.7 Different Types of Name Servers: ISP, Root, TLD, and SLD

3.4.8 A Graphical Look at a DNS Query and Response

3.5 Examples of Domain Name Server Files (June 1997)

3.5.1 Top-Level InterNIC Zone Files

3.5.2 Sources of DNS Networking Information

3.5.3 Definitions: DNS Domains and Zones

3.5.4 Definitions: Types of Configuration Files on a DNS Name Server

3.5.5 Definitions: What do . ("dot"), IN, SOA, A, NS, 518400, and 172800

in a Resource Record Mean?

3.5.6 InterNIC Readme file

3.5.7 A Multilevel Hierarchy for Identifying a Host Address

Chapter 4. Follow the RFCs: The Development of the Domain Name System

4.1 Introduction: The Origins of the Internet

4.2 Jon Postel, the Czar Who Wears Multiple Hats

4.3 Requests for Comment (RFCs)

4.4 DNS Chronology: Follow the RFCs

4.5 Governance and Control Issues (1946-1993)

4.6 Assigned Numbers Terminology

4.7 Assigned Numbers (starting 1971)

4.8 Network Addresses

4.8.1 8-Bit Network Addresses (1974 to 1981)

4.8.2 32-Bit Network Addresses (1981)

4.9 Domain Naming Convention (1982)

4.10 Resource Records (1983)

4.11 Name Servers, Resolvers, Domain Name Space, Zones, and Domain Authority (1983)

- 4.12 The .COM, .ORG, .NET, .GOV, .EDU, and .MIL Top Level Domains (1984)
- 4.13 SRI Network Information Center (NIC) (1984)
- 4.14 Defense Data Network Information Center (SRI-NIC) (1987)
- 4.15 NIC Handle and WHOIS (1987)
- 4.16 Organizations Active in Internet Standards Matters (1988)
- 4.17 Internet Assigned Numbers Authority (IANA)
 - 4.17.1 IANA: "A Riddle Wrapped in a Mystery Inside an Enigma" (1988)
 - 4.17.2 Internet Standards Activity (1993)
 - 4.17.3 Authority by Announcement (1994)
- 4.18 RFC "Numbers" File Sizes (1972-1994)
- 4.19 High-Performance Computing Act (December 9, 1991)
- 4.20 National Science Foundation
 - 4.20.1 Transfer Registration Activity to GSI (1991)
 - 4.20.2 Fund USC-ISI to Operate .US Top-Level Domain (1992)
 - 4.20.3 Transfer Registration Activity to NSI (1993)
- 4.21 Chronology of Organization Creation (1946-1993)

Chapter 5. Introduction to Internet Registries, InterNIC Policies, and NSF/NSI Agreements

- 5.1 The Internet Registries
- 5.2 Introduction to Network Solutions, Inc. (NSI) Policies & "A Lightning Rod for Lawsuits"
- 5.3 Original NSI Domain Dispute Policy (July 28, 1995)
 - 5.3.1 Recommended Section Titles for July 28, 1995 Version
 - 5.3.2 Right to Use Name
 - 5.3.3 Disclaimer: Waiver of NSI Liability
 - 5.3.4 Trademark Challenges
 - 5.3.5 Domain Names That are Covered by the Policy
 - 5.3.6 Binding Arbitration
 - 5.3.7 "Hold" Status
- 5.4 Fee Policy for Registration of Domain Names (September 14, 1995)
- 5.5 NSI Domain Dispute Policy - Revision 01 (November 23, 1995)
 - 5.5.1 Recommended Section Titles for Revision 01
 - 5.5.2 Eliminate the Word, Resolution
 - 5.5.3 Specify the .COM, .ORG, .GOV, .EDU, and .NET Domains
 - 5.5.4 Indemnify NSI, NSF, IANA, IAB, and ISOC
 - 5.5.5 Arbitration Panel
 - 5.5.6 Trademark Challenges
 - 5.5.7 What is Identical?
 - 5.5.8 "Hold" Status
 - 5.5.9 The Crossover Effect
 - 5.5.10 Indemnification Agreement
- 5.6 NSI Domain Dispute Policy - Revision 02 (September 9, 1996)
 - 5.6.1 Revision 02 Section Titles
 - 5.6.2 Revision 02 Changes
 - 5.6.3 Secret Proceedings
 - 5.6.4 Special Relief
- 5.7 NSI Domain Dispute Policy - Revision 03 (February 25, 1998)
- 5.8 Lame Delegation Policy - not yet implemented (announced February 13, 1996)

5.9 Follow the Money; The Bankroller: NSF –National Science Foundation

5.9.1 The Ante: Cooperative Agreement No. NCR-9218742
(January 1993)

5.9.2 Additional Chips: Amendments 1, 3 and 5 (1994-1995)

5.9.3 The Jackpot: Amendment 4 (September 1995)

5.10 Office of the Inspector General Report: The Administration of Internet Addresses (February 1997)

5.11 Network Solutions, Inc. Initial Public Offering (July 3, 1997)

5.12 Other Registries

5.12.1 Australia (AUNIC)

5.12.2 France (French Network Information Center - NIC France)

5.12.3 United Kingdom (Nominet UK)

5.12.4 Canada (CA Net)

5.12.5 China (China Internet Network Information Center- CNNIC)

5.12.6 Japan (Japanese Network Information Center - JPNIC)

5.12.7 Switzerland and Lichtenstein (Swiss Academic and Research Network - SWITCH)

5.12.8 Comparative International TLD Registration Fees

Chapter 6. Domain Registration and Modification

6.1 Introduction

6.2 Who May File for a Domain?

6.3 The InterNIC Web Site

6.3.1 The Search Engine for Registration Services

6.3.2 WHOIS: How to Find Information About Domains and Sites, Part I

6.3.3 Overview of the Registration Process

6.3.4 InterNIC Policies and Processes

6.4 Domain Name Registration: The Difficult, Easy and the Important Items

6.4.1 Domain Name Registration Templates: Web and Text Versions

6.4.2 Domain Name Template Blank Version 3.5

6.4.3 Example: Completed Version 3.5 Template

6.4.4 NIC Handle

6.4.5 The Difficult . . .

6.4.6 The Easy . . .

6.4.7 . . . and the Important

6.4.8 Primary and Secondary Name Servers

6.4.9 Guardian Authentication

6.4.10 Domain Name and Organization Using Domain Name

6.4.11 Administrative, Technical, and Billing Contacts

6.4.12 Other Registration Templates

6.4.13 Registration and Renewal Fees

6.4.14 Modify, Transfer or Delete Registration

6.4.15 A Dozen Tips to Simplify Processing

6.5 Registration-Related Tools

6.5.1 WHOIS: How to Find Information About Domains and Sites, Part II

6.5.2 The Registration Services Home Page

- 6.5.3 Help Desk
- 6.5.4 Registration Tracking System
- 6.5.5 FTP Archive
- 6.5.6 InterNIC-hosted Mailing Lists (Listservs)
- 6.5.7 Server Digital ID for Internet Service Providers
- 6.5.8 Referral Whois (RWhois)
- 6.6 Frequently Asked Questions (FAQs)
 - 6.6.1 How Many Domain Names Can a Corporation Register?
 - 6.6.2 Our Organization Name is Already Registered to Someone Else. What Can We Do?
 - 6.6.3 Can I Register the Same Name in More Than One Top Level Domain?
 - 6.6.4 If Another Company Has a Trademark for the Name We Want, But it is used for a Different Class of Goods, Can We Register the Name?
 - 6.6.5 Can a Foreign Company Register a .COM Domain?
 - 6.6.6 Should the ISP Register as Administrative Contact for a Client's Domain?
 - 6.6.7 What Happens to the .COM Registration Fee After the NSI Agreement Terminates?
 - 6.6.8 Can the Organization Listed in Section 3 of the Domain Registration Agreement be Changed?
 - 6.6.9 Can Anybody Submit a Request to Change My Domain Record if I Don't use PGP or Choose an Encrypted Password?
 - 6.6.10 How Will I be Billed by InterNIC?
 - 6.6.11 Who Receives the Maintenance Billing?
 - 6.6.12 What Happens if I Do Not Pay?
 - 6.6.13 What Happens if a Domain Name Lapses?
 - 6.6.14 Is the Registration/Maintenance Fee Taxable?
 - 6.6.15 Can I take My Name if I Change Service Providers?
 - 6.6.16 How Do We Notify InterNIC of a Domain Registration Change, or Do We Bother?
 - 6.6.17 My Original ISP Was Bought Out. What Do I Do Next?
 - 6.6.18 Do You accept domain name record modifications via fax?
 - 6.6.19 How Do You Transfer a Domain Name?

Chapter 7. Basic Principles of Trademark Law

- 7.1 The Lanham Act of 1946
- 7.2 Trademark Registration
- 7.3 Trademark Infringement
- 7.4 Trademark Dilution
- 7.5 Internet Trademark Issues
- 7.6 International Coordination
 - 7.6.1 World Intellectual Property Organization (WIPO)
 - 7.6.2 The Paris Convention
 - 7.6.3 The Madrid Agreement and Madrid Protocol
 - 7.6.4 The Nice Agreement
 - 7.6.5 The Lisbon Agreement
 - 7.6.6 The Vienna Agreement
 - 7.6.7 The Nairobi Treaty
 - 7.6.8 The Treaty of European Union
 - 7.6.9 Trademark Law Treaty
 - 7.6.10 The Uruguay Round and the World Trade Organization

7.6.11 Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS)

7.6.12 International Trademark Association (INTA)

Chapter 8. Domain Name Collisions

- 8.1 KAPLAN.COM: Arch-Rival's Ruse
Kaplan Educational Center, Ltd. v. Princeton Review Management Corp. (filed March 9, 1994)
- 8.2 MTV.COM: The Curry Chronicles
MTV Networks v. Adam Curry - Memorandum and Order (October 28, 1994)
- 8.3 MCDONALDS.COM Mac Attack
Joshua Quittner/McDonalds Corp. (October 1994)
- 8.4 BOB.COM and NOT-BOB.COM: Strange Bedfellows
Bob Antia/Microsoft Corp. (May 1995)
- 8.5 BBB.ORG: A Famous Identifier
Council of Better Business Bureaus, Inc. v. Mark Sloo - (filed May 9, 1995)
- 8.6 INTER-LAW.COM: Almost Identical
Jeff Liebling, dba The 'Lectric Law Library v. Interlaw Ltd., et. al. (filed February 15, 1996)
- 8.7 JURIS.COM: Safety Net
The Comp Examiner Agency, inc. dba 25th Century Internet Publishers v. Juris, Inc. - Preliminary Injunction (April 26, 1996; corrected May 22, 1996)
- 8.8 CANDYLAND.COM: Club Love Meets Milton Bradley
Hasbro, Inc. v. Internet Entertainment Group, Ltd. - Preliminary Injunction (February 9, 1996)
- 8.9 PETA.ORG: Acrimony Over an Acronym
People Eating Tasty Animals/People for the Ethical Treatment of Animals (March 1996)
- 8.10 AVON.COM: Federal Dilution
Avon Products, Inc. v. Carnetta Wong Associates (filed February 2, 1996)
- 8.11 INSET.COM: Personal Jurisdiction
Inset Systems, Inc. v. Instruction Set, Inc. - Denial of Defendant's Motion to Dismiss (April 17, 1996)
- 8.12 CYBERGOLD: Purposeful Availment
Maritz, Inc. v. CyberGold, Inc. - Memorandum and Order (August 19, 1996)
- 8.13 ESQWIRE.COM: Phonetically Similar
Hearst Corp. v. Ari Goldberger - Complaint (May 15, 1996)
Report and Recommendation (February 26, 1997)
- 8.14 CARDSERVICE.COM: Permanent Injunction
Cardservice International, Inc. v. Webster R. McGee and WRM & Associates - Memorandum, Order and Permanent Injunction (January 16, 1997)
- 8.15 ZIPPO.COM: Remote Transactions
Zippo Mfg. Co. v. Zippo Dot Com - Summons and Complaint (November 18, 1996)
Memorandum Opinion (January 16, 1997)
- 8.16 GATEWAY.COM: Famous, Not First
Gateway 2000, Inc. v. Gateway.Com, Inc. and Alan B. Clegg -

Order (February 6, 1997)

- 8.17 PLANNEDPARENTHOOD.COM: Confusion Likely
Planned Parenthood Federation of America v. Richard Bucci, dba
Catholic Radio - Opinion and Order (March 24, 1997)
- 8.18 PRINCE.COM: Battle Royale
Prince PLC v. Prince Sports Group - High Court Opinion (July 31,
1997)
- 8.19 Other Disputes

Chapter 9. Caught in the Crossfire: Challenges to NSI

9.1 Domain Registrants vs. NSI

9.1.1 ROADRUNNER.COM: Leading the Charge

Roadrunner Computer Systems, Inc. v. Network Solutions,
Inc. - Complaint (March 26, 1996)

Declaration in Support of Preliminary Injunction (March 26,
1996)

Memorandum in Support of Preliminary Injunction (March
26, 1996)

Amended Complaint (April 15, 1996)

NSI Answer and Counterclaim for Declaratory Relief (April
25, 1996)

Stipulated Order Dismissing Preliminary Injunction as
Moot (May 21, 1996)

Memorandum of Points and Authorities in Support of
Defendant's Motion for Summary Judgment (June 3, 1996)
Defendant's Motion for Summary Judgment (June 14,
1996)

Roadrunner Computer Systems, Inc. v. Network Solutions,
Inc. (June 21, 1996)

9.1.2 DCI.COM: No Executive Privilege

Data Concepts, Inc. v. Digital Consulting, Inc. and Network
Solutions, Inc. - Complaint (May 8, 1996)

Report and Recommendation (January 31, 1997)

9.1.3 TY.COM: Reverse Name Hijacking

Philip L. Giacalone v. Network Solutions, Inc. and Ty, Inc. -
Complaint for Declaratory Judgment (May 30, 1996)

Order for Preliminary Injunction (June 13, 1996)

9.1.4 CLUE.COM: Mismatched Opponents

Clue Computing, Inc. v. Network Solutions, Inc. -
Complaint (June 12, 1996)

Motion for Temporary Restraining Order and Preliminary
Injunction (June 12, 1996)

Complaint for Interpleader (June 21, 1996)

Brief Amicus Curiae in Support of Motion to Dismiss (July
22, 1996)

Motion to Dismiss Interpleader Complaint (July 22, 1996)

Order of Dismissal (October 29, 1996)

Hasbro, Inc. v. Clue Computing, Inc. - Complaint (January
10, 1997)

Hasbro, Inc. v. Clue Computing - Memorandum and Order
(September 30, 1997)

9.1.5 DISC.COM: Choice Initials

Dynamic Information Systems Corp. v. Network Solutions,

- In. - Docket. (filed June 24, 1996)
- 9.1.6 REGIS.COM: The Usual Suspects
Regis McKenna, Inc. v. Regis Corp. - Docket (filed July 9, 1996)
- 9.1.7 JUNO.COM: Half a Million Accounts
Juno Online Services v. Juno Lighting, Inc. - Memorandum Opinion and Order (September 29, 1997)
- 9.1.8 PIKE.COM: Double Jeopardy
Peter Pike v. Network Solutions, Inc. and Floyd S. Pike Electrical Contractor, Inc. - Complaint (November 25, 1996)
FSPEC Answer, Affirmative Defenses and Counterclaims (February 13, 1997)
- 9.1.9 The Tunisian Gambit
- 9.1.10 REALWORLD.COM: Ex-Parte Decisions
Database Consultants, Inc. v. Network Solutions, Inc. - Complaint (March 18, 1997)
Stipulation of Dismissal (April 23, 1997)
- 9.2 Trademark Owners vs. NSI
- 9.2.1 KNOWLEDGENET.COM: Ghosts of Domains Past
Knowledgenet, Inc. v. David L. Boone, NSI, Inc. and Digital Express Group - Amended Complaint (December 12, 1994)
- 9.2.2 FRYS.COM: Default Judgment
Fry's Electronics v. Octave Systems, Inc. - Docket (filed July 12, 1995)
- 9.2.3 PRESTONE.COM: Speedy Resolution
Prestone Products Corp. v. Maynerd Collision & Autobody, Inc. - Docket (March 5, 1996)
- 9.2.4 PANAVISION.COM: Targeting California
Panavision Intl., L.P. v. Dennis Toeppen, et. al. - Order Denying Defendant's Motion to Quash (September 19, 1996)
Order Granting and Denying in Part Plaintiff's Motion for Summary Judgment (November 5, 1996)
Order Granting NSI's Motion to Dismiss (November 27, 1996)
- 9.2.5 MIKASA.COM: Sports and Saucers
American Commercial, Inc. v. Sports & Leisure Intl, Inc. (filed July 25, 1996)
- 9.2.6 PORSCHE.COM: Car Cachét
Porsche Cars North America, Inc. v. Chen (filed July 26, 1996)
- 9.2.7 EMPRESSTRAVEL.COM: Franchisee Face-Off
Empress Travel and Travel Impressions, Ltd. v. Stephen Kaufman, Traveler's Choice Inc. and Network Solutions, Inc. (May 22, 1997)
- 9.2.8 SKUNKWORKS.COM: A Stink About Tortfeasors
Lockheed Martin Corp. v. Network Solutions, Inc. and Does 1-20 (October 22, 1996)
Order Denying Defendant's Motion to Partially Dismiss Plaintiff's Claims and Related Relief (March 19, 1997)
Order Granting Defendant's Motion for Summary

Judgment (November 17, 1997)
9.2.9 ACADEMYAWARD.COM: Goodwill in Achievements
Academy of Motion Picture Arts and Sciences v. Network
Solutions, Inc. and Does 1-50 (filed August 26, 1997)

Chapter 10. Bigfoot Letters and Brickbats

- 10.1 Trademark Muscle
- 10.2 Network Solutions' Clout
- 10.3 A Square Peg

Chapter 11. Squatters, Speculators, Cybergluttony and Ostrichmeat

- 11.1 Domain Resale
- 11.2 What's It Worth?
- 11.3 Squatters and Grabbers
- 11.4 Super Cybergluttony

Chapter 12. Gone CyBerserk

- 12.1 CyBerserk Award: Procter and Gamble
- 12.2 Cyberversosity
- 12.3 The CyberSaver: International Business Machines

Chapter 13. Alterweb -- A Parallel Universe

- 13.1 Rough Consensus and Running Code
- 13.2 Resolving Alternate TLDs
- 13.3 AlterNIC, an Experimental Registry
- 13.4 The Republic of IAHC
 - 13.4.1 Memorandum of Understanding on the Generic Top Level Domains
 - 13.4.2 What is the gTLD-MoU?
 - 13.4.3 What is the Intent of the gTLD-MoU
 - 13.4.4 How Can We Participate?
 - 13.4.5 A Self-Regulatory Framework
 - 13.4.6 Seven New gTLDs
 - 13.4.7 Globally Distributed Competitive Registrars
 - 13.4.8 Signatories to the gTLD-MoU
 - 13.4.9 Criticism of the gTLD-MoU
- 13.5 Other Open Market Models
 - 13.5.1 eDNS -- Enhanced Domain Name System
 - 13.5.2 uDNS -- Universal Domain Name System
 - 13.5.3 Image Online Design : Rival Registry Sues IANA
 - 13.5.4 PG Media v. NSI: No Borders
 - 13.5.5 Root Server Confederations
- 13.6 Examples of Root and Name Server Files (June 1997)
 - 13.6.1 Alternate Top-Level Name Servers
 - 13.6.2 Why the Concern Over Alternate Top-Level Domain Names (TLDs)?
 - 13.6.3 db_root.bin -- Alternic
 - 13.6.4 db_cache.bin -- AlterNIC
 - 13.6.5 udns.cache -- uDNS
 - 13.6.6 udns.zone -- uDNS
- 13.7 How to Do "Alternate" DNS

Chapter 14. The Coming of Age of the Internet

14.1 The Future of the DNS: Governance and Administration

14.1.1 Internet Principles

14.2 Stability in the Presence of Chaos: Overview of the Issues

14.2.1 Governance: Who Should Own and Manage the ". "?

14.2.2 Structure: TLD Expansion or Nationalization?

14.2.3 Legal Aspects: The Trademark-cum-Domain Name Dilemma

14.2.4 Internet Use: A Directory for DNS?

14.3 The Future of the DNS: Proposals and Initiatives

14.4 DNS for the Toasternet Society

14.4.1 Introduction

14.4.2 Toasternet Definitions and Examples

14.4.3 Toasternet Humor

Chapter 15. DOMAINHANDBOOK.COM: Domain Diaries and Updates

Glossary

Index

TOP ↑

TABLES | FIGURES | CD-ROM

[Special Features](#) | [News](#) | [Order](#) | [Glossary](#) | [Opinions](#) | [Acknowledgments](#) | [Contacts](#)

The Domain Name Handbook: High Stakes and Strategies in Cyberspace
Copyright© 1998 Ellen Rony and Peter Rony. All Rights Reserved.

<http://www.domainhandbook.com/toc.html>

Website hosted by [Bullfrog Communications, Inc](#)

Designed and maintained by Ellen Rony, Alexander Works - Tiburon, CA



Trademark Examination of Domain Names

Internet domain names have generated a number of questions that directly pertain to trademark law. For the Patent and Trademark Office (PTO), the question most commonly faced is whether a term which is a domain name can also be registered as a trademark.

The quick answer is that an Internet domain name that is used to identify and distinguish the goods and/or services of one person, from the goods and/or services of others, and to indicate the source of the goods and/or services may be registered as a trademark in the PTO. See 15 U.S.C. § 1127. Trademark applications for Internet domain names usually seek registration of service marks. Lately, the PTO has received an increasing number of applications to register Internet domain names.

In order to register an Internet domain name, an applicant must show that it offers services via the Internet. Further, specimens submitted in support of the application to show use of the mark must show use of the Internet domain name as a source identifier. The use of an Internet domain name as a mere directional reference, similar to use of a telephone number or business address on stationery, business cards, or advertisements, is not use of the name as a source identifier. See *In re Advertising & Marketing Development, Inc.*, 821 F.2d 614, 620, 2 USPQ2d 2010, 2014 (Fed. Cir. 1987) ("It is not enough for the applicant to be a provider of services; the applicant also must have used the mark to identify the named services for which registration is sought"). Also, providing "a service which is normally 'expected or routine' in connection with the sale of one's own goods is not a registrable service." *In re Dr Pepper Co.*, 836 F.2d 508, 509, 5 USPQ2d 1207, 1208 (Fed. Cir. 1987). By analogy with the registration of trade names, the more distinctive the presentation of the Internet domain name and the further it is physically removed from other informational data appearing on the specimen, the more likely the name will be perceived to function as a service mark. See *In re Antenna Specialists Co.*, 408 F.2d 1052, 161 USPQ 284 (CCPA 1969).

Recently, the PTO has clarified how it administratively classifies services associated with the World Wide Web. "Identification and Classification of Certain Computer Related Goods and Services," <http://www.uspto.gov/web/offices/tac/domain/domcl.html>.

The PTO uses the phrases "connection" provider, "access" provider, and "content" provider to differentiate and classify services rendered via the Internet. An entity providing the technical connection needed for communication is a "connection" provider--a service classified in Class 38 (Telecommunications). The closely-related service rendered by entities such as America Online®, CompuServe®, or Prodigy® is an "access" provider--a service classified in Class 42 (Computer Service). An "access" provider furnishes "multiple-user access to a global computer information network."

Most applicants will be "content" providers who furnish information via the Internet, i.e., offer the service of providing information. In such cases, the service offered is an information service classifiable according to the information provided, e.g., a service that offers business information is classified in Class 35, a service that offers financial information is classified in Class 36, and a service that offers building construction, repair or maintenance information is classified in Class 37.

However, all "content" providers do not offer registerable services vis-a-vis an Internet domain name. For example, Internet domain name locations that simply contain advertisements or other information normally expected or routine in promoting an entity's goods or services are not registerable services.

Therefore, Internet domain names must meet the same requirements for registration as all trademarks and service marks. 15 U.S.C. § 1051 et seq. If a domain name does meet these requirements, it will be registered.

RETURN TO THE USPTO HOME PAGE

Please Send Comments and Suggestions Regarding this Web Server to www@pioneer.uspto.gov

Last Modified: 16 January 1998

IDENTIFICATION AND CLASSIFICATION OF CERTAIN COMPUTER RELATED GOODS AND SERVICES

Class 9:

Pre-recorded software on CD-ROMs, diskettes, magnetic tapes, etc. is in Class 9. The description must provide an indication of the subject matter or function of the software and the subject matter or function indication must be detailed and specific. Very broad statements of function such as "computer programs for business use" are not acceptable.

Class 9:

"Computer software [specify the function of the programs, e.g., for use in data base management, for use as a spreadsheet, for word processing, etc.] that is downloaded from a remote computer site" is classified in Class 9.*

* NOTE: This is a change in classification policy. Previously, "downloadable computer software" was being classified in International Class 42. After a review of this policy, the PTO has decided to classify downloadable software in Class 9 with other software. The placement of downloadable software in International Class 9 is consistent with the practice in a number of other countries.

Class 16:

Only hard copy publications, e.g., printed magazines and books, are considered to be Class 16 goods.*

* NOTE: Magazines or books that are downloadable from a computer network are not considered to be "hard goods" and they are classified in International Class 42 rather than Class 16. The service is defined as providing the publications on a global computer network and the subject matter of the publications must be specified. If an entire magazine or other publication is presented at a web site, the computer service of providing that publication electronically is considered to be the primary service involved in this activity. The service being provided is that of making available magazines, books and/or other publications via a computer. Appropriate language for these services would be: "Computer services, namely, providing on-line [indicate specific nature of the publication] in the field of [indicate subject matter of the publication]" in Class 42. As with Class 16 publications, the

subject matter of the publication does not effect the classification of this service.

Classes 35, 36, 37, 39, 40 & 41:

Any activity consisting of a service that ordinarily falls in these classes (e.g. computer games, various financial transactions, etc.) that also happens to be provided by means of a global computer network, is classified in the class where the underlying service is classified. For example, banking services are in Class 36 whether provided in a bank or on-line by means of a global computer network. Similarly, the service of providing information by means of a global computer network is classified in the class of the information subject. Entities who offer these services by computer are considered "content providers," that is, they provide the information or substantive content for a web site and/or home page. A recitation of services for these specific content providers should read "providing information in the field of . . . by means of a global computer network". The service would be classified by the class of the subject matter of the information. If an entity provides information in a wide variety of fields, this must be reflected in the identification and the service may be classified in Class 42 (e.g., providing information in a wide variety of fields by means of a global computer information network.) Please note that the term "access" should be reserved for use in recitations for network service providers, such as, America OnLine®, Prodigy® and CompuServe®. The PTO considers the use of the term "access" by a content provider to be inaccurate because it causes confusion with the service provider activities.

These guidelines also apply to activities in Classes 38 and 42, however, the comments below also apply to Classes 38 and 42.

Class 38:

The service of providing telecommunications connections to a global computer network is classified in Class 38. These services are purely telecommunications "connections" such as those provided by AT&T®, MCI® or other telecommunications providers. It is ONLY the technical means by which one computer can communicate with another. The telecommunications provider does NOT provide the computer hardware that stores and processes the data; it provides the means by which data is transferred. This service connects the user to the "link provider" (see Class 42 discussion below) or the web site itself.

Class 42:

The service of providing multiple-user access to a global computer information network for the transfer and dissemination of a wide range of information is classified in International Class 42.

This language covers those services provided by entities such as America OnLine®, Prodigy® and CompuServe®. They provide the computer service (often using the telecommunications services of other entities as described above in Class 38) that enable computer users to access data bases and home pages of others. These entities are considered "link providers" in that they provide the computer/server connection required for computer users to access a content provider. The word

"access" should be limited to these services and should not be used in describing the service of a content provider.

NOTE: A single entity may provide one or more of the services described above. However, each service must be properly identified and classified.

General comment:

The term "Internet" is still the subject of a proceeding at the Trademark Trial and Appeal Board. Therefore, this term should not be used in identifying any goods or services connected with a global computer information network. Language such as "global computer information network" or a substantive equivalent should be used instead of the term "Internet."

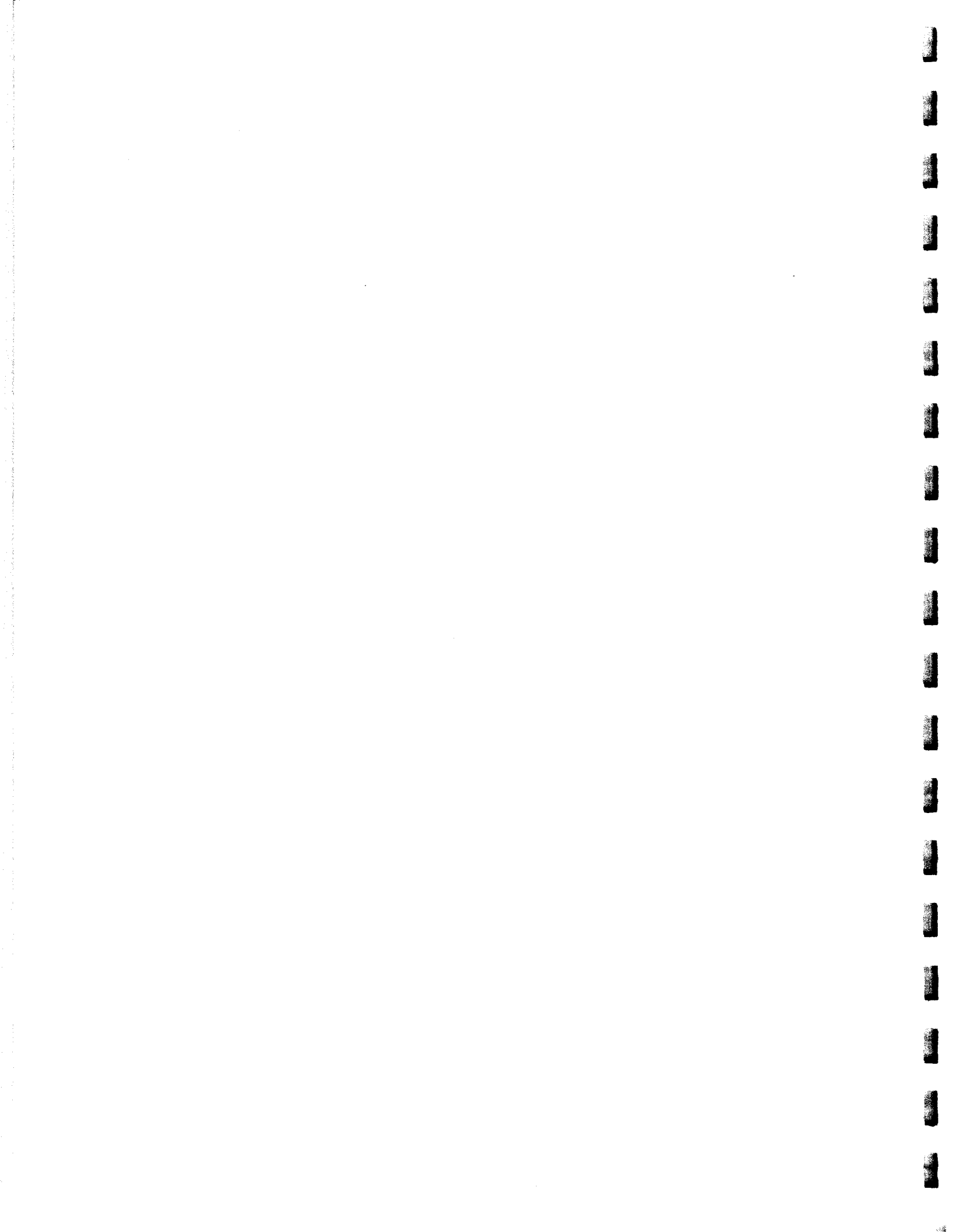


**TAX ISSUES ARISING OUT OF E-COMMERCE
AND OTHER RELATED ISSUES**

Bill E. Webb
Director of Electronic Commerce (Ohio Valley Region)
Ernst & Young
Cincinnati, Ohio

Copyright 1999, Bill E. Webb. All Rights Reserved.

SECTION G



Electronic Commerce Tax Issues

Bill Webb
Area Electronic Commerce
Service Line Leader

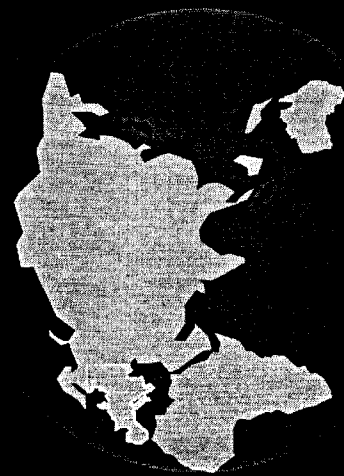
eCommerce & Tax: Implications/Opportunities

- Tax Implications of eCommerce
 - Removal of physical barriers
 - Tax rules developed prior to advent of eCommerce
 - Historical transaction tax collection methods do not work with eCommerce
 - Alternatives present unrealistic burdens for businesses
 - Transaction tax costs can eliminate profits



◆ Opportunities

- Alignment of Tax and eCommerce strategies
- Tax planning creates competitive advantage
- Trading companies easier to implement through eCommerce
- eCommerce coalition (Internet Tax Freedom Act Advisory Commission)



Tax eC Issues and Related

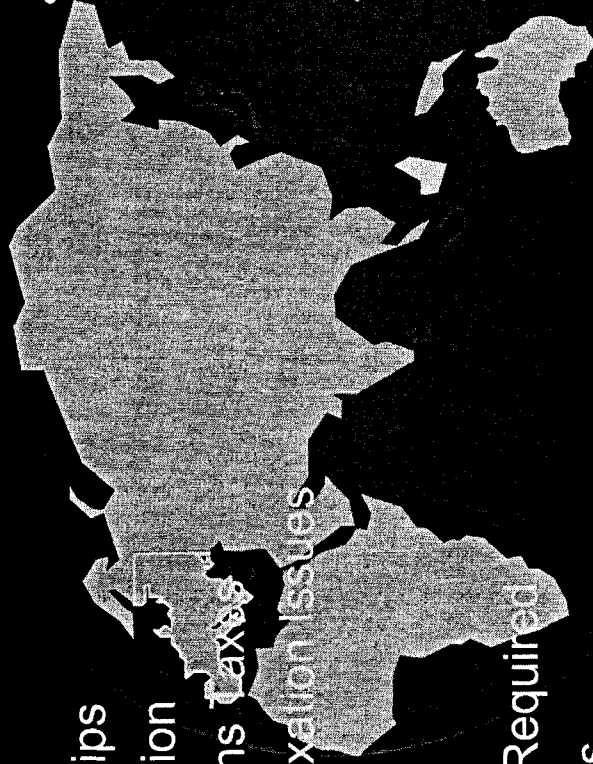
Services/Solutions

ISSUES

- Taxability - if, who, where
- Server Site Location
- Information Services-Special Rules
- Agency Relationships
- Electronic Distribution
- Telecommunications Taxes
- Entrepreneurial Taxation Issues
- Physical Records Required
- Billing/Tax Systems Compatibility
- Electronic Invoicing Requirements
- Outsourcing Implications
- Automation of internal functions

IONS

- Nexus (Taxability) Studies
- Tax Incentives
- Tax Planning
 - Transaction (Sales/VAT)
 - International, SALT, M&A
 - Excise
- Personal Financial Planning
- Accounting Methods
- Records Retention Agreements
 - Systems Design & Implementation
 - Outsourcing



Internet Tax Provisions

Federal:

Internet Tax Freedom Act

- Enacted October 21, 1998
- Bars State & Local Governments from imposing
 - (1) Taxes on internet access, unless such tax was generally imposed and actually enforced prior to October 1, 1998; and
 - (2) Multiple or discriminatory taxes on electronic commerce
- Moratorium runs from October 1, 1998 - October 21, 2001

Internet Tax Provisions

State & Local Taxes:

- Methods of Taxation
 - Income/Franchise Taxes
 - Sales & Use Taxes
 - Property Taxes
- Issues/Prohibitions Associated with Internet Taxation
 - Internet Tax Freedom Act
 - U.S. Constitution
 - Due Process Clause - Minimum connection (nexus) with taxing state.
 - Commerce Clause - Physical presence with taxing state.
Bars discrimination of interstate commerce.
 - State Constitutions

Internet Tax Provisions

- Kentucky
 - No specific tax provisions applicable to internet services.
- Indiana
 - No specific tax provisions applicable to internet services.
- Ohio
 - Imposes sales and use tax on automatic data processing and computer services provided for use in a business. R.C. 5739.01(B)(3).
- Tennessee
 - Imposes sales and use tax on internet access and e-mail service when telecommunications service originates or is received in TN and is provided to a location within TN or billed to a TN address.



**RECENT DEVELOPMENTS AND EMERGING ISSUES
IN ON-LINE SALES AND LICENSING**

*Open, Click Or Download:
What Have You Agreed To? The Possibilities Seem Endless*

Stephen J. Davidson
Scott J. Bergs
Leonard, Street and Deinard, P.A.
Minneapolis, Minnesota

Copyright 1999, Stephen J. Davidson and Scott J. Bergs. All Rights Reserved.

SECTION H

**RECENT DEVELOPMENTS AND EMERGING ISSUES
IN ON-LINE SALES AND LICENSING**

TABLE OF CONTENTS

I. INTRODUCTION	H-1
II. PROTECTIONS IMPLICIT IN ON-LINE WORKS	H-1
A. Copyright	H-1
1. Necessary computer copies	H-5
2. First sale	H-5
3. Fair use	H-5
4. Digital Millennium Copyright Act of 1998	H-7
B. Other Protections	H-8
III. EXPANDING PROTECTION OF ON-LINE WORKS BY CONTRACT	H-10
A. Shrink-Wrap Licenses	H-10
B. Click-Wrap Licenses	H-13
IV. PRACTICAL PROBLEMS CREATED BY ON-LINE LICENSE	
AGREEMENTS AND NOTICES	H-14
A. Notice Of The Existence Of License Terms	H-14
B. Layered And Embedded Notices And Agreements	H-15
C. Contract Terms Transferred From Physical To Electronic Licenses	H-17
V. CONCLUSION	H-17
VI. ENDNOTES	H-18



INTRODUCTION

The Internet provides a seemingly limitless target audience for those who post information and/or conduct business online. Reaching this expansive prospect base while maintaining control over online products and business risks, however, creates challenges not always apparent to unsophisticated entrants into the online arena. While posting material on the Internet may not make it fair game for anyone to simply download and use as they wish, the scope of intellectual property protection available for online offerings, and the potential liability of their offerors is very unclear.

This article does not purport to address all of the commercial implications of online enterprise, but rather merely serves to illuminate some of the emerging issues and, hopefully, stimulate thought about others. Because intellectual property rights (and copyright, trade secret and trademark rights, in particular) are among the most common concerns, this article will focus on that. In the text to follow, the authors will review some of the primary protections available for online works and their respective limitations, review how the courts have addressed various approaches to contract formation, and anticipate some of the legal issues that may be confronted as the number and manner of online informational and business transactions increase.

PROTECTIONS IMPLICIT IN ONLINE WORKS

Copyright

Online works, like any work, will be afforded some protection automatically upon being created. The Federal Copyright Act, 17 U.S.C. et seq., protects "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.”¹ Therefore, to be covered by the act, a work must be (1) an original work of authorship, and (2) fixed in a tangible medium. Online works can, and routinely do, meet these criteria.

To be an “original work of authorship,” an item must be composed of some original expression beyond basic ideas, procedures, processes, systems, etc.² Here the analysis is the same for online as for traditional works; to the extent that the information being posted online has some creativity and is not just a basic idea, the creative expression is potentially protectible.³

A work is “fixed in a tangible medium” under the Copyright Act “when its embodiment in a copy . . . is sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than a transitory duration.”⁴ Works stored on a disk or a hard drive have been consistently held to be sufficiently fixed and thereby covered by the Copyright Act.⁵ In order to be posted on a Web site or other media on the Internet, information must be saved in the host computer’s memory. When this happens, the information is sufficiently “fixed” to be protected under the Copyright Act.⁶

The Copyright Act only provides protection for the “owner” of a copyright.⁷ Ownership of a copyright “vests initially in the author or authors” but “may be transferred in whole or in part by any means of conveyance or by operation of law.”⁸ The owner has the exclusive right to exercise or license all of the rights granted by the Act.⁹ These rights include the right to: (1) reproduce the work, (2) make derivative works, (3) distribute copies of the work, and (4) display the work publicly.¹⁰

A violation of these rights constitutes infringement, actionable by the owner. In the context of online materials, however, what constitutes a violation of these rights is far from

clear. The most basic example is browsing. When a copyrighted work is posted on a Web site by the owner, presumably the owner wants the work to be downloaded by end users. This desirable downloading, however, may constitute a violation of the owner's exclusive rights, the right to reproduction, right to display the work publicly, and others.

The right to reproduction may be violated several times during the downloading of a work.¹¹ Perhaps the area of greatest concern is the information residing in the RAM¹² of the computer downloading the information. The question of whether information stored in RAM is "fixed" for Copyright purposes, has been addressed by the courts on several occasions yielding varying determinations.¹³ The majority view of those courts having considered the question appears to be that absent some other consideration, the storage of complete files representing copyrighted works in the RAM of the computer downloading does constitute a "fixation" and thus an illegal copying of the work if not authorized by the copyright owner.¹⁴ This often does not result in a liability for infringement, however, because of the doctrines of fair use and implied license. In fact, it appears obvious that the mere act of downloading a file posted on a Web site should not expose the user to liability. Presumably, the only reason to post information is to enable other people to download it.

An implied license is merely a recognition by the court that, absent a written license agreement required to transfer the interest of a copyright owner under the Copyright Act, certain conduct by the copyright owner should bar it from suing another for copyright infringement. An implied license is created where (1) a person requests the creation of a work, (2) the creator makes and delivers the work requested, and (3) the licensor/creator intends that the licensee/requester will copy and/or distribute the work.¹⁵

An online transaction could easily satisfy these elements. For example, the browsing user makes a request, by entering a search query or linking to the URL of a Web site. The host party then provides access to the copyrighted work and allows it to be downloaded. In this context, it would be difficult to argue that the copyright owner, who placed the information online, did not intend for the user to copy the work, at least to their RAM or that of their Internet service provider ("ISP").

The ambiguity arises when considering the scope of the implied license.¹⁶ Does an online implied license allow unlimited non-commercial copying? How about distributing or selling copies? The answers to these questions will be very fact specific and perhaps inconsistent as the courts begin to evaluate these transactions.

Additional difficulties arise where the party posting the copyrighted work is not the owner, but instead, a third-party who lacks authorization from the copyright owner. In this context, the party posting the work has likely infringed the copyright, but what about the party who downloads it? Because intent is not required to establish copyright infringement,¹⁷ these parties may technically be infringing the copyright as well.

Browsing may also violate reproduction rights when the user's computer caches¹⁸ the downloaded file. This process creates a copy of the work that remains stored or "fixed" for an indefinite period of time. Thus, similar to RAM storage, this arguably violates the rights of the copyright owner.

Not all apparent violations of the copyright owner's exclusive rights create liability for infringement. The Copyright Act expressly limits the owner's exclusive rights in several ways.¹⁹ The limitations contained in sections 117, 109 and 107 of the Act are especially applicable to online works.

Necessary Computer Copies

Section 117 provides that the owner of a copy of a computer software program may make another copy without infringing so long as the additional copy is either essential to the utilization of the program or is for archival purposes only.²⁰ This exception raises some interesting questions in the online context. Who is an owner? When someone downloads software legally posted on the Internet, without paying for it, do they own a copy of it? If not, then arguably, the first copy they make to their hard drive infringes the copyright and is not excepted by § 117. Certainly, a downloaded file must be “copied” into RAM to be viewed; but is a hard drive or floppy disk copy “essential” to the utilization of the program?

First Sale

The first sale doctrine of § 109 of the Copyright Act, 17 U.S.C. § 109, cuts off the distribution rights as to a specific copy of a work upon the first sale of that copy. The buyer may sell or otherwise distribute that copy so long as they do not retain any duplicate, for example, on their hard drive. If, however, the transmission of software over the Internet is not a “sale” then does the “buyer” have the right to sell or give the copy away?²¹

Fair Use

Section 107 of the Act provides that no infringement occurs where the use alleged is a “fair use . . . for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research.”²² The Act outlines four non-exclusive factors to be considered in the determination of whether a particular act constitutes fair

use: (1) the commercial vs. nonprofit use of the work, (2) the nature of the copyrighted work itself, (3) the substantiality of the portion used compared to the work as a whole, and (4) the effect the use has on the market for the copyrighted work.²³ This fourth factor is frequently cited as being the most important.²⁴

There is authority for the proposition that when one violates one of the copyright owner's exclusive rights but it has no negative effect on the market for the work, no liability exists.²⁵ Where, however, the infringing work diminishes the existing or expected market of the copyrighted work, the tendency is to treat the use as not a "fair use."²⁶ While these principles appear well settled at the extreme ends of the spectrum, it is unclear what happens to those activities in the middle of this spectrum. The court decisions are very fact specific and divided.

For example, in Playboy Enterprises, Inc. v. Frena, the defendant operated a BBS where paid subscribers posted erotic pictures.²⁷ When pictures taken from the plaintiff's magazine were posted and downloaded, the plaintiff sued the BBS operator for copyright infringement. The court found that the defendant's action constituted infringement and was not fair use because the defendant solicited the postings, and they resulted in damage to the plaintiff's market for its magazine.²⁸

The court in Religious Tech. Ctr. v. Netcom On-line Commun. Svc., Inc. denied summary judgment, holding that a genuine issue of fact existed as to the defendant BBS operator's fair use of the infringing material because the effect of the infringing material on the market was unclear.²⁹ The court suggested, however, that the use was fair in part because, even though the defendant gained financially from the operation of the BBS, it received "no direct financial benefit from the acts of infringement."³⁰ The court differentiated the case from

Playboy by emphasizing that unlike the defendant in Playboy, Netcom did not directly benefit from the infringing materials because it did not solicit the posting of infringing works but instead merely acted as a conduit.³¹

The Netcom court's attempt to differentiate its facts from those in Playboy evidences the ambiguity in this area of the law. The factual differences highlighted by the court are tenuous at best. Contrary to the court's suggestion in Netcom, the Playboy court did not base its holding on the direct relationship between the defendant's solicitation of infringing works and the financial gain by the defendant. In fact, the court made no mention of such a specific solicitation. The Playboy defendant did not even appear to know that any of the material was infringing. Yet, the court stated that "[i]t does not matter that Defendant . . . may have been unaware of the copyright infringement. Intent to infringe is not needed . . ." ³² The divergent holdings in these two cases evidenced the need for further clarity in this area.

Digital Millennium Copyright Act Of 1998

Congress attempted to clear some of the ambiguity surrounding copyright in the realm of the Internet by passing the Digital Millennium Copyright Act of 1998, Pub. L. No. 105-304, 112 Stat. 2860 (Oct. 28, 1998). This statute expressly limits infringement liability for ISPs³³ for "copying" by storing information in the RAM of their servers during online transmissions, among other things. Therefore, the Ninth Circuit's holding in Mai Systems, Inc. v. Peak Communications appears to be overruled on that point. This protection is only available if an ISP does not modify the content of the information requested by the user, adopts a policy to drop users who transmit infringing works, does not control what or to whom the information goes, and only stores the information for a reasonable time.³⁴

The Act also protects ISPs from liability due to caching. Again, this protection is only available if certain steps are taken. An ISP must not modify the content of the information, must not interfere with the posting party's "hit" tracking technology, must limit users access according to the posting party's password or other security requirements, and must remove any unauthorized material promptly when notified.³⁵ The act does not address caching at the user level.

Finally, the Act protects ISPs from infringement liability for materials posted on the ISPs Web site by a user. To qualify for protection, the ISP must not know that infringing material resides in its site, must not directly financially benefit from the infringing activity, and must take the information down promptly upon notification of infringement. This appears to codify the Netcom holding, however, no definition of "directly financially benefit" is provided in the Act. The controversy between the Playboy and Netcom decisions, therefore, may not be effectively resolved by the Act.

While the statute may provide some protection for ISPs, its does not clarify the protection afforded to the copyright owner against infringement by parties other than an ISP. The Act also fails to define copying. Therefore, other than the specific exceptions outlined for ISPs, any "copies" made by online users may be infringing.

Other Protections

In addition to copyright, online information may also be protected by the trademark and trade secret laws.³⁶ The scope of these protections for online materials is no more clear than that afforded by copyright. Trademark law, like copyright law, does not require a showing of intent to establish infringement, but generally does require a showing that the specific allegedly

infringing use is likely to cause confusion as to the source or quality of the goods or services.³⁷ Therefore, a user probably does not infringe a legally posted trademark just by downloading to browse. If the user, however, uploaded and posted the mark somewhere else, infringement may occur if the use of the mark could confuse the public about who the mark belongs to. A few cases have dealt with this issue in the context of linking and framing; however, none have reached final judgment.³⁸

Linking allows a user to go directly from one Web site to another, unrelated site simply by clicking on a "link" provided by the original site. Conversely, in framing, part of the material created by the original site remain on the user's screen while material from a separate site is displayed within the image generated by the original site. With either practice, the second site being accessed is often an interior page of a Web site that does not contain identifying marks. As a result, the goods or services of the trademark owner may appear to belong to the operator of the Web site using framing or initiating the link, thus causing the likelihood for consumer confusion or dilution of the trademark.³⁹

The scope of protection afforded by trade secret law or specifically the Economic Espionage Act, 18 U.S.C. § 1831 et seq., is likewise uncertain. Very few cases have been brought under the Act, and traditional state trade secret law has not often been raised in the context of online materials. One court, however, considered the effect of posting trade secret information on a Web site. The court stated that if the information posted were specific enough, it would destroy the protection otherwise afforded this information because it is no longer secret.⁴⁰ As more information is transmitted online, various questions about trade secret protection arise. How secure must an Internet connection be to adequately protect the secret

nature of information being transmitted? What actions by a defendant will constitute the unlawful acquisition of such secret information if it is being transmitted online?

Certainly, some protections are available for online materials. The present and future scope of these protections is, however, quite unclear.

EXPANDING PROTECTION OF ONLINE WORKS BY CONTRACT

Shrink-Wrap Licenses

Software developers and publishers have long sought to expand the implicit protections afforded to software programs by imposing additional terms on end users by contract, usually in the form of a license agreement. In the mass market context, these license agreements came to be known as "shrink-wrap" licenses because they initially were included on the outside of the software package under a layer of shrink-wrap plastic. Until recently, those few cases examined the enforceability of shrink wrap licenses resulted in holding them invalid on contract formation grounds.⁴¹ Arguably, the holdings in those cases relieved purchasers of any duty to affirmatively search for and read the license terms and elect either to object or be bound by them. The tide turned markedly in favor of software producers, however, when the Seventh Circuit in ProCD v. Zeidenberg upheld the enforceability of such bundled "contracts."⁴²

In ProCD, the court held that the shrink-wrap agreement enclosed in the software package were assented to and therefore were enforceable.⁴³ Judge Easterbrook writing for the court, justified the decision on two grounds and two provisions of the UCC. First, he stated that the seller or licensor in a transaction has the power to condition acceptance on certain conduct by the buyer. He found that ProCD had done that by including a provision in the license agreement

that stated that using the software constituted acceptance of the terms.⁴⁴ The second UCC provision cited in support of the court's holding was 2-606. This section states that "[a] buyer accepts goods . . . when, after an opportunity to inspect, he fails to make an effective rejection."⁴⁵ The court reasoned that the defendant had an opportunity to review the license, was aware of the contract terms and failed to object, thereby accepting the them.

The court's decision appeared to be conditioned on the explicit notice of the contract terms provided to the buyer.⁴⁶ However, in Hill v. Gateway 2000, a subsequent case before the Seventh Circuit, Judge Easterbrook again upheld a bundled contract despite the complete lack of notice on the outside of the package or on the user's screen during operation.⁴⁷ However, in Gateway, the court did note that the buyer knew when ordering the product by phone that some sort of contract likely would be included in the transaction. The court reasoned that because of this knowledge, the buyer could be bound by any terms not expressly rejected.⁴⁸

The Ninth Circuit appears to have followed that lead in Micro Star v. Formgen, Inc.⁴⁹ In Micro Star, the Ninth Circuit reversed the district court and held that an injunction against the defendant's sale of its game software was appropriate because the software was a derivative work that violated plaintiff's copyright.⁵⁰ The plaintiff had created a computer game that allowed and encouraged users to create new advanced levels of the game and to post them on the Internet so others could use them. The defendant downloaded and copied these new, user-made versions to CDs and resold them. The court distinguished the user's lawful use from the illegal use by the defendant, stating that the users were granted a written license while the defendant was not.⁵¹ The defendant argued that the user's written license was invalid, but that plaintiffs granted an implied license when they encouraged the creation of the derivative works. The defendant

further argued that this implied license extinguished plaintiff's rights to the user made derivative works.

The court rejected this argument, stating that users were prohibited by the license agreement from selling the user-made versions and that this prohibition evidenced the plaintiff's intent to preserve its exclusive right to commercially distribute these works. The court did not mention what, if any, notice of these license terms was given to the users. The defendant, who received no actual notice, was held bound by the restrictive terms.⁵² In other words, the defendant did exactly what the plaintiff hoped online users would do; it downloaded the authorized derivative works made by the users. In so doing, it had no notice of any restrictions placed on this authorized and encouraged behavior. Yet, the court enforced rights against the defendant based on the unknown contractual restriction.⁵³ These cases suggest that the burden may now be on the buyer/user to seek out the terms on which digital products are offered or risk being bound by default, at least to the extent of terms that are not unconscionable or otherwise illegal.⁵⁴

The doctrine of unconscionability is designed to avoid oppression or unfair surprise. Therefore, to the extent that license agreements contain one sided terms, they may be held entirely or partially unenforceable. Traditional concepts of unconscionability will likely be helpful in determining what is oppressive in online contracts. These historical concepts may, however, be less helpful in determining what creates unfair surprise online. An unsuspecting buyer may be more likely to be lured into a contract online without knowing what terms are included in a hyperlink set of terms and conditions than if the same terms were contained on the face of a box or even on a piece of paper in the box. These conceptual differences between

tangible shrink-wrap licenses and online "click-wrap" licenses have not, to date, prevented the latter from being enforced.

Click-Wrap Licenses

While no court has directly addressed the enforceability of click-wrap agreements, at least two cases suggest that such agreements will be enforced.⁵⁵ In Compuserv, Inc. v. Patterson, the court held that by typing "agree" on an online registration form, the defendant had agreed to be bound by the terms of the shareware license that was displayed on the screen. The formation of the contract, however, was not the primary issue in the case. Instead, the court stated that a contract had been formed in the context of a discussion of whether the defendant was subject to personal jurisdiction in Ohio, where the plaintiff's computer and operation resided.⁵⁶

In Hotmail Corp. v. Van\$ Money Pie, Inc., the court granted an injunction preventing the defendant, a user of the plaintiff's Internet e-mail product, from sending "spam"⁵⁷ messages. The defendant registered online and received several of the plaintiff's e-mail boxes. The terms of the online license agreement prohibited sending spam or obscene messages. The court granted the plaintiff's requested injunction, finding that the plaintiff was likely to prevail on its breach of contract claim because the defendant had agreed to abide by the terms of the agreement by using the e-mail boxes and had breached the contract by violating its terms.⁵⁸

According to these cases, click-wrap agreements, like shrink-wraps before them, appear to be enforceable even where notice of the terms is minimal. While the enforceability of such agreements may still be limited by the statute of frauds, unconscionability and other doctrines,

the application of these principles to online materials creates some unique problems even beyond the ambiguities present in shrink-wrap licenses.

PRACTICAL PROBLEMS CREATED BY ONLINE LICENSE AGREEMENTS AND NOTICES

Notice Of The Existence Of License Terms

As discussed above, the cases finding shrink-wrap and click-wrap agreements enforceable state or suggest that the defendant was (or should have been) aware that at least some form of contract would be involved in the transaction. This, however raises at least as many questions as it answers. For example, what type of notice (if any) is sufficient to inform a buyer/user what contract terms will apply?

ProCD printed a notice on the box, informing buyers that additional terms were contained inside. Is notice prior to purchase necessary? Gateway suggests not, but what happens if the buyer claims to have had no idea that any additional terms would be included? Moreover, what facts would justify such a contention by an online buyer? Could an online buyer claim that he/she had no notice of additional terms where the terms are identified only on an interior page of a Web site, accessed by an inconspicuous link located at the bottom of an initial Web page that requires scrolling in order to find it? What if the link to the notice is in extra small type? Even if these tiny "notices" are sufficient under the ProCD standard, do they constitute unfair surprise and thus become unconscionable? Do they meet the legal requirement that certain notices be "conspicuous" if the language of the deeply linked contract is conspicuous but the link to it is not?

If the trend (if it can be called a trend) toward enforcing all license agreements continues, then online software providers are likely to make notices smaller and less conspicuous to minimize the possibility that buyers will refuse to buy as a result of them. What will the courts do when the extreme becomes absurd and a notice is limited to a linked © or no notice whatsoever is provided?

Layered And Embedded Notices And Agreements

Unlike paper transactions, where anyone looking through the contents of a box has a reasonable chance of stumbling over bundled contract forms, where transaction terms are located in different places on a single Web site (or perhaps even linked to different sites), the reasonable buyer/user may not notice them or have reason to search them out. It is becoming common for Web pages to contain links to a sets of "terms and conditions," sometimes as inconspicuous as the highlighted word "documents" or "software" appearing at he bottom of the page. Is the buyer/user expected to know that these are in fact links to purported contract terms? Must they look for more than one? If there are links to multiple statements of terms, are they bound by all?

Where more than one set of contract terms or restrictions are present or accessible on a given site, the terms of multiple sets of terms often conflict with one another or at least create ambiguities. This may be the result of poor drafting or simply referencing incompatible provisions, sometimes contained in documents from different sources with different purposes or different interests at stake. When this occurs, which terms will be enforceable? The most restrictive? The least restrictive? Will the entire agreement be unenforceable?

What if one notice is listed on the first page viewed by a buyer but additional terms are listed on a page accessible only after "agreeing" to purchase? The battle of the forms analysis

under UCC § 2-207 may exclude such layered notices. Under the UCC analysis, additional terms offered by the accepting party are treated as offers in a consumer transaction. Where both parties are merchants, the terms are included in the agreement unless they materially alter the agreement.⁵⁹ In the context of online transactions, who is the offeror and who is the acceptor? Are terms in an "additional" copyright notice material to the agreement as a whole? How about restrictions on the use of trademarks or purported agreements not to challenge the enforceability of the agreement or restrictions on the buyer/licensee's ability to take specified actions unrelated to the transaction? Disclaimers of warranties are often included in copyright provisions on a web page. Does this placement provide adequate notice to the user? Are disclaimers material to the online agreement?⁶⁰

The UCC warranty disclaimer provisions may prove yet another source of contention between online sellers and buyers. Section 2-316 states that a seller may disclaim certain warranties, provided that the disclaimer is "conspicuous." The conspicuous requirement is typically met by using larger type, bold letters, and/ or all capital letters. In a tangible agreement, the use of distinguishing typeface justifiably fulfills the purpose of the UCC - *i.e.*, section, to give the buyer fair notice of this important disclaimer. In online agreements, however, disclaimers are often found on interior pages of a Web site that are only accessible through a link from the main page or perhaps even by multiple links through multiple pages or even multiple sites. These links are frequently small and/or located at the bottom of a long page of material requiring the buyer/user to scroll down to even see it and/or expressed in ways that do not necessarily suggest they lead to a contract at all. Are these linked disclaimers conspicuous? Do they truly fulfill the purpose of UCC § 2-316 to give the buyer/user notice of the disclaimer?

Contract Terms Transferred From Physical To Electronic Licenses

Another recent phenomenon that has caught the authors' attention is the surprisingly common occurrence of license or other contract terms that appear to have been ported from one context to another without much thought about whether they make sense in the new context. For example, the authors have seen provisions in online "click on" licenses purport to take effect upon opening the package. What package is opened in this context and when? How far will the courts be willing to go to interpret such language to render the "agreement" enforceable in an online transaction? Another example is a statement in the opening pages of printed books purporting to impose restrictions on the buyer, including prohibition of "decompilation of the contents." How is a tangible book decompiled? While the courts seem to be tempting license drafters to expand the scope of the license provisions, care must be taken to remain in the bounds of the possible, if not the fair and reasonable.

CONCLUSION

The digital revolution has arrived, and the evolution toward electronic commerce is growing at an exponential rate. As more products are offered and more goods sold online, the relative legal rights and obligations of the parties to such transactions will be called increasingly into question. Both the practices of online merchants and others who offer information or other material over the Internet, and the law that governs their rights and liabilities, needs to evolve just as quickly in ways that make practical sense. Recent decisions upholding the enforceability of bundled and electronic agreements portend broad enforcement of bundled or linked terms, at

least insofar as is necessary to reasonably protect intellectual property rights, but it is too early to tell how that will be balance against the courts' willingness to find such agreements unenforceable when necessary to protect the rights of injured consumers. Perhaps proposed new UCC Article 2B will provide more certainty. Perhaps we need to await more court decisions to illuminate the path to justice in the digital age. Perhaps both. In the meantime, however, the authors suggest that commercial parties in particular who venture into the online arena need to give more thought to how they will establish and define their legal relationships in enforceable ways.

ENDNOTES

¹ 17 U.S.C. § 102(a).

² See Feist Publications, Inc. v. Rural Telephone Service Co., 499 U.S. 340 (1991); 17 U.S.C. § 102(b).

³ See 1 M. Nimmer and D. Nimmer, Nimmer on Copyright, § 1:10[B][2] (describing the idea vs. expression dichotomy of protectible material under the Copyright Act and the Constitution of the United States) (herein after "Nimmer on Copyright").

⁴ 17 U.S.C. § 101.

⁵ See, e.g., Vault Corp. v. Quaid Software Ltd., 947 F.2d 255, 259 (5th Cir. 1988); Novell, Inc. v. Network Trade Center, Inc., 25 F. Supp.2d 1218, 1230 (D. Utah 1997).

⁶ Ordinarily, the work will be stored first on the author's computer or disk and then transferred to the Internet host computer. Therefore, the copyrightability is not first established at the host but upon first fixation by the author.

⁷ 17 U.S.C. § 106.

⁸ 17 U.S.C. § 201(a), (d).

⁹ 17 U.S.C. § 106.

¹⁰ 17 U.S.C. §106.

¹¹ See David L. Haynes, Advanced Copyright Issues On the Internet, in The School of Law, University of Southern California, Nineteenth Annual Computer Law Institute, p. 4 (May 28-29, 1998) (hereinafter "Haynes") (when a picture is downloaded from a Web site, at least seven copies of the information comprising the image are made in the process of delivering the image).

¹² RAM refers to Random Access Memory which stores data and instructions while a computer is being used and then is erased when the computer is turned off.

¹³ See Mai Systems Corp. v. Peak Computer, 991 F.2d 511 (9th Cir. 1993) (holding that information stored in RAM was "fixed" and thus constituted copyright infringement) but cf. Advanced Computer Services v. MAI Systems Corp., 845 F. Supp. 356 (E.D. Va. 1994) (information stored in RAM is "fixed" only if it is stored there for a significant period of time).

¹⁴ See Nimmer on Copyright, § 8.08[A][1].

¹⁵ See I.A.E., Inc. v. Shaver, 74 F.3d 768, 776 (7th Cir. 1996).

¹⁶ See, e.g., MacLean Assoc., Inc. v. Mercer-Meidinger-Hansen, Inc., 952 F.2d 769, 779 (3d Cir. 1991) (overturning the district courts directed verdict, reasoning that the creator of a software program designed to manage human resource activities, granted an implied license to the corporation for which he developed the software but that the corporation exceeded the scope of the license by redesigning the software to fit the needs of other customers and marketing the redesigned versions).

¹⁷ See Religious Technology Center v. Netcom On-line Commun. Svc., Inc., 907 F. Supp. 1361, 1367 (N.D. Cal. 1995) (holding that an Internet service provider ("ISP") and a bulletin board service operator ("BBS") were not liable for direct infringement where a third party posts infringing material that is saved on the servers of both the ISP and the BBS).

¹⁸ "Caching" refers to the common Internet practice of saving a copy of the downloaded information on the user's computer or a server, to save the time and available bandwidth used when the user returns to a file that has already been accessed. In this process, a "copy" is cached for a limited period of time that may be only seconds or, with modern browser software, until the user's online session is terminated. See Haynes at 60-61.

¹⁹ 17 U.S.C. §§ 107-121.

²⁰ 17 U.S.C. § 117.

²¹ See Haynes, at 94 (noting that it is unclear whether online transmissions of software constitute "sales" in the context of the "first sale doctrine" of 17 U.S.C. § 109).

²² 17 U.S.C. §107.

²³ See Religious Technology Center v. Netcom On-Line Commun. Svc., Inc., 907 F. Supp. 1361 (N.D. Cal. 1995).

²⁴ Netcom, 907 F. Supp. at 1378.

²⁵ See Lewis Galoob Toys, Inc. v. Nintendo of America, Inc., 964 F.2d 965, 971 (9th Cir. 1992) (holding that by creating and selling software that modifies the plaintiff's game, but only during a single user session, defendant's created a derivative work but the use was fair because the market for plaintiff's products was not diminished and perhaps enhanced).

²⁶ See Micro Star v. Formgen, Inc., 154 F.3d 1107, 1113 (9th Cir. 1998) (plaintiff that allowed users of its game software to legally modify and post the revised versions on the Internet, defeated a claim of fair use where the defendant collected the modified versions of the game from the Internet for repackaging and resale, because plaintiff intended to sell a similar product and the intended market was diminished by defendant's use).

²⁷ Playboy Enterprises, Inc. v. Frena, 839 F. Supp. 1552, 1554 (M.D. Fla. 1993).

²⁸ Playboy, 839 F. Supp. at 1558-59.

²⁹ See Netcom, 907 F. Supp. at 1381.

³⁰ Netcom, 907 F. Supp. at 1379.

³¹ Netcom, 907 F. Supp. at 1379.

³² Playboy, 839 F. Supp. at 1559.

³³ The Act defines OSP or service provider broadly to include any "entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received." 17 U.S.C. 512(k)(1).

³⁴ 17 U.S.C. § 512(a).

³⁵ 17 U.S.C. § 512(b).

³⁶ See, e.g., Playboy, 839 F. Supp. at 1561 (the use of the plaintiff's registered trademarks to identify the files containing the copyright-infringing photographs, constitutes trademark infringement and unfair competition in violation of the Lanham Act, 15 U.S.C. §§ 1114, 1125(a)), see also, Economic Espionage Act, 18 U.S.C. § 1831 et seq. (1996):

(a) Whoever, with intent to convert a trade secret, that is related to or included in a product that is produced for or placed in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly-- . . .

(2) without authorization copies, duplicates, sketches, drawings, photographs, *downloads*, *uploads*, alters, destroys, photocopies, *replicates*, *transmits*, *delivers*, *sends*, mails, communicates, or conveys such information; . . . shall be . . . fined under this title or imprisoned . . . or both. (Emphasis supplied.)

³⁷ See Playboy, 839 F. Supp. at 1560.

³⁸ 3 J. Thomas McCarthy, McCarthy on Trademarks and Unfair Competition, § 25:70 (1997 and supp. Dec. 1998) (hereinafter "McCarthy on Trademarks").

³⁹ McCarthy on Trademarks, § 25:70 (describing the allegations in The Washington Post, Co. v. Total News, Inc., filed in the Southern District of New York on February 20, 1997, wherein the plaintiffs alleged that the defendant infringed its trademark and copyrights by framing the content of its Web sites with buttons containing advertising sold by the defendant. The case later settled before final resolution with the defendant agreeing to stop framing and clearly identify any information that the defendant linked to, was that of the plaintiffs).

⁴⁰ See DoubleClick, Inc. v. Henderson, 1997 WL 731413 (N.Y. Super. Ct., Nov. 7, 1997) (defendants, former executives of an Internet advertising company, successfully defended against claims of trade secret violations in connection with leaving the company to compete with the plaintiff. The court rejected their argument that the customer pricing and other information posted on the plaintiff's Web site was specific enough to destroy the secret nature of the underlying pricing and marketing strategies).

⁴¹ See Vault v. Quaid Software, Ltd., 847 F.2d 255 (1988) (holding that a shrink-wrap license was an unenforceable adhesion contract and the state statute authorizing such contracts was pre-empted by federal copyright law); Step-Saver Data Systems v. Wyse Tech. and Software Link, Inc., 939 F.2d 91 (3d Cir. 1991) (holding that a license agreement was not part of the contract between the parties where they orally agreed to the sale without mention of the shrink-wrap license agreement because the opening of the package was insufficient to establish expressed assent to modify the contract under UCC 2-209 and the new terms were not included under the battle of the forms analysis of UCC 2-207); Arizona Retail Systems v. Software Link, Inc., 831 F. Supp. 759 (D. Ariz. 1993) (same).

⁴² ProCD, Inc. v. Zeidenberg, 86 F.3d 1447 (7th Cir. 1996).

⁴³ ProCD, 86 F.3d at 1452.

⁴⁴ ProCD, 86 F.3d at 1452.

⁴⁵ ProCD, 86 F.3d at 1452 (citing UCC § 2-606(1)(b) in support of its holding).

⁴⁶ ProCD, 86 F.3d at 1452 (“[defendant] had no choice [to avoid the opportunity to read the license], because the software splashed the license on the screen and would not let him proceed without indicating acceptance”).

⁴⁷ Hill v. Gateway 2000, Inc., 105 F.3d 1147 (7th Cir. 1997) (holding that an arbitration agreement packaged inside a computer shipping box was enforceable despite the fact that the original agreement between the parties took place over the phone and no mention of the specific license terms was made at that time).

⁴⁸ See Gateway, 105 F.3d at 1150.

⁴⁹ Micro Star, 154 F.3d at 1113.

⁵⁰ Micro Star, 154 F.3d at 1112.

⁵¹ Micro Star, 154 F.3d at 1114.

⁵² In fact, the court recognized that no license existed between these two parties. The court even declined to decide whether the license between the user and the plaintiff was valid. Micro Star, 154 F.3d at 1114. The court appears to contradict itself by assuming that the license agreement is not valid, and the plaintiff granted an implied license or abandoned its rights to the derivative work, but that plaintiff reserved its rights to commercially distribute the derivative work, by prohibiting such action *in the license agreement*.

⁵³ Micro Star, 154 F.3d at 1114. The court appears to contradict itself by assuming that the license agreement is not valid and that the plaintiff granted an implied license or abandoned its rights to the derivative work, but that plaintiff reserved its rights to commercially distribute the derivative work, by prohibiting such action *in the license agreement*. Id. Under this reasoning, whether or not the license agreement is valid, the copyright owner gets the benefit of its restrictions on the user's use of the work.

⁵⁴ The UCC provides that unconscionable contracts may not be enforceable in whole or in part. U.C.C § 2-302.

⁵⁵ See Compuserv, Inc. v. Patterson, 89 F.3d 1257 (6th Cir. 1996); Hotmail Corp. v. Van\$ Money Pie, Inc., 1998 WL 388389 (N.D. Cal., April 16, 1998).

⁵⁶ Compuserv, 89 F.3d at 1264.

⁵⁷ Spam is "unsolicited commercial bulk e-mail akin to junk mail sent through the postal mail." Hotmail, 1998 WL 388389 at *1.

⁵⁸ Hotmail, 1998 WL 388389 at *6.

⁵⁹ See Step-Saver, 939 F.2d at 99.

⁶⁰ The court in Step-Saver held that a warranty disclaimer was a material term and thus absent express acceptance it was excluded from any agreement despite the fact that both parties were merchants. Step-Saver, 939 F.2d at 105.

**NEGOTIATION OF SOFTWARE LICENSE AGREEMENTS
AND RELATED AGREEMENTS**

Cynthia L. Stewart
Brown, Todd & Heyburn PLLC
Louisville, Kentucky

**NEGOTIATION OF SOFTWARE LICENSE AGREEMENTS
AND RELATED AGREEMENTS**

TABLE OF CONTENTS

I.	PRE-CONTRACT PLANNING	I-1
A.	Put Your Team Together	I-2
B.	Do Your Homework	I-2
C.	If Appropriate, Send Out A Request For Proposal	I-2
D.	Obtain Software Provider's Form Agreement As Early As Possible	I-2
E.	Assess The Balance Of Power	I-2
II.	SOFTWARE LICENSE AGREEMENT NEGOTIATION	I-3
A.	Specifications	I-3
B.	License Grant	I-3
C.	Warranties	I-4
D.	Delivery, Installation, And Training	I-5
E.	Modifications	I-5
F.	Acceptance Testing	I-6
G.	Warranty Period	I-6
H.	Fulfillment Of Warranty	I-6
I.	Support	I-6
J.	Maintenance	I-7
K.	Payment Structure	I-7
L.	Copies Of Software And Documentation	I-7
M.	Confidentiality	I-8
N.	Software Escrow	I-8
O.	Termination	I-9
P.	Indemnification	I-9
Q.	Boilerplate	I-10
1.	Force majeure	I-10
2.	Insurance	I-11
3.	Merger clause	I-11
4.	Applicable law	I-11
5.	No assignment	I-11
6.	Jurisdiction	I-11
7.	Taxes, waiver and severability	I-11
R.	Other Agreements	I-12
III.	NEGOTIATING TIPS AND TRICKS	I-12
A.	Form Agreement	I-12
B.	The Big Rush	I-12
C.	Everyone Else Has Signed This Agreement	I-12
D.	The Stalemate	I-12
IV.	CONCLUSION	I-13

SECTION I



NEGOTIATION OF SOFTWARE LICENSE AGREEMENTS AND RELATED AGREEMENTS

(Or More Than You Ever Wanted To Know About Software License Agreements)

The vast majority of businesses throughout the world employ some form of software in their daily activities. To remain competitive, businesses are purchasing expensive, sometimes specially tailored, software to enable them to become more efficient, to automate entire departments, to conduct e-commerce and to otherwise conduct business in a more efficient and productive manner. As this move toward computerization progressed, the software industry gained a slight edge in the marketplace. Businesses were sometimes reluctant to give the proper attention to the software purchasing and contract negotiation process. Often businesses delegated these tasks to technology administrators who were capable of evaluating the software product, but who may not have been aware of the long term business plans of their company and who were generally not skilled in negotiating software contracts. At the time, many software providers took advantage of this situation. Now, finally, top level executives are waking up to the significance of technology in the modern business world and are better at allocating the proper resources, time and money to major software acquisitions. Even better, in-house counsel and outside counsel have been invited to serve as a part of the software acquisition team.

This article was prepared primarily for the benefit of counsel who represent companies in purchasing software, but should also be helpful to lawyers representing software providers. The goal is not to "win" or to receive an unfair advantage, but to negotiate a contract that is fair and reasonable for both sides. This article is meant to provide a broad overview on the issues that regularly arise in connection with the negotiation of software license agreements, and is divided into three segments, the first relating to pre-contract planning, the second discussing the actual contract negotiation process and likely terms of the contract, and the third addressing negotiation tactics and tips.

In this article, the term "user" refers to a business that is proposing to acquire software, and the terms "software provider" and "provider" refer to the software vendor.

I. Pre-Contract Planning.

Unfortunately, as counsel, you are often called in at the eleventh hour when many of the deal terms have been finalized, and you are assigned what clients typically think of as the administrative task of dotting the i's and crossing the t's. As outside counsel, there is often little you can do about this situation, because you probably are unaware that one or more of your clients are contemplating the purchase of expensive software. To the extent you become aware of a proposed acquisition, however, there are some steps you can take early in the process to minimize negotiating conflicts and maximize negotiating leverage.

A. **Put Your Team Together.**

Step one in the process is to put the team together who will make the acquisition decision. Most companies now form an internal team to take on the project, but do not include legal counsel, who can be much more helpful on the back-end if plugged in on the front-end. Your team should include a technology expert, who can be in-house or, as is becoming more common, an independent contractor who specializes in assisting third parties in purchasing complicated software, a decision-maker, a user of the software, and legal counsel.

B. **Do Your Homework.**

Although it seems to be an obvious point, many companies rush the acquisition process due to a real or artificial deadline and do not thoroughly research their options. In addition to doing research and comparing providers, the company needs to check references, and if possible, spend time with other companies who have purchased the software and are in the midst of using it in their businesses.

C. **If Appropriate, Send Out A Request For Proposal.**

Depending on the money to be spent on a software package and the resources of the company, it is often helpful to issue a Request for Proposal that sets out the needs of the user and the proposed specifications of the software, and that can further include a form agreement. The advantages to this approach are enormous. First, it forces both parties to the transaction to be very specific up front about the software, which reduces conflicts on the back-end. It also creates an environment of competition. A company responding to an RFP does not know whether others are responding, and the mere issuance of an RFP causes participants to assume that there is competition. Finally, it can otherwise maximize the user's negotiating leverage. One requirement of an RFP can be that negotiations be based on the form agreement included with the RFP. Further, to the extent the software provider tries to waffle on a particular software specification or obligation, the user can refer back to the RFP, which may very well indicate that the software provider earlier agreed to that particular specification or obligation.

D. **Obtain Software Provider's Form Agreement As Early As Possible.**

To the extent a user does not offer its own form as a starting point for negotiations, it is important to obtain a copy of the agreement as early as possible in the process to allow for the negotiation and resolution of differing positions sooner rather than later. This helps avoid having the deal killed due to objectionable contract provisions. No lawyer wants to be blamed for killing a deal for a client, especially when the client is not convinced of the seriousness of the point of conflict.

E. **Assess the Balance of Power.**

This step is often taken subconsciously, but it is helpful for the counsel involved to consciously evaluate the answers to the following questions: How desperate is the user for the software? What is user's time table? How many providers are there of the software in question? What monies are to be spent? If the user is happy with the software, could there be additional

purchases of goods and services from the software provider? Finally, what is the general demand for the program and the relative size of the negotiating parties? These questions should have been answered early on, but to the extent counsel is being brought in late in the game, answers to the aforementioned questions help counsel assess the negotiating leverage of the client.

II. Software License Agreement Negotiation

Set forth below is a discussion of sixteen key provisions of a software license agreement and a separate discussion on some of the so-called "boilerplate" provisions of a license agreement.

A. Specifications.

Setting out the standards and desired requirements of the software program is one of the most important aspects, if not the most important aspect, of the entire software contract process. Unfortunately, it is too often the case that the marketing representative for the software company talks to the marketing representative for the buyer, and it is not until both parties have invested a significant amount of time in the process that someone with the technical expertise actually articulates the software needs of the user. Sometimes there are published specifications, which the technical specialist representing the user should carefully review. Where there are no published specifications or where specifications beyond that which are published are needed by the user, these specifications must be set out very carefully. If the specifications for the software are sufficiently comprehensive, there are generally very few problems implementing the agreement. As part of the specifications, users who must have compatibility with other programs should reference such other programs and the compatibility requirement. Some users must have software written in certain programming languages; some users must have certain documentation for different levels of users within the organization and so on. This should all be included in the specifications for the software. If the user attracted the software company through an RFP, the user may be able to rely upon the detail set out in the RFP to describe its software needs.

B. License Grant.

The actual license grant in the agreement is typically couched in terms of a perpetual license that may or may not include improvements and/or modifications to this particular version of the software and that may or may not include source code.

Software has traditionally been licensed rather than sold outright so that the software provider has more control over the use of the software. If sold outright, the "first sale doctrine" under the Federal Copyright Act would allow the owner of a copy of the software to resell the copy and would give the owner broad rights with respect to its use of the copy. A license agreement enables the software provider to forbid or limit transfers and modifications to the software and to otherwise restrict the manner in which the software is used.

With respect to source code, naturally a user would prefer that the license include the underlying source code for the program. Typically, the software provider does not want to allow

access to the source code. This is a negotiable point, although it is not unusual for a user not to receive a license to the source code as a part of the user's software acquisition. Different situations give rise to different levels of need for source code access. In cases where the user does not receive access to the source code as a part of its license, then the user should consider whether a source code escrow would provide the user adequate protection and address the user's source code access concerns.

As an aside, the case and statutory law on reverse engineering by no means gives software users the green light to reverse engineer licensed software. The seminal case on the matter, *Sega Enterprises, Ltd. v. Accolade, Inc.*, 977 F.2d 1510 (9th Cir. 1993), holds that reverse engineering for the purpose of making computer games compatible with certain machines is fair use of the copyright where the reverse engineering was the only way to gain access to the "unprotected ideas" and "functional elements" of the computer program.

C. Warranties.

As is true with almost all contracts, there are express warranties and possibly some implied warranties in software license agreements. The following is a typical express warranty: "This Software is free from significant programming errors and conforms to the specifications set out in Annex A to this Agreement [and to the other criteria set out in the materials attached to Annex A.]" The express warranty emphasizes the importance of having appropriate specifications to the success of the transaction. A user might also attach marketing or other materials provided by the software provider (e.g., manuals and documentation) to the agreement to attempt to hold the software provider to the promises set out in those materials.

An additional warranty that should be provided is a warranty with respect to ancillary services. In almost all cases, the software provider will perform some services, such as installation, support, or maintenance, in connection with the software. An appropriate performance warranty is as follows: "Provider will perform services in a workman-like manner, according to standards of care and diligence and a level of skill, knowledge and judgment normally provided by [national] [regional] companies in the industry."

There are also implied warranties that might apply to a software license agreement. The two most relevant implied warranties include the warranty of merchantability (found in the Uniform Commercial Code ("UCC") at 2-314) and the warranty of fitness for a particular purpose (found at 2-315 of the UCC). The warranty of merchantability provides that goods must be fit for the ordinary purpose for which such goods are used. The warranty of fitness for a particular purpose provides that when the seller knows of a particular purpose for which the goods are to be used, and the buyer is relying upon the seller's skill or judgment, then there is implied warranty that the goods will be fit for such particular purpose. Both of these warranties could be helpful to a user in a software license context, especially if the user has failed to adequately express its software needs and requirements in the agreement. It is not crystal clear that the sale of software through a software license is a sale of goods to which the Uniform Commercial Code would apply; however, the courts appear to be leaning in favor of software licenses being goods under the Uniform Commercial Code. (See, *Advent Systems Ltd. v. Unisys Corp.*, 925 F.2d 670 (3rd Cir. 1991)). As an aside, the proposed new Uniform Computer

Information Transactions Act ("UCITA") would provide a body of statutory law that would apply to software licensing, however, it is difficult to predict when or if the new proposed UCITA will be adopted by The National Conference for Commissioners on Uniform State Laws or by any state.

Another appropriate and timely representation for a software license agreement is a representation relating to the year 2000 compliance of the software. A sample representation is as follows:

All Software and any updates, patches and fixes to the same shall (1) properly execute with all date data, whether from years in the same century or in different centuries, by yielding correct results in arithmetic operations, comparisons, sorting of date fields and otherwise, and (2) not abnormally cease to execute or return an erroneous error message due to date-related processing.

Finally, a software provider should make the standard representations and warranties that the provider has title to the software and that the software does not infringe any third party intellectual property rights.

D. Delivery, Installation, and Training.

These terms are negotiable depending on the software and the level of provider involvement necessary to get the program up and running. One issue that commonly arises is whether the cost of installment and/or training is included in or is in addition to the then-negotiated purchase price. To the extent a user needs delivery, installation and/or training as of particular date, this should be set out in the agreement. The user's expectations with respect to training should also be clearly expressed in the agreement.

E. Modifications.

Most license agreements prohibit modifications to the code or at a minimum cause any express warranties to terminate upon modification of the code. It is useful for a user to negotiate the ability to make certain minor modifications. Had users who wanted to engage in year 2000 self-help remediation negotiated such modification rights, those users would continue to be in good standing under their license agreements following the implementation of year 2000 changes. If a user cannot anticipate a situation where it would need the right to modify its code, one approach is to negotiate the right to make modifications as necessary to enable the program to function as intended by the parties. When modifications are not forbidden but cause the warranty to be compromised, the user should propose that the warranty remain intact (1) if the software provider approved the modification, (2) if modification does not affect the part of the program with respect to which warranty is being relied upon; or (3) if the user can remove the modification and such modification and removal do not otherwise compromise the program.

F. **Acceptance Testing.**

The accepted testing clause seems to be missing from many software license agreements, and it is critical to a user who is paying significant amounts for a unique software program. Following installation and user training, the user should have a period of time to test the program, and the agreement should provide options for the user should program fail the acceptance test. Those options include the requirement that the provider correct the program for no additional charge, with the user then having the right to retest. The user should also ultimately be able to terminate the agreement and receive a refund of amounts paid if the program continues to fail the acceptance test.

One issue relating to testing is determining whether the program has passed the test. One option that is not popular with software providers is for the program test to be satisfactory to the user. A common middle ground is for the parties to agree that the program has passed the test if it performs in accordance with the agreed upon specifications. If the user has been careful enough to negotiate these carefully and to test thoroughly, the user should be adequately protected.

G. **Warranty Period.**

The express warranty typically starts following the acceptance of the program by the user and continues for a period of time, which time period is negotiable. The time period for a warranty generally runs from 30 days to one year.

H. **Fulfillment of Warranty.**

If during the warranty period, the software fails to perform in accordance with the terms of the license agreement, then the software provider should be obligated to "promptly" correct any such defects at its own expense. If the software is not made compliant within a reasonable time, the user should have the right to terminate the agreement and receive a full or pro-rated refund, depending on the circumstances involved. To the extent a user has concerns about the ability of a provider to perform (in which case one may wonder why the provider was hired), the software user may demand a performance bond on behalf of the provider that would offer the user some added protection.

I. **Support.**

Even if the software provider has conducted training, users' employees and staff will have questions and issues that will later arise as a part of the actual use of the system. Some software providers have pre-established time periods during which they will be accessible by phone, but this is sometimes negotiable. Depending on the system being installed, the user may also want to negotiate for access to after-hours support, on-site support and may want to specify minimum response times.

J. **Maintenance.**

Maintenance is often covered by a separate agreement with separate consideration. In its most basic form, it is merely an extension of the warranty period, meaning the software provider's obligation is to maintain the program so that it operates in accordance with the original specifications and in accordance with other warranties (such as the Y2K warranty) during the term of the maintenance agreement. To sell a maintenance package, however, software providers may add features, and users should know that additional features, such as enhancements and/or upgrades, are often negotiable at a free or reduced cost as a part of the maintenance package. A software license may already contain an obligation that the software provider forward for free improvements to the particular version of software that is licensed (improvements meaning changes that increase efficiency and effectiveness of the basic program but do not change functions or create new ones), so the maintenance agreement, or maintenance sections of the license agreement, may be an appropriate place to negotiate for other added benefits.

In any case, a user may want to specifically address the provider's obligations with respect to maintenance, including the manner in which the maintenance will be implemented and procedures used to deal with emergency situations.

K. **Payment Structure.**

Typically, the license fee is presented as a lump sum payment, which the software provider wants paid up front, and the user wants to pay as late in the game as possible. To the extent possible, the user should hold back the bulk of the payment at least until the software has been tested and accepted. Some users may have the negotiation leverage to space out payments over a period of years, but in most cases the latest time that a payment for the software can be made is at the time of acceptance.

L. **Copies of Software and Documentation.**

Some software is priced based on the number of individual users of the software, and therefore the license agreement already specifically addresses the number of copies the user may make of both the program and the instructional materials or other documentation supporting the program. The right to make copies should be specifically addressed in some manner in the agreement. Otherwise, the presumption is that no copying is permitted. Of course, the user would prefer a provision allowing the user to make as many copies as necessary to satisfy the user's internal needs. If that approach is not agreeable to a software provider, then a reasonable number of copying allowances should be negotiated, taking into consideration that the user will need one or more backup copies for the user's in-house backup efforts, and the user may also have a third-party contract with a disaster recovery company for which copies of the programs may be necessary.

M. **Confidentiality.**

There is typically an obligation in a license agreement that the user maintain the confidentiality of the software and other materials licensed, especially when access to source code has been provided. This is standard and appropriate, but the user needs to ensure that its reasonable use of the program is not unduly restricted by this provision. Employees and other representatives will use the program, and third parties may need access to the program, and these circumstances should be specifically addressed in the agreement. Also, users may employ a third-party disaster recovery company where copies of programs and information of the user are stored and maintained at a third-party location, which situation should be specifically provided for in the agreement. Finally, the user may have confidential information to which the software provider may have access in connection with the provision of installation and other services, and, therefore, it is often appropriate for the confidentiality provision to be mutual.

N. **Software Escrow.**

If the user does not obtain access to the software source code as a part of the license, and the user has paid a significant price for such software, obviously the user will have concerns about the ability to preserve the usefulness of the software for the long term. A separate article could be written on software escrow agreements alone; however, this section will the focus only on the most critical provision of a source code escrow agreement, which is the provision that triggers the release of the code. The following are possible triggering events for the release of the source code to the user:

1. The software provider's inability during the warranty period to correct any malfunction, defect or nonconformity that prevents the software from performing in accordance with agreed-to specifications;
2. The software provider's inability to fulfill its maintenance obligations;
3. The sale of the software provider or of substantially all of its assets, or some other change in control of the software provider; and
4. The insolvency, bankruptcy or other similar occurrences affecting the software provider.

Paragraphs 2 and 4 are fairly common in source code escrow agreements. The other two paragraphs are negotiable and the ability to include these provisions in the escrow agreement depends on the particular circumstances of the parties.

Most escrow agreements outline a detailed procedure that a user must follow to trigger the release of the source code and further provide a procedure allowing for the challenge of the release by the software provider. If challenged by the provider, the dispute is typically automatically referred to arbitration or some other dispute resolution procedure for resolution.

Banks can serve as escrow agents, but many banks are unfamiliar with the practice of escrowing source code. There are a growing number of escrow firms that deal primarily in software, including Lincoln-Parry Associates, Inc. at www.softescrow.com; Data Securities International, Inc. at www.dsiescrow.com; and Fort Knox Escrow Services, Inc. at www.fortknoxescrow.com. Many of these firms have their own escrow agreements that a user and software provider must modify to suit their needs.

O. **Termination.**

The license agreement should contain standard language allowing for a termination after a notification of breach by the non-breaching party and the passage of a reasonable period of time to cure the breach. A user might also want to include as a default under the agreement the repeated occurrence of problems causing downtime, even if the problems have ultimately been remediated each time. For example, a user may want to be able to declare a default under the agreement if within a six-month period the system malfunctions to a degree that it disrupts business for more than a specified period of time or more than a specified number of times. Most agreements include bankruptcy and similar events as a basis for terminating a license agreement. Further, the breach of a maintenance agreement might trigger a breach of a license agreement and vice versa.

If the software provider is a talented but a relatively new start-up company, the user might consider requiring the provider to post a performance bond to better ensure the completion of the project.

What happens upon termination should be carefully outlined out in the agreement. Does the user receive a full or prorated refund? Does the termination trigger a release of the source code from escrow? Can the user retain the software and engage in self-help or employ a third party to modify it so that it is usable? The user should think through the most likely termination scenarios and address them in the agreement.

In the current environment, users may have the technological capability to correct problems in house or may have access to outside expertise. To the extent a user has or can hire this capability, it should specifically negotiate for the right to correct the software through self or third party help. If this option is not specifically provided for in the agreement, the presumption is that the user has no right, directly or indirectly, to modify or correct the software, even when the provider is not able to correct the problem.

P. **Indemnification.**

The software provider should indemnify a user for any loss or expense arising out of any claims of infringement of third-party intellectual property rights. In most cases, this clearly is the responsibility of the provider, and indemnification in this case should not be limited. Further, the software provider should indemnify a user for any damages caused to person or property in relation to the negligence or other acts of any software provider employee or agent who accesses user's property to install or maintain the software or provide training. To the extent a user accesses the provider's property, then this indemnification should go both ways. Finally, both

parties should indemnify the other for breaches relating to the obligation of each party to maintain the confidentiality of the other party's confidential information.

However, with respect to indemnification due to the inadequate or failed performance of the software, many licensors demand that certain limits apply, such as a limit on consequential damages and a limit in damage amount to the amount paid for the software. These provisions are becoming more common, and the argument supporting these provisions is that software development is not a precise science and it is difficult to know in advance the full ramifications of a certain software code. A software provider will argue that it is the user's responsibility to test the program thoroughly, while protecting its existing programs and data, before going live with any software program. This argument has merit; however, to the extent a user has the negotiation leverage to obtain more protection, or a higher dollar threshold limitation, it should certainly pursue such protections.

Other common limitations include a contractual statute of limitations, typically of one year. Without the contractual statute of limitations, a statute of limitations of four to fifteen years may apply. Finally, many providers limit the user's remedy upon nonperformance of software to a repair or a replacement of the software. This, of course, is not as desirable as a refund, and does not address the situation where the software can not be corrected, so users should review license agreements carefully for this type of limitation.

Most of the limitations discussed above, have been held enforceable in one context or another. See *ProCD, Inc. v. Zeidenberg*, 86 F.3rd 1997 (7th Cir.1996) for a case addressing the enforceability of limitations on consequential damages and on remedies. Also, please refer to *NMP Corp. v. Parametric Technology Corp.*, 958 F.Supp. 1536 (N.D. Okla. 1997) for a discussion on the enforceability of warranty periods and remedy limitations. Finally, an article by Deborah Kemp entitled "*Mass Marketed Software: The Legality of the Form License Agreement*," 48 LA. L. REV. (1987), discusses the enforceability of various provisions in the shrink-wrap context. If such provisions are enforceable in a shrink-wrap context, it would be difficult to argue that they would not be enforceable in the case of a negotiated license agreement.

Counsel should keep in mind, however, that the year 2000 litigation may rewrite some of the prior law and may provide new rules regarding or the enforceability of damage, warranty and remedy limitations.

Q. **Boilerplate.**

It is unfortunate that standard legal provisions are given the title of "boilerplate" because often those provisions offer the client some very important protections. This section of the article briefly discusses some of these so-called "boilerplate" provisions and highlights those provisions that should be considered for inclusion in software license agreements for the protection of one or both parties.

1. **Force Majeure.** Most providers will insist on a force majeure clause in the license agreement, which excuses the non-performance of providers in certain circumstances.

From a user's perspective, the list of force majeure events should be reviewed carefully to ensure that all listed events are applicable and appropriate, and further a user should include a clause allowing termination even if the event is not the fault of the provider if the force majeure event lasts over a certain period of time, such as 30 days.

2. **Insurance.** It may be to the user's benefit to require that the software provider have certain insurance, especially if the software provider will be sending its employees or representatives on-site to user's location. In addition, the user may be able to negotiate an indemnification amount in the case of the malfunction of the program up to the amount of insurance coverage, and that amount could specifically override any damage limitation. In addition, it is appropriate in some cases for the user to request to be added as an additional insured to the provider's policy.

3. **Merger Clause.** From the software provider's perspective, the merger clause is a very important provision. In some cases, the absence of this provision can be beneficial to the user. This provision takes away any pre-agreement representations, warranties, statements and other promises and "merges" those out of existence, with the agreement being the final statement of understanding between the parties.

4. **Applicable Law.** Typically, the software provider will insist that the law of its state apply to the agreement, and the argument supporting this request is the provider's need for consistency. The provider may sell computer software in all of the United States and maybe throughout the world, and it needs a consistent application of law to its agreement. In most circumstances, this is not an unreasonable position; however, a user with significant leverage may be able to insist that the law of its state govern the agreement.

5. **No Assignment.** Software providers generally insist that the software program be non-assignable. The user may want to carve out certain exceptions to that non-assignment restriction, such as in the case of a sale of substantially all of user's assets or the line of business to which the software applies. Further, the user may want the right to shift the software to a related company, in case there is a reorganization of the company. Additionally, in cases where the user has significant negotiating leverage, it may want to negotiate for certain rights upon the sale of the software provider, such as the release of source code from escrow if the successor company cannot perform under the license and/or maintenance agreements.

6. **Jurisdiction.** The software provider will usually propose that the user submit to the jurisdiction of the software provider's home state. To the extent the user cannot win this negotiation point, the user may want to insist on mandatory and/or permissive mediation or arbitration.

7. **Taxes, Waiver and Severability.** The Taxes, Waiver and Severability provisions are fairly standard in a license agreement. The Taxes provision typically provides that the user is responsible for sales or use taxes, which is appropriate. The Waiver provision generally provides that any act of waiver by one party does not enable the beneficiary to assume that future acts of noncompliance will be waived. The Severability clause provides that if a particular provision of the agreement is not enforceable, it will be reduced or removed from the agreement to allow the remainder of the agreement to be enforceable. This provision should be

carefully drafted and perhaps limited to provide that to the extent the elimination or reduction of the provision frustrates the essential purpose of the agreement, then the entire agreement will be considered null and void.

R. **Other Agreements.**

The other agreements that have a relationship to a software license agreement include a maintenance agreement, a software escrow agreement, a support agreement and a software development agreement. While this article does not allow for a full discussion of each of those agreements, many of the principles discussed earlier can be applied to a negotiation of these agreements. With respect to the software development agreement in particular, the user and the provider will likely negotiate a detailed schedule of work allowing for acceptance testing and the making of payments as certain pre-agreed to milestones are timely achieved.

III. Negotiating Tips and Tricks.

A. **Form Agreement.** One of the best ways to obtain negotiating leverage in a software license context is the method earlier mentioned of using a Request for Proposal that sets out a user's form agreement. This communicates to the software provider that it is in a competitive environment and that it must use the RFP as a basis for negotiation.

B. **The Big Rush.** As in many contexts that require a negotiation of price and other aspects of a transaction, the party selling goods routinely employs a rush tactic. The software provider may claim that it is about to allocate resources elsewhere that otherwise would be allocated to the user, or the provider impresses upon the user that the user must promptly purchase the software to ensure that the user is on the cutting edge of its business, and so on. Users and their counsel should recognize this "hurry up and buy" tactic for what it is and take all the time necessary to negotiate an appropriate agreement and purchase appropriate software. On the other hand, sometimes the user really is behind the eight ball, and this situation compromises the negotiating leverage of the user.

C. **Everyone Else Has Signed This Agreement.** One of the most common statements made by a software provider is that every other user has signed its form agreement. There may be some cases where this is true, since software providers have had an advantage over users in this cutting edge field for various reasons. Furthermore, if evidence can be presented that the signing parties included large nationwide companies, then a user may assign some creditability to this statement. However, in most cases, either the statement is untrue or the buyers of the software did not involve their lawyers in the agreement negotiation process. In any case, each user has different concerns and needs that must be addressed and that require a certain amount of tailoring of an agreement.

D. **The Stalemate.** Sometimes it appears impossible that the parties will be able to move beyond a particular point of disagreement. In such cases, it is imperative that counsel be able to explain the full ramifications and meaning of a particular provision to a client and to draw out from the client the client's particular concerns, so that those can be directly addressed. Counsel should use the same principals when dealing with the other side, however, this is much

more difficult because parties are accustomed to concealing their true motives and desires in the contract negotiation process for fear of giving up some leverage. Getting to the bottom of a problem sometimes involves talking directly with the decision makers of the parties and/or getting these decision makers together. Fortunately, more often than not, when the true concerns of a party are sincerely expressed, the parties and their counsel find some way, through additional insurance, a performance bond, a software escrow, or some other means, to resolve the disagreement and move on.

IV. Conclusion.

In conclusion, hopefully, this article has provided a broad overview of software license agreements and some helpful tips for negotiating those agreements. For additional information and guidance, I highly recommend the Allen & Davis treatise on computer contracts entitled "*Computer Contracting: A User's Guide With Forms and Strategies*," published by Prentice Hall.



**JURISDICTIONAL ISSUES ARISING
OUT OF E-COMMERCE**

Kenneth J. Tuggle
Brown, Todd & Heyburn PLLC
Louisville, Kentucky

Copyright 1999, Kenneth J. Tuggle. All Rights Reserved.

SECTION J



NOTES

NOTES

NOTES



**INTERNET / E-MAIL PRIVACY ISSUES; ENCRYPTION
AND ELECTRONIC ESPIONAGE**

Civil Law Perspective

Joseph J. Zaluski
Judge B. Wilson II
Wyatt, Tarrant & Combs
Lexington, Kentucky

Criminal Law Perspective

David J. Beyer
Chief Division Counsel
Federal Bureau of Investigation
Louisville, Kentucky

**INTERNET / E-MAIL PRIVACY ISSUES; ENCRYPTION
AND ELECTRONIC ESPIONAGE**

CIVIL LAW PERSPECTIVE

Ethics, Privilege, And Confidentiality Considerations When Using E-Mail And Internet

Joseph J. Zaluski
Judge B. Wilson II
Wyatt, Tarrant & Combs
Lexington, Kentucky

SECTION K(a)

**INTERNET / E-MAIL PRIVACY ISSUES; ENCRYPTION
AND ELECTRONIC ESPIONAGE**

CIVIL LAW PERSPECTIVE

TABLE OF CONTENTS

I.	INTRODUCTION	K(a)-1
II.	PART I: SNIFFERS, SNOOPERS, HACKERS AND CRACKERS	K(a)-2
III.	PART II: ATTORNEY-CLIENT PRIVILEGE AND E-MAIL	K(a)-7
	A. Confidentiality On-Line	K(a)-8
	B. Inadvertence	K(a)-10
	C. Arizona Treatment	K(a)-13
	D. Kentucky Treatment	K(a)-13
	E. Pennsylvania Treatment	K(a)-14
	F. District Of Columbia Treatment	K(a)-14
IV.	PART III: ADVERTISING AND SOLICITATION	K(a)-15
V.	PART IV: CONCLUSION	K(a)-16



Introduction

“A whole calling may have unduly lagged in the adoption of new and available devices. It never may set its own tests, however persuasive may be its usages. Courts in the end must say what is required...” The T.J. Hooper, 60 F.2d 737 (2nd Cir. 1932)(an opinion by Learned Hand).

For the ill-fated T.J. Hooper, it was whether or not to equip the tugboat with radio receivers to warn of approaching storms. In today's business environment, it is the decision of what technology to use. One of the most powerful tools available to today's business person (and lawyer) is the Internet, but since its birth and subsequent explosion into the mainstream, the Internet has created a tempest of legal debate. Of all the issues spawned in the tumult, perhaps those closest to the day-to-day life of a practicing attorney are the issues of ethics, confidentiality, and privilege. Clients have always expected speed and accuracy, but now as more people and businesses communicate electronically, these expectations have radically changed. To meet a client's expectations, now lawyers must be able to communicate using e-mail and the Internet. However, there are a number of choices to be made in the protection of a client's privacy and confidentiality. This paper will explore some of the practical issues of using the Internet and examine how the practical needs of attorneys and the demands of their clients can collide with confidentiality, privilege, and ethics.

By now, most people know that the Internet is a global network of interconnected computers. Many people also know that the Internet is the descendant of the ARPAnet (an acronym for Advanced Research Projects Agency). The Internet sends information through multiple computers, using variable routing. The "routing" computers choose the most efficient path (which may not be a straight line) to send the information based on amounts of traffic and other variables. This has the advantage of achieving speed while maintaining the maximum reliability, enabling the Internet to function even while portions of the network are malfunctioning. This design is the product of the ARPAnet's emphasis on maintaining communications even in the event of a nuclear attack. The downside of the Internet's design is that information passes through several hands before reaching its destination. On the way, it can be intercepted.

After a brief introduction describing the dangers and benefits of the Internet, this discussion will examine the attorney-client privilege and how the courts are likely to approach the issue of waiver when communicating on the Internet or with e-mail. Part II discusses privilege and confidentiality issues and the ethics of on-line legal advice. On-line advertising and solicitation issues are tackled in Part III.

Part I. Sniffers, Snoopers, Hackers, and Crackers.

All information is susceptible to theft. A letter can be opened, a phone line tapped, a cell or cordless phone transmission received, a safe cracked. The difficulty posed by Internet and e-mail communication is that no one is really sure how frequently interception

occurs. Thus without all the facts, many observers with an eye to maintaining privilege and confidentiality look for analogies in the law rather than in the facts. The most obvious and noted analogy is that those mediums of communication considered sufficiently "secure" to maintain privileges are illegal to intercept.¹ Since 1986, the Electronic Communications Privacy Act ("ECPA") has made the interception of electronic communications illegal. The ECPA also makes information gathered in violation of its provisions inadmissible as evidence.² However, this analogy does not truly address the ethical issues of maintaining a client's confidentiality and it remains to be seen how the courts will decide the issue.

The benefits of e-mail and the Internet are substantial.³ First there is speed. From the earliest days of the Internet, the U.S. Postal Service has been referred to as "snail mail,"⁴ and the name fits. The cost of sending information is also substantially less with e-mail. One page via snail mail is the cost of a first-class stamp; for about the same price, you can send 100 pages via e-mail.⁵ In terms of storage space requirements, there is no comparison between digital storage of information and the storage of thousands of pages of documents.

¹ See ABA/BNA Lawyer's Manual of Professional Conduct, Current Reports, vol. 14, 256, (June 12, 1998) citing District of Columbia Bar Legal Ethics Comm., Op. 281 (February 12, 1998, released May, 15, 1998);

² 18 U.S.C.A. § 2515.

³ The Internet is more than a communication device, it is a powerful source of information, sometimes even for the adverse party. See Stevens R. Miller, *Tracking Down E-mail Evidence*, New York Law Journal May 18, 1998, available at <http://ljj.com/securitynet/articles/0518emailv.html>. For an excellent article on search engines for use by attorneys, see Hon. Jefferson Lankford, *Internet Browser Search Engines*, <http://azbar.org/ArizonaAttorney/July98/7-98d4.asp>.

⁴ Robert L. Jones, *Client Confidentiality: A Lawyer's Duties with Regard to Internet E-mail*, August 16, 1995, <http://www.kuesterlaw.com/netethics/bjones.htm#content2/>.

⁵ *Id.*

Further, information in digital form can be more easily searched, accessed, and reproduced. Using e-mail is decidedly more efficient simply because the marginal time-cost of sending a message to multiple recipients is minimal by comparison to regular mail.

The Internet also holds opportunities for visibility and marketing. A 1997 survey conducted by the ABA found that 51 percent of large firms have home pages and 60 percent of the remainder have plans to make one.⁶ A companion survey of small firms found that 64 percent used the Internet- up from 38 percent the year before.

Despite its benefits, the use of the Internet and e-mail holds hidden dangers. To the ends of knowing the enemy, a brief but by no means exhaustive description of e-mail and Internet security issues is in order. There are several names for Internet eavesdroppers, thieves, and spies. The most commonly used name is "hacker" which generally refers to persons intensely interested in complex computer systems who may break into a computer system for a thrill ride through its files. "Crackers" are a more malevolent breed of hackers who deliberately damage or modify existing systems. Not only are these persons a threat to the security of e-mail while it travels through the electronic no-man's-land that is the Internet, but they may attempt to breach the security of a firm's own network.

Internet e-mail has been likened to a postcard or a call on a party line.⁷ E-mail messages share several intermediate computers as they travel through the network to reach their destinations. Another enemy of Internet and network security are called "sniffers" who

⁶ ABA/BNA Lawyers' Manual on Professional Conduct, Current Reports, vol. 14, 237 (May 27, 1998).

⁷ Robert L. Jones, *Client Confidentiality: A Lawyer's Duties with Regard to Internet E-mail*, August 16, 1995, <http://www.kuesterlaw.com/netethics/bjones.htm#content2/>.

capture the information as it passes through the intermediate computers. When computers are connected using common "ethernet" connections, e-mail is broken down into "packets" of information. Each packet has a label on it called a "header" telling the intermediate routing computers where to send it, where it is from, and other information to help it on its way. Following the header, the body of the packet consists of a portion of the e-mail message in plain text. When the packets reach their destination, they are reassembled. Sniffer software intercepts messages, and can even be programmed to use the address labels to capture messages to or from a certain machine or machines.⁸ Intercepted packets of data stored on the sniffer's drive can be reassembled. Then the sniffer can do whatever he pleases with your message: send it on, alter it, or simply delete it. Unless encryption is used to code the message, the sniffer's reassembled data is in readable text form just as it was sent.⁹

An often overlooked threat is the internal one. Like the outside hacker or cracker attack on a computer network, technical support staff and unscrupulous Internet service providers can access e-mail from within. However, some of these activities are incidental to the service they provide.¹⁰ Though internal firm security is outside the scope of this paper, it is important to protect the computers from which e-mail comes if Internet e-mail security is to have any real meaning.¹¹ A confidentiality agreement should be signed by all persons having access to a law firm's computers who are not a part of the firm.

⁸ *Id.*

⁹ The packet is in readable text form unless encrypted.

¹⁰ Jones, note 6, *supra*.

¹¹ For a discussion of firewalls, see *Firewall FAQ*, <http://www.v-one.com/pubs/fw-faq/faq.htm>; *Thinking about Firewalls*, <ftp://coast.cs.purdue.edu/pub/doc/firewalls>; *Routers and Firewalls*, <ftp://ftp.livingston.com/pub/livingston/firewall/firewall-1.1.ps.z>.

Another dangerous con game is called "spoofing." In spoofing, the victim is tricked into thinking that he or she is in one Internet site or network, but is actually in another. The attacker tricks the victim into making a mistaken decision that compromises his or her system's security.¹² This can include a situation in which the victim (attorney) believes that he is in contact with the client (spoofers). Some security measures only lead to a false sense of security where the spoofer is concerned. For example, if the user employs a "secure" Web access (using software with a Secure Sockets Layer) in the false environment, everything will look normal.¹³ In fact, the user does have a secure link, only not to where he thinks he is. In sum, whatever they are called, these various misanthropes can steal your e-mail, intercept your litigation strategy, thumb through your confidential files, and generally wreak havoc on all digitally stored information.

The bottom line is that the Internet is not secure. We cannot verify all users to make sure that they are not spoofers and we cannot protect every bit of information traveling on the Web. But, we can use encryption. It is not a cure-all to the dangers of the Internet, but it can substantially ensure that e-mail will not be altered or destroyed as it travels through the network.¹⁴ In simple terms, encryption codes messages so that they cannot be read without a password. Should a hacker attempt to read an encrypted file, all he will see is gibberish

¹² See Albert Barsocchini's article on spoofing at <http://www.ljx.com/tech/asked/articl12.htm>. Another excellent article is found at <http://ftp.cs.princeton.edu/sip/pub/spoofing.html>.

¹³ *Id.*

¹⁴ Jones, note 6, *supra*.

(unless he can break the code).¹⁵ Sniffer software cannot read it, and even the header (addresses) can be encrypted to make sniffing completely impractical.

Part II. Attorney-Client Privilege and E-mail.

A number of writers on the subject suggest that the place to begin in examining privilege is in the criminal law.¹⁶ In the area of ethics opinions, the most influential legislation concerning on-line communication is the federal Electronic Communications Privacy Act (ECPA).¹⁷ Though this law makes the interception of electronic messages illegal and unlawfully intercepted messages inadmissible, the effects of this legislation have gone far beyond evidence issues. As mentioned above, many courts and ethics committees rely on this law to justify the holding that there is in fact a reasonable expectation of privacy in the Internet. Thus, this law impacts the area of ethics and confidentiality as well.

The law of privilege is diverse. In federal courts, where state law supplies the rule of decision, the state's law of privilege governs. Otherwise, federal courts are to apply their common law.¹⁸ There are two fundamental bases for not finding that a communication is privileged. The first is that there was no expectation of confidentiality in the first place,

¹⁵ For an example of encrypted text see <http://www.mindspring.com/~bobjones/pgpsampl.htm>; Depending upon the complexity of the code, breaking it could take hours to centuries.

¹⁶ Joan C. Rogers, *Ethics, Malpractice Concerns Cloud E-mail, On-line Advice*, ABA/BNA Lawyers' Manual on Professional Conduct, Current Reports, vol. 12 (March 6, 1996); Albert Gidari, *Privilege and Confidentiality in Cyberspace*, <http://www.perkinscoie.com/resource/ecommm/priv.htm>.

¹⁷ 18 U.S.C.A. § 2510 et seq.

¹⁸ Fed. R. Evid. 501.

which can hinge on the type of communication used. Secondly, the privilege can be waived, even inadvertently. Many courts conflate these two theories, but in the context of e-mail the difference is important.

Of any number of ways in which an unintended person can gain access to an e-mail message, the two most likely are a violation of the ECPA, or an inadvertent disclosure by the attorney or client. When evidentiary issues are the only concern, a violation of ECPA makes the communication inadmissible.¹⁹ But, the mere use of the Internet may amount to a finding of non-confidentiality, defeating a claim of privilege before it begins. In the case of inadvertent disclosure, the evidence may or may not be admissible depending on the jurisdiction.

Confidentiality On-line.

The initial finding of privilege requires confidentiality, which means that the communication must not be disclosed to or made in the presence of third persons. Thus, a conversation between an attorney and client in a crowded room, or among friends can result in a finding that the communication was not privileged. In the context of e-mail and the Internet, the question becomes “is the Internet confidential in the first place?” This is

¹⁹ 18 U.S.C.A. § 2515. It is interesting to note that Wigmore advocated the view that privileges should not preclude testimony by eavesdroppers. This view asserts that those communications that the law of privileges are intended to protect are not discouraged by an unknown eavesdropper. See LAWSON, KENTUCKY EVIDENCE LAW HANDBOOK, vol. 3, §5.05 citing 7 Wigmore, EVIDENCE IN TRIALS AT COMMON LAW 633 (McNaughton rev. 1961). However, this argument is not as convincing where the Internet is concerned. The Internet is often the most efficient way to communicate, but the possibility of unknown “electronic eavesdroppers” could and does have a serious chilling effect on its use.

determined by the existence of "a reasonable expectation of privacy." Again however, the difficulty in determining how much information is snooped, sniffed, and intercepted makes this determination anyone's guess. This leads to the issue of where the burden lies for establishing the privilege. Without accurate information concerning security, how can the *reasonable* expectation of privacy be established. Fortunately, the ECPA answers this question in large part by making illegally intercepted communications inadmissible.²⁰ This is in accord with other authority to the effect that stolen documents retain their privileged status.²²

There is some judicial guidance on the subject of e-mail expectations in the context of internal networks and for semi-public commercial networks.²¹ In both instances, a reasonable expectation of privacy was found to protect the communication. However, the use of Internet e-mail, which is decidedly less secure, remains an undecided issue. An analogous medium in terms of security is the cellular phone. In a private action brought under the ECPA for the interception of a cellular phone conversation between an attorney and his client, a federal court found no violation of the ECPA.²² Though this was a private action and the court did not reach the waiver issue, the court's reasoning (that there was no expectation of confidentiality) indicates that waiver would have been found or alternatively that the privilege never would have attached. However, the court emphasized the fact that

²⁰ 18 U.S.C.A. § 2515.

²¹ U.S. v. Keystone Sanitation Co., 903 F.Supp. 803 (M.D. Pa. 1995) (a CERCLA case in which e-mail records were subject to discovery only after an inadvertent waiver); U.S. v. Maxwell, 42 M.J. 568 (USAF Ct. Crim. App. 1995) (semi-private commercial network such as America Online, or CompuServe).

²² Edwards v. Bardwell, 632, F.Supp. 584 (M.D.La. 1986).

cell phones use radio waves broadcast in all directions; this is an important factual difference between a cell phone and the Internet.

Because confidentiality must be maintained continuously to maintain the attorney-client privilege, the same "expectation of privacy" question is asked when determining if the later use of the Internet is a waiver of the privilege. Here, the ECPA does not give a direct answer. However, in ethics opinions it has become particularly influential. Most jurisdictions now state that encryption is unnecessary, and the Internet is expected to be private. However, some bar associations strongly suggest encryption, and most agree that it is necessary in the case of especially sensitive documents. The recent trend is toward not requiring any sort of protection when using e-mail.²³

Of course, every client thinks that his or her confidentiality is of crucial importance. Those states noted as adhering to the minority rule requiring encryption to avoid a breach of confidentiality include: Colorado, Iowa, and North Carolina.²⁴ In these states however, informed written consent of the client can waive this requirement. However, it is unclear if this sort of waiver of the requirement would also amount to a waiver of privilege or an acknowledgment of non-confidentiality.

Inadvertence:

The inadvertent e-mailing of privileged materials to an adverse party will likely be governed by the same law as any other inadvertent disclosure. Though the law varies

²³ ABA/BNA Lawyers' Manual on Professional Conduct, Current Reports, vol. 14, 256 (June 10, 1998).

²⁴ ABA/BNA Lawyers' Manual on Professional Conduct, Current Reports, vol. 13, 316 (October 15, 1997).

significantly by jurisdiction, there are three major schools of thought on the issue of inadvertent waiver: the lenient approach, the middle-of-the-road (Hydraflow), and the strict approach.²⁵ The lenient approach applies the theory that waiver must be knowingly made.²⁶ Since the client holds the privilege, it is inequitable to waive his privilege through the carelessness of his attorney.

The strict approach has the benefit of avoiding litigation of the issue by a strict adherence to the principle that inadvertent waiver is effective as to the document actually revealed as well as all related documents.²⁷ The justification of this theory is that the importance of the document is determined by the care used to protect it.

The middle approach assesses five factors to determine the presence or absence of a waiver. The factors are: the reasonableness of the precautions taken, the number of inadvertent disclosures, the extent of the disclosures, the promptness of remedial measures, and the overriding interest of justice.²⁸ At the court's discretion, the waiver, if found, may be extended to the related but unrevealed documents.²⁹

In most states, the lawyer is expected to refrain from examining materials if they clearly appear to be intended for another.³⁰ The ABA further warns that though the attorney

²⁵ Gray v. Bicknell, 86 F.3d 1472 (8th Cir. 1996).

²⁶ *Id.*

²⁷ In re Sealed Case, 676 F.2d 793 (D.C. Cir. 1982).

²⁸ Gray, at 1484.

²⁹ *Id.*

³⁰ ABA/BNA Lawyer's Manual of Professional Conduct, Opinion E-374 (Kentucky), Nov. 1995 1001:3905, 41. See also ABA/BNA Lawyer's Manual of Professional Conduct, Opinion 90 (Colorado), 1001:1902, Nov. 14, 1992, 34

should not be disciplined for use pursuant to a bona fide good faith belief that the privilege has been waived, he or she risks exclusion of the evidence as well as disqualification.³¹

Some issues are best avoided. Waiver through inadvertence is one of them. So many attorneys find it advisable to obtain informed client consent to use e-mail even in those jurisdictions in which it is not required. There are difficulties in even this simple solution. First, it is unresolved if this waiver amounts to a waiver of privilege, particularly in those minority states requiring written consent. Secondly, there may be a continuing duty to update the client as to changes in the law. Since the law is uncertain and changing this could prove burdensome. A confidentiality cover sheet on all e-mail, much like what is standard on fax transmissions is another option, though it may or may not be effective to avoid a waiver in the accidental disclosure situation. Encryption is another option, but it too has costs. There are some monetary costs in its purchase and time costs in its use. Also, a warning to those attorneys who travel abroad with their laptop computer - traveling out of the country with a laptop equipped with encryption software may be illegal.³²

The following is a brief description of four representative states' approaches to Internet communication. Note the irony that some authorities state that especially sensitive materials may require encryption. This in essence bases the finding of confidentiality on the content of the message, not the context in which it is made.

³¹ *Id.*

³² Codes and code-breaking were crucial to our victory in World War II, and now encryption products are still classified as "munitions." See George N. Grammas and Lisa M. Sotir, *Traveling with a Laptop May Land You in Trouble*, The National Law Journal C01 (Feb. 2, 1998) available at <http://www.ljx.com/securitynet/articles.0202laptop.html>. See also, 22 U.S.C. § 2778 and 22 CFR § 123.1. 22 U.S.C. § 2778(c) provides for criminal sanctions for a willful violation of the export laws and regulations.

ARIZONA:³³

The Arizona State Bar Committee on Rules of Professional Conduct has strongly cautioned attorneys of the dangers of Internet use.³⁴ A confidentiality statement at a minimum is required. This should read similarly to the standard fax cover sheet. Encryption is also mentioned as a possible option, but it is not required.

KENTUCKY:³⁵

Kentucky has recently adopted what might be called the majority rule except that Ethic Op E-403 strongly favors Illinois Opinion 96-10 (1997) and incorporates it as an appendix. This Illinois opinion analogizes the Internet to land-based telephone communications, to the point of stating "a home page is the functional equivalent of a 'yellow pages' entry." Though this means that e-mail need not be encrypted except in "unusual circumstances," it may overstate the security of the Internet.³⁶

³³ See ABA/BNA Lawyers' manual on Professional Conduct, Current Reports, vol. 13, 125 (May 14, 1997), for a synopsis of Arizona State Bar Committee on Rule of Professional Conduct, Opinion 97-04, (April 7, 1997).

³⁴ *Id.*

³⁵ Ky. Bar Ass'n Ethics Comm., Formal Op. E-403.

³⁶ This analogy does have the interesting effect of turning an impersonal, even anonymous chat room conversation into a telephone call. This strongly suggests the formation of an attorney-client relationship. The Illinois opinion states that participation in an on-line service involving the giving of "personalized legal advice" leads to the recipient becoming the attorney's client.

PENNSYLVANIA:³⁷

An attorney must take appropriate measures to guard the confidentiality of the client. Extraordinary measures are not required for ordinary messages. Tighter security is required only when the circumstances demand it, encryption is not required for most communications. The attorney fulfills his or her obligations if the client consents after being informed of the risks by the attorney.

DISTRICT OF COLUMBIA:³⁸

The District of Columbia attorney is not required to encrypt e-mail to comply with Model Rule 1.6 governing confidentiality. Citing the fact that the balance of authorities find the e-mail is acceptable and the ECPA, the D.C. Ethics Committee finds that there is a reasonable expectation of privacy on the Internet. Thus, encryption is unnecessary except in the presence of "special factors" which require it. These factors would include extraordinary sensitivity of the materials or other circumstances demanding higher security.

³⁷ Pa. Bar Ass'n Comm. on Legal Ethics and Prof. Responsibility 97-130 (Sept. 26, 1997), acknowledging the lack of consensus on the dangers of unencrypted e-mail.

³⁸ ABA/BNA Lawyer's Manual of Professional Conduct, Current Reports, vol. 14, 256, (June 12, 1998) *citing* District of Columbia Bar Legal Ethics Comm., Op. 281 (February 12, 1998, released May, 15, 1998).

Part III. Advertising and Solicitation.

The consensus on Internet advertising is that it must conform to the applicable rules regarding the use of public media.³⁹ The rules vary by jurisdiction, but there are some key considerations to consider before advertising on the Internet or giving on-line advice.

First, avoid the unauthorized practice of law. The Internet makes distance unimportant, and in the process attorneys may forget that they are not licensed everywhere. A strong disclaimer clearly identifying the license limitations of a firm should be used on any web page.⁴⁰ Whatever is said regarding areas of practice and licensing must also conform to the Rules and any mandatory disclosures must be made.⁴¹ A related consideration is that the rules regarding solicitation. Recently, a massive e-mail solicitation lead to the suspension of a Tennessee attorney.⁴² However, in at least one instance, an unsolicited posting on Internet news groups advertising for two immigration attorneys went unpunished.⁴²

Another consideration is that an on-line contact can lead to the inadvertent formation

³⁹ See ABA/BNA Lawyers' Manual on Professional Conduct, Current Reports, vol. 13, 125, discussing Az. State Bar Comm. on Rules of Prof. Conduct, Op. 97-04 (April 7, 1997); Pa. Bar Ass'n Comm. on Legal Ethics and Prof. Responsibility, Informal Op. 96-17 (May 3, 1996), 1996 WL 928126; See also, Jefferey R. Kuester, *Attorney Sites Can Avoid Violations of Ethics Rules*, 18 Special to the Nat'l L. J. B11, (August 12, 1996) available at <http://www.computerbar.org/netethics/nlj.htm>.

⁴⁰ See Pa. Op. 96-17, *id.* For sample disclaimers visit: <http://www.brobeck.com> (Brobeck, Phleger & Harrison); or <http://www.andersonkill.com> (Anderson, Kill & Olick).

⁴¹ See ABA/BNA Lawyers' Manual on Professional Conduct, Current Reports, vol. 12, 314 (Sept. 18, 1996) discussing Iowa Supreme Ct Brd of Prof. Ethics and Conduct, Formal Op. 96-1 (Aug. 29, 1996).

⁴² Joan C. Rogers, *How do Advertising Rules Apply to Lawyers on the 'Net*, ABA/BNA Lawyers' Manual on Professional Conduct, Current Reports, vol. 12, 37. Unsolicited advertising is a breach of on-line etiquette, called netiquette.

of an attorney client relationship with all its attendant duties and responsibilities. This can lead to malpractice liability. It should also be noted that attorney client privilege can attach to prospective clients as well as actual ones.⁴³ This can pose difficulties in the anonymous on-line world. Some ethics committees advise that before answering questions in a chat room an attorney should inquire if the recipient is represented.⁴⁴

There are some ethics opinions permitting lawyer referral services so long as they are not misleading.⁴⁵ Further, links between a client's home page and the attorney's are permissible so long as the attorney did not ask for it and the client is not compensated for it.⁴⁶ An attorney or law firm may list clients on its own web page so long as it obtains prior written consent.⁴⁷

Part IV. Conclusion.

Traditional rules on advertising and solicitation can answer most of the questions associated with web pages, e-mail soliciting, and on-line referral services. But answers are

⁴³ Lovell v. Winchester, 941 S.W.2d 466, (Ky. 1997) citing Ky. R. Evid. 503(a)(1).

⁴⁴ Peter Krakaur, *the Ethics of Giving Casual Legal Advice On-line*, The Internet Newsletter, http://www.ljx.com/newsletters/internet/1998/1998_05_00.html.

⁴⁵ ABA/BNA Lawyers' Manual on Professional Conduct, Current Reports, vol. 13, 42 (March 5, 1997); Note however, that for-profit referral services are not permitted: ABA/BNA Lawyers' Manual on Professional Conduct, Ethics Opinions 1991-1995, 1001-3901, Kentucky Bar Ass'n Ethics Comm., Op. E-344 (March 1991); other states require that the referral service be approved, State Bar of Arizona, Bar Comm. on Rules of Prof. Conduct, Op. 98-03, (January 1998).

⁴⁶ ABA/BNA Lawyers' Manual on Professional Conduct, Current Reports, vol. 13, 235, (Aug. 6, 1997) discussing Cincinnati Bar Ass. Ethics and Prof. Responsibility Comm., Op. 96-97-01.

⁴⁷ *Id.*

not so easy concerning the use of the Internet as a communications tool. This lack of concrete answers makes the most frequently asked question "should I encrypt?" Because the mere use of Internet e-mail may lead to a waiver of the attorney client privilege on matters involved in the on-line communication, one is well advised to inform clients of the dangers and at the very least offer the option of encryption. Though opinions vary on the issue of whether or not there is a reasonable expectation of privacy when using the Internet, and whether or not there is an ethical duty to protect a client's confidence with encryption, attorneys owe it to their clients to minimize the risks of litigating additional issues. Encryption can prevent the inadvertent disclosure problem; it can avoid disputes over privilege; it can minimize the risks of spoofing. On the whole, saving the time and expense of litigation and giving clients additional security may simply make encryption the best option.

**INTERNET / E-MAIL PRIVACY ISSUES; ENCRYPTION
AND ELECTRONIC ESPIONAGE**

CRIMINAL LAW PERSPECTIVE

David J. Beyer
Chief Division Counsel
Federal Bureau of Investigation
Louisville, Kentucky

SECTION K(b)

**INTERNET / E-MAIL PRIVACY ISSUES; ENCRYPTION
AND ELECTRONIC ESPIONAGE**

CRIMINAL LAW PERSPECTIVE

TABLE OF CONTENTS

I.	INTRODUCTION	K(b)-1
II.	PRIVACY AND U.S. CONSTITUTIONAL PROTECTIONS	K(b)-1
	A. Generally	K(b)-1
	B. First Amendment	K(b)-2
	C. Third Amendment	K(b)-2
	D. Fourth Amendment	K(b)-2
	E. Fifth Amendment	K(b)-3
III.	PRIVACY AND STATUTORY PROTECTIONS	K(b)-3
	A. Privacy Protection Act	K(b)-3
	B. Omnibus Crime Control Act Of 1968 (Title III)	K(b)-3
	C. Pen Register And Trap And Trace Devices	K(b)-4
	D. Stored Wire And Electronic Communications	K(b)-4
IV.	COMPUTER CRIMES	K(b)-5
	A. Fraud And Related Activity In Connection With Computers	K(b)-5
	B. Fraud By Wire	K(b)-6
	C. Internet And Sexual Exploitation Of Children	K(b)-7
	D. Material Involving Sexual Exploitation Of Children	K(b)-7
	E. Trafficking In Copies Of Computer Programs	K(b)-7
V.	ENCRYPTION ISSUES	K(b)-7
	A. Balancing Of Interest	K(b)-7
	B. Need For Encryption	K(b)-7
	C. Maintaining Status Quo	K(b)-8
	D. Recent Examples	K(b)-8
	E. Pending Legislation	K(b)-8
VI.	ADDITIONAL RESOURCES	K(b)-8



**INTERNET/E-MAIL PRIVACY ISSUES;
ENCRYPTION; ELECTRONIC ESPIONAGE
CRIMINAL LAW PERSPECTIVE**

Presented By:

David J. Beyer
Chief Division Counsel
Federal Bureau of Investigation
Louisville, Kentucky

I. Introduction

The tremendous expansion in the use of computers, E-mail, and the Internet by individuals, businesses, governmental entities has created a plethora of complex legal issues for lawyers, courts and law enforcement agencies who seek to apply existing statutory and caselaw to rapidly changing technology. Congress has been in the forefront of enacting laws to address many of the emerging issues. The courts are beginning to define the hazy contours of this embryotic area of the law. Meanwhile legal scholars, privacy rights advocates and law enforcement agencies have begun to grapple with the competing interests of public safety and privacy of electronic communications.

II. Privacy and U.S. Constitutional Protections

A. Generally

1. Right of Privacy not specifically mentioned
2. Found within the penumbras See Griswold v. Connecticut, 381 U.S. 479 (1965)
3. Virtually every governmental action interferes with personal privacy to some degree. The question in each case is whether that

interference violates a command of the United States Constitution .

- B. First Amendment - Imposes limitations upon governmental abridgment of freedom to associate and privacy in one's associations. NAACP v. State of Alabama, 357 U.S. 449 (1958)
- C. Third Amendment - Prohibition against the unconsented peacetime quartering of soldiers protects another aspect of privacy from governmental intrusion. Katz v. U.S. 389 U.S. 347, 350 (1967)
- D. Fourth Amendment - "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated...."
 - 1. Fourth Amendment cannot be translated into a general constitutional "right to privacy." That Amendment protects individual privacy against certain kinds of governmental intrusion, but its protections go further, and often have nothing to do with privacy at all. Katz v. U.S., 389 U.S. at 350
 - 2. Fourth Amendment protects those items or areas where a reasonable expectation of privacy (REP) exists. Katz
 - 3. REP does not extent to areas a person knowingly opens to public access. See Oliver v. United States, 466 U.S. 170 (1984)
 - a. Computer "banner" inviting all but law enforcement agents to use a system is unlikely to be considered sufficient to create REP;

- b. Cf Consent - Business computer network banner that states information on system is not considered private and use of system constitutes consent of system operator to review any information on the system. See Bumpers v. North Carolina, 391 U.S. 543 (1968)

- E. Fifth Amendment - Reflects the Constitution's concern for the right of each individual to a private enclave where he may lead a private life. See Tehan v. United States ex rel. Shott, 382 U.S. 406 (1966)

III. Privacy and Statutory Protections

A. Privacy Protection Act - 42 U.S.C. §2000aa

- 1. Result of Supreme Court decision in Zurcher v. Stanford Daily, 436 U.S. 547 (1978) - Use of search warrant permitted on both non-suspect third parties and the media.
- 2. Purpose of statute is to limit searches for materials held by persons involved in First Amendment activities who are themselves not suspected of participation in criminal activity.
- 3. Not to limit ability of law enforcement to search for and seize materials held by those suspected of committing crimes.
See S. Rep. No. 874, 96th Cong. 2d Sess. 4 (1980)

B. Omnibus Crime Control Act of 1968 (Title III) - 18 U.S.C. 2510 - 2522

- 1. Generally prohibits the interception of wire, oral or electronic communications unless one party to communication provides consent.

2. Applies to communications in transit - not applicable stored to communications .
3. Government must obtain court order to intercept.
 - a. Requires showing of probable cause that:
 - (1) Crime has been, is being, or is about to be committed:
 - (2) Facility being used to discuss same; and
 - (3) Other investigative techniques have been tried and failed or reasonably appear unlikely to succeed or too dangerous. See 18 U.S.C. 2518

C. Pen Register and Trap and Trace Devices - 18 U.S.C. 3121 - 3127

1. Pen Register - Records electronic impulses produced when phone is dialed.
2. Trap and Trace - Captures incoming electronic impulses which identify originating number of person calling.
3. Both require court order authorizing installation upon showing of relevancy to ongoing criminal investigation.

D. Stored Wire and Electronic Communications - 18 U.S.C. 2701 - 2711

1. Prohibits public electronic communication services and public remote computing services from disclosing contents of any communication maintained by the service.
2. Exceptions -
 - a. May disclose to addressee or intended recipient; or

- b. Consent of originator or addressee.
- 3. Governmental Access - 18 U.S.C. 2703
 - a. Contents of electronic communication in electronic storage
 - (1) 180 days or less - Search warrant (probable cause)
 - (2) More than 180 days -
 - (a) Search warrant - no notice required
 - (b) Subpoena - notice required¹
 - (c) Court order - notice required
 - b. Contents of electronic communication in a remote computing service - Same as a.(2) above.
- 4. Congress did not intend for "intercept" in Federal Wiretap Act to apply to "electronic communication" when those communications are in "electronic storage." Steve Jackson Games, Inc. v. United States Secret Service, 36 F. 3d 457 (1994)

IV. Computer Crimes

A. Fraud and Related Activity in Connection with Computers - 18 U.S.C.

1030

- 1. **1030 (a)(1)** - Prohibits knowingly accessing a computer without authorization or exceeding authorization and obtaining national defense or foreign relation information [1st offense - 10 years; 2nd offense - 20 years].
- 2. **1030 (a)(2)** - Prohibits intentionally accessing a computer without

¹ Government may request court to permit delayed notice.

authorization or exceeding authorization and obtaining information from:

- a. A financial institution;
 - b. Department or Agency of United States; or
 - c. Any computer if conduct involved interstate communication [1st offense - 1 year, but if for commercial advantage or private gain, then 5 years; 2nd offense - 10 years].
3. **1030 (a)4** - Prohibits knowingly and with the intent to defraud, accessing a computer without authorization or exceeding authorization and by such conduct obtains anything with value of \$5,000 or more [1st offense - 5 years; 2nd offense - 10 years].
 4. **1030(a)(5)** - Prohibits knowingly causing the transmission of a program, code or command which causes damage to a computer [1st offense up to 5 years; 2nd offense - 10 years].
 5. **1030(a)(6)** - Prohibits trafficking in password or other information through which a computer may be accessed [1st offense - 1 year; 2nd offense - 10 years].
 6. **1030(a)(7)** - Prohibits transmitting in interstate commerce any threat to cause damage to a computer with the intent to extort [1st offense - 5 years; 2nd offense - 10 years].

B. Fraud by Wire - 18 U.S.C. 1343

1. Prohibits devising a scheme to defraud or for obtaining property by means of false pretenses and transmitting or causing to be

transmitted any communication in interstate commerce for the purpose of executing the scheme [Penalty fine + 5 years; if scheme involves financial institution - up to 30 years and \$1 million fine].

C. Internet and Sexual Exploitation of Children - 18 U.S.C. 2251

1. Prohibit inducing or coercing a minor to be transported in interstate commerce with the intent to engage in sexual conduct for the purpose of producing a visual depiction of such conduct [1st offense 10-20 years; 2nd offense 15-30 years; 3rd offense 30 - life; if death results - death penalty may be imposed].

D. Material Involving Sexual Exploitation of Children - 18 U.S.C. 2252

1. Prohibits person from knowingly transporting in interstate commerce, including by computer, any visual depiction involving the use of a minor engaging in sexual conduct [1st offense up to 15 years; if prior convictions, then no less than 5 years up to 30 years].

E. Trafficking in Copies of Computer Programs - 18 U.S.C. 2318

1. Prohibits knowingly trafficking via interstate commerce in a copy of a computer program or documentation or packaging for a computer program [5 years + fine].

V. Encryption Issues

A. Balancing of Interest

1. Commercial and personal privacy interest
2. Public Safety and National Security

B. Need for encryption

- C. Maintaining status quo
- D. Recent examples
- E. Pending Legislation

VI. Additional resources

- A. "Computer Crimes," 34 Am. Crim. L. Rev 409 (1997)
- B. "Old Wine in New Bottles: Cyberspace and the Criminal Law", 41 Jun B. B.J. 12 (1994)
- C. "Computer Crime," 45 Emory L.J. 931 (1996)
- D. "Computer Crime; Law Enforcement's Shift from a Corporeal Environment to the Intangible, Electronic World of Cyberspace," 41 Fed. B. News & J. 489, 494 (1994)

**ETHICAL AND PROFESSIONAL RESPONSIBILITY
CONCERNS ARISING FROM THE USE OF TECHNOLOGY
IN THE PRACTICE OF LAW**

Kurt X. Metzmeier
Shaun E. Esposito
University of Kentucky
College of Law

Copyright 1999, Kurt X. Metzmeier, Shaun E. Esposito. All Rights Reserved.

SECTION L



**ETHICAL AND PROFESSIONAL RESPONSIBILITY CONCERNS ARISING FROM
THE USE OF TECHNOLOGY IN THE PRACTICE OF LAW**

TABLE OF CONTENTS

I. ETHICAL ISSUES RAISED BY THE USE OF E-MAIL IN THE PRACTICE OF LAW IN KENTUCKY	L-1
A. Why Use E-Mail?	L-1
B. Client Confidentiality: Issues	L-1
C. Encryption	L-1
D. Inadvertent Disclosure	L-1
1. Inadvertent Disclosure: Sample Warning Disclaimer	L-1
E. Disclosure By Nonlawyer Assistants	L-2
F. Disclosure By Nonlawyers Assistants: Preventative Measures For Nonlawyer Employees Including Information Systems Staff	L-2
G. Disclosure By Nonlawyer Assistants: Preventative Measures For Contract Employees And Consultants	L-2
H. Solicitation & Advertising	L-2
I. Solicitation Issues	L-2
J. Spam	L-2
K. Spam & Kentucky Rules Of Professional Conduct	L-3
L. Listservs	L-3
M. Listservs: Solicitation	L-3
N. Listservs: Establishment Of Attorney-Client Relations	L-3
O. Listservs: Avoiding The Establishment Of Attorney-Client Relations	L-3
P. Chatrooms	L-4
Q. Suggested Reading	L-4
II. APPENDIX	L-5
Appendix I: KBA E-403	L-7
Appendix II: Sample Forms	L-13
Appendix III: Password Protection Of Microsoft Word And Corel Word Perfect Documents	L-17
Appendix IV: Kurt Metzmeier & Shaun Esposito, <i>How to Avoid Losing Your License on the Information Superhighway: Ethical Issues Raised by the Use of the Internet in The Practice of Law</i> (Kentucky Bench & Bar, Spring 1998)	L-19
Appendix V: Web-Site Listing	L-29



Ethical Issues Raised by the Use of E-mail in the Practice of Law in Kentucky

Kurt X. Metzmeier
University of Kentucky College of Law
May 7, 1999

Why Use E-mail?

- More efficient than a form letter
- Provides more documentation than a phone call
- Clients will increasingly demand that lawyers use e-mail keep them abreast of their cases.

Client Confidentiality: Issues

- Encryption
- Inadvertent Disclosure
- Malicious or Negligent Disclosure by Non-lawyer Assistants

Encryption

- Not required (KBA E-403) "unless unusual circumstances require enhanced security measures"

Encryption

- Should be considered for highly sensitive communications
- PGP -- Difficult to configure
- Encryption of attached documents easier solution
 - Microsoft Word & Corel Word Perfect [see Appendix III]

Inadvertent Disclosure

- Mis-addressed e-mail far more serious likelihood than interception
- Prevention:
 - Avoid vague "nicknames"
 - Use warning/disclaimer

Inadvertent Disclosure: Sample Warning Disclaimer [See Appendix II.1]

This e-mail message, together with any attachments, is intended only for the personal and confidential use of the recipient(s) named above. This message may be an attorney-client communication and as such is privileged and confidential. If you are not the intended recipient, you are hereby notified that you have received this document in error and that any review, dissemination, distribution, or copying of this message is strictly prohibited. If you have received this message in error, please notify us immediately ... and delete the message from your computer.

Disclosure by Nonlawyer Assistants

- Computer security experts agree that the most serious risk for disclosure of confidential communications is through employee misconduct
- The most famous disclosure of client information in Kentucky, the Brown & Williamson case, occurred this way (though without computers)

Disclosure by Nonlawyer Assistants

- KRPC 5.3 requires that lawyers supervising nonlawyers “employed or retained by or associated with” a law practice have “in effect measures giving reasonable assurance” that these employees uphold the KRPC.
- Supervising attorneys have an ethical obligation to assure that **computing and networking staff** are trained as to the obligations of the KRPC, **especially** those relating to **client communications**

Disclosure by Nonlawyer Assistants: Preventative measures for nonlawyer employees including information systems staff

- Employee orientation
- Employee manuals [Appendix II.2]
- Computer use policies (for all employees) [Appendix II.3]

Disclosure by Nonlawyer Assistants: Preventative measures for contract employees and consultants

- Choosing reputable consultants with strong references
- Contractual language incorporating confidentiality assurances

Solicitation & Advertising

- “Unless the lawyer uses the Internet or other electronic mail service to direct messages to a specific recipient [in which case the rules governing solicitation would apply] only the general rules governing communications regarding a lawyer's services and advertising [KRPCs 7.10, 7.20, and the so-called advertising rules set forth at KRPCs 7.01-7.08] should apply...” (KBA E-403)

Solicitation Issues

- Mass mailings (Spam)
- Lawyer participation in listservs
- Lawyer participation in “chat rooms”

Spam

- Unsolicited commercial e-mail
- Disliked by both e-mail users and Internet Service Providers (ISP's)
- CompuServe has successfully sued commercial e-mailers under theory that they

abused computer facilities owned by the ISP

Spam & the KRPC

Shapiro v. KBA, 486 US 466 (1986)

- KRPC 7.30 bars all solicitation when
 - (2)(a) client makes desire known that he or she does not want it
 - (2)(b) it involves coercion, duress or harassment
- (3) Written solicitation must follow 7.10 advertising rules
- By using what the Internet community considers in an abusive and harassing means of communications, legal services solicitation by spam appears to fall outside the spirit of the KRPC as "conduct that is prejudicial to the administration of justice." (KRPC 8.4(e)).
- Tennessee in **In Re Canter**, No. 95-831-O-H (2-25-1997) suspended an attorney for one year under this theory, citing DR 1-102(A)(5), which is analogous to KRPC 8.4(e). *But see* NYSBA Ethics Opinion 709 (9-16-1998).

Listservs

- Listserv is a server that distributes e-mails to all list members
- Members post public messages to entire list
- Only limited anonymity
- *Very valuable tool for keeping up on breaking developments*

Listservs

- The participation of lawyers on listservs raise a number of issues:
 - Solicitation
 - Inadvertent creation of an attorney-client relationship
 - Unauthorized practice of law (in jurisdictions where they are not licensed)

Listservs: Solicitation

- KRPC 7.02(1)(f) states that: "Any communication by a lawyer to third parties that is published or broadcast by a third party who is not in any way controlled by the lawyer, and for which publication or broadcast the lawyer pays no consideration, shall be exempt from all the provisions of these Rules except Rule 7.10 [barring "false, deceptive or misleading" information]."
- The participation by lawyers on listservs maintained by third parties is consistent with KRPC 7.02(1)(f) and KBA opinions regarding appearances by lawyers on radio and TV programs (KBA E-50, E-270).

Listservs: Establishment of an Attorney-Client Relations

- Will turn on what the "client" reasonably perceives
- Lawyers should be wary of seeming to respond to specific questions

Listservs: Avoiding the Establishment of an Attorney-Client Relations

- Include disclaimer in signature line [**Appendix II.4**]

- Lawyers should avoid going “off-list” to discuss specific problems
- Seek out “lawyer’s only lists”
- Avoid lists where non-lawyers tend to trade in bad legal advice

Chat Rooms

- Forums for anonymous, real-time discussion
- Regularly exercised option to take public discussions private
- Hosted by users ISP (traditionally AOL strength) or by free websites like Yahoo!
- While none of the published state opinions on the use of e-mail specifically bar attorney’s from participating (as lawyers) in chat rooms, the atmosphere of anonymity and privacy intensifies the dangers suggested for listserv participation.

Suggested Reading

- Peter Krakaur’s www.legaethics.com
- Paul D. Shaw, *Managing Legal and Security Risks in Computing* (1998)
- David J. Icové, *Computer Crime: A Crime Fighters Handbook* (1995)

APPENDIX

- Appendix I: KBA E-403**
- Appendix II: Sample Forms**
- Appendix III: Password Protection Of Microsoft Word
And Corel Word Perfect Documents**
- Appendix IV: Kurt Metzmeier & Shawn Esposito, *How to Avoid
Losing Your License on the Information
Superhighway: Ethical Issues Raised by the Use of the
Internet in The Practice of Law*
(Kentucky Bench & Bar, Spring 1998)**
- Appendix V: Web-Site Listing - Addendum To Metzmeier &
Esposito, *How to Avoid Losing Your License on
the Information Superhighway: Ethical Issues
Raised by the Use of the Internet in the Practice
Of Law* (Kentucky Bench & Bar, Spring 1998)**

KBA E-403

Question 1:

May a lawyer use electronic mail services including the Internet to communicate with clients without encryption?

Answer:

Yes, unless unusual circumstances require enhanced security measures.

Question 2:

Is the creation and use by a lawyer of an Internet "web site" containing information about the lawyer and the lawyer's services that may be accessed by Internet users, including prospective clients, a communication falling within KRPCs 7.09 [Prohibited Solicitation] or 7.30 [Direct Contact With Prospective Client]?

Answer:

Qualified No. Unless the lawyer uses the Internet or other electronic mail service to direct messages to a specific recipient [in which case the rules governing solicitation would apply] only the general rules governing communications regarding a lawyer's services and advertising [KRPCs 7.10, 7.20, and the so-called advertising rules set forth at KRPCs 7.01-7.08] should apply to a lawyer's "web-site" on the Internet.

References: Illinois Op. 96- 10 (1997); Kurt Metzmeier & Shaun Esposito, How to Avoid Losing Your License on the Information Superhighway: Ethical Issues Raised by the Use of the Internet in The Practice of Law (*Kentucky Bench & Bar*, Spring 1998).

OPINION

Despite widespread use of the Internet, the Committee has received few inquiries regarding its use. Still, the Committee is of the view that this opinion should be issued to provide some guidance and some comfort. The subject is addressed in a recent article cited in the references, which is available from the UK Law Library, and which has been submitted for publication in the *Bench & Bar*.

The Committee finds persuasive the comprehensive and thoughtful opinion of the Illinois State Bar Association, ISBA Advisory Opinion No. 96-10, excerpts of which we attach as an Appendix.

APPENDIX

ILLINOIS STATE BAR ASSOCIATION

ISBA Advisory Opinion on Professional Conduct

Opinion No. 96-10

May 16, 1997

Topic: Electronic communications; confidentiality of client information; advertising and solicitation.

Digest: Lawyers may use electronic mail services, including the Internet, without encryption to communicate with clients unless unusual circumstances require enhanced security measures. The creation and use by a lawyer of an Internet "web site" containing information about the lawyer and the lawyer's services that may be accessed by Internet users, including prospective clients, is not "communication directed to a specific recipient" within the meaning of the rules, and therefore only the general rules governing communications concerning a lawyer's services and advertising should apply to a lawyer "web site" on the Internet. If a lawyer uses the Internet or other electronic mail service to direct messages to specific recipients, then the rules regarding solicitation would apply. Ref.: Illinois Rules of Professional Conduct, Rules 1.6, 7.1, 7.2, 7.3 and 7.4
ISBA Opinion Nos. 90-07 and 94-11
Electronic Communications Privacy Act, 18 USC §2510, et seq.

QUESTIONS

The Committee has received various inquiries regarding ethical issues raised by use of electronic means of communication, including electronic mail and the "Internet," by lawyers. These inquiries usually involve two general areas of concern. The first is whether electronic mail may be used to communicate with clients regarding client matters in view of a lawyer's duty under the ethics rules to maintain the confidentiality of client information. The second is whether the creation and use of a "web site" and other forms of contact with prospective clients may be conducted by lawyers on the Internet, and if so, whether the rules regarding "in person" solicitation should apply to such contact. Because of the technical nature of the discussion, the Committee will use the following commonly accepted definitions in this opinion. The Internet is a super network of computers that links together individual computers and computer networks located at academic, commercial, government and military sites worldwide, generally by ordinary local telephone lines and long-distance transmission facilities. Communications between computers or individual networks on the Internet are achieved throughout the use of standard, nonproprietary protocols.

Electronic mail, commonly known as e-mail, is an electronic message that is sent from one computer to another, usually through a host computer on a network. E-mail messages can be sent through a private or local area network (within a single firm or organization), through an electronic mail service (such as America Online, CompuServ or MCI Mail), over the Internet, or through any combination of these methods.

A bulletin board service (sometimes called a "BBS") is an electronic bulletin board on a network where electronic messages may be posted and browsed by users or delivered to e-mail boxes. A "newsgroup" is a type of bulletin board service in which users can exchange information on a particular subject. A "chat" group is a simultaneous or "real time" bulletin board or newsgroup among users who send their questions or comments over the Internet.

The World Wide Web is that part of the Internet consisting of computer files written in a particular format (the "HTML" format) that includes "hyperlinks" (text or symbols that the user may click on to switch immediately to the item identified) as well as graphics

and sound, to enable the creation of complex messages. A "home page" is a computer file containing text and graphics in the HTML format usually containing information about its owner, which can be obtained over the Internet and viewed by transmitting it from the owner's computer to the user's terminal. A "web site" is a set of computer files containing text and graphics in the HTML format and organized around a central home page. The Electronic Communications Privacy Act, 18 USC §2510, et seq. (the "ECPA"), is the federal codification of the intrusion arm of the common law tort of invasion of privacy applied to electronic communication and provides criminal and civil penalties for its violation. The ECPA is actually the 1986 revision of the federal wiretap statute originally enacted in 1968, but the term ECPA is now commonly used to refer to the entire statute, as amended.

OPINION

The first issue, whether a lawyer may use electronic mail services including the Internet to communicate with clients, arises out of a lawyer's duty to protect confidential client information. Rule 1.6(a) of the Illinois Rules of Professional Conduct provides that "...a lawyer shall not, during or after termination of the professional relationship with the client, use or reveal a confidence or secret of the client known to the lawyer unless the client consents after disclosure." AS the Terminology provisions of the Rules state, the information a lawyer must protect includes information covered by the lawyer-client privilege (a "confidence") as well as information that the client wishes to be held inviolate or the revelation of which would be embarrassing or detrimental to the client (a "secret").

The duty to maintain the confidentiality of client information implies the duty to use methods of communication with clients that provide reasonable assurance that messages will be and remain confidential. For that reason, the Committee concluded in Opinion No. 90-07 (November 1990) that a lawyer should not use cordless or other mobile telephones that were easily susceptible to interception when discussing confidential client matters. The Committee also opined that a lawyer conversing with a client over a cordless or mobile telephone should advise the client of the risk of the loss of confidentiality.

With the increased use of electronic mail, particularly electronic mail transmitted over the Internet, have come suggestions that electronic messages are not sufficiently secure to be used by lawyers communicating with clients. At least two state ethics opinions have concluded that because it is possible for Internet or other electronic mail service providers to intercept electronic mail service providers to intercept electronic mail messages, lawyers should not use electronic mail for "sensitive" client communications unless the messages were encrypted or the client expressly consented to "non-secure" communication. South Carolina Bar Advisory Opinion 94-27 (January 1995); Iowa Supreme Court Board of Professional Ethics and Conduct Opinion 96-1 (August 29, 1996). After reviewing much of the available literature on this issue, the Committee disagrees with these opinions.

Among the numerous recent articles regarding a lawyer's use of electronic mail, the Committee found three to be particularly useful and informative. These are: Joan C. Rogers, "Malpractice Concerns Cloud E-Mail, On-Line Advice," ABA/BNA Lawyers' Manual on Professional Conduct (March 6, 1996); Peter R. Jarvis & Bradley F. Tellam, "High-Tech Ethics and Malpractice Issues," 1996 Symposium Issue of the Professional Lawyer, p. 51 (1996); David Hricik, "Confidentiality and Privilege in High-Tech Communications," 8 Professional Lawyer, p. 1 (February 1997). From these and other authorities, there is a clear consensus on two critical points. First, although interception of electronic messages is possible, it is certainly no less difficult than intercepting an ordinary telephone call. Second, intercepting an electronic mail message is illegal under the ECPA.

Courts and ethics committees have uniformly held that persons using ordinary telephones for confidential communications have a reasonable expectation of privacy. The three common types of electronic mail messages appear no less secure. For example, electronic messages that are carried on a local area or private network may only be accessed from within the organization owning the network. Such messages would therefore clearly appear subject to a reasonable expectation of privacy.

Other electronic messages are carried by commercial electronic mail services or networks such as America Online, CompuServ or MCI Mail. Typically, these services transmit e-mail messages from one subscriber's computer to another computer "mailbox" over a proprietary telephone network. Typically, the computer mailboxes involved are password-protected. Because it is possible for dishonest or careless personnel of the mail service provider to intercept or misdirect a message, this form of electronic mail is arguably less secure than messages sent over a private network. AS a practical matter, however, any ordinary telephone call may also be intercepted or misdirected by dishonest or careless employees of the telephone service provider. Again, this possibility has not compromised the reasonable expectation of privacy of ordinary telephone users. The result should be the same for electronic mail service subscribers.

The third type of electronic mail, that carried on the Internet, typically travels in another fashion. Rather than moving directly from the sender's host computer to the recipient's host computer, Internet messages are usually broken into separate "packets" of data that are transmitted individually and then re-assembled into a complete message at the recipient's host computer. Along the way, the packets travel through, and may be stored temporarily in, one or more other computers (called "routers") operated by third parties (usually called an "internet service provider" or "ISP") that help distribute electronic mail over the Internet.

Unlike a cordless cellular telephone message, for example, an Internet e-mail is not broadcast over the open air waves, but through ordinary telephone lines and the intermediate computers. When an Internet message is transmitted over an ordinary telephone line, it is subject to the same protections and difficulties of interception as an ordinary telephone call. To intercept an Internet communication while it is in transit over telephone lines requires an illegal wiretap.

Consequently, the real distinction between an Internet electronic message and an ordinary telephone call is that Internet messages may be temporarily stored in, and so can be accessed through, a router maintained by an ISP. It is possible that an employee of an ISP (as part of the maintenance of the router) could lawfully monitor the router and thereby read part or all of a confidential message. As in the case of telephone and proprietary electronic mail providers, it is also possible for dishonest employees of an ISP to intercept messages unlawfully. The Committee does not believe that the opportunity for illegal interception by personnel of an ISP makes it unreasonable to expect privacy of the message.

As noted above, it is also clear that unauthorized interception of an Internet message is a violation of the ECPA, which was amended in 1986 to extend the criminal wiretapping laws to cover Internet transmissions. As part of the 1986 amendments, Congress also treated the issue of privilege in 18 USCA §2517(4), as follows:

No otherwise privileged wire, oral, or electronic communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character.

This provision demonstrates that Congress intended that Internet messages should be considered privileged communications just as ordinary telephone calls.

In summary, the Committee concludes that because (1) the expectation of privacy for electronic mail is no less reasonable than the expectation of privacy for ordinary telephone calls, and (2) the unauthorized interception of an electronic message subject to the ECPA is illegal, a lawyer does not violate Rule 1.6 by communicating with a client using electronic mail services, including the Internet, without encryption. Nor is it necessary, as some commentators have suggested, to seek specific client consent to the use of unencrypted e-mail. The Committee recognizes that there may be unusual circumstances involving an extraordinarily sensitive matter that might require enhanced security measures like encryption. These situations would, however, be of the nature that ordinary telephones and other normal means of communication would also be deemed inadequate.

With respect to the second general issue, the extent to which a lawyer may use Internet web site to communicate with clients and prospective clients, the Committee believes that the existing Rules of Professional Conduct governing advertising, solicitation and communication concerning a lawyer's services provide adequate and appropriate guidance to a lawyer using the Internet. For example, the Committee views an Internet home page as the electronic equivalent of a telephone directory "yellow pages" entry and other material included in the web site to be the functional equivalent of the firm brochures and similar materials that lawyers commonly prepare for clients and prospective clients. An Internet user who has gained access to a lawyer's home page, like a yellow pages user, has chosen to view the lawyer's message from all the messages available in that medium. Under these circumstances, such materials are not a "communication directed to a specific recipient" that would implicate Rule 7.3 and its provisions governing direct contact with prospective clients. Thus, with respect to a web

site, Rule 7.1, prohibiting false or misleading statements concerning a lawyer's services, and Rule 7.2, regulating advertising in the public media, are sufficient to guide lawyers and to protect the public.

On the other hand, lawyer participation in an electronic bulletin board, chat group, or similar service, may implicate Rule 7.3, which governs solicitation, the direct contact with prospective clients. The Committee does not believe that merely posting general comments on a bulletin board or chat group should be considered solicitation. However, if a lawyer seeks to initiate an unrequested contact with a specific person or group as a result of participation in a bulletin board or chat group, then the lawyer would be subject to the requirements of Rule 7.3. For example, if the lawyer sends unrequested electronic messages (including messages in response to inquiries posted in chat groups) to a targeted person or group, the messages should be plainly identified as advertising material.

Finally, lawyers participating in chat groups or other on-line services that could involve offering personalized legal advice to anyone who happens to be connected to the service should be mindful that the recipients of such advice are the lawyer's clients, with the benefits and burdens of that relationship. In Opinion No. 94-11 (November 1994), the Committee addressed an analogous situation arising out of a "call-in" legal advice service as follows:

The committee believes that callers to the legal advice service are clients of the law firm who are entitled to the protection of clients afforded by the Rules of Professional Conduct. However, it does not appear that either the law firm or the cellular telephone service makes any effort to determine the identity of the callers and check for potential conflicts of interest prior to the time that the callers' questions are asked and the legal advice is given. (Presumably the callers' identities are revealed after the advice is rendered through the billing process. If the cellular telephone company handles the billing for the law firm, this procedure may also violate client confidences. See ISBA Opinion No. 93-04) Under these circumstances, it would be possible for the law firm to give legal advice to callers whose interest are directly adverse to other firm clients, including other callers, in violation of Rule 1.7(a), or whose interests are materially adverse to the firm's former clients, including other callers, concerning the same or a substantially related matter, in violation of Rule 1.9

Lawyers participating in similar activity over the Internet would be subject to the same concerns expressed in Opinion No. 94-11.

For these reasons, the Committee believes that Illinois lawyers may appropriately make use of the Internet in serving and communicating with clients and prospective clients subject to the existing rules governing confidentiality, advertising and solicitation.

II-1. Confidentiality Warning Disclaimer for E-mail Signature

This e-mail message, together with any attachments, is intended only for the personal and confidential use of the recipient(s) named above. This message may be an attorney-client communication and as such is privileged and confidential. If you are not the intended recipient, you are hereby notified that you have received this document in error and that any review, dissemination, distribution, or copying of this message is strictly prohibited. If you have received this message in error, please notify us immediately by telephone (555-555-5555) or by return e-mail and delete the message, along with any attachments, from your computer. Thank you.

II-2. Sample Warning to Computing Staff

The Rules of Professional Responsibility that bind all practicing lawyers in Kentucky make attorneys responsible for ensuring that these rules of ethical conduct are followed by the "non-lawyers" they employ. Therefore, *Gates, Jobs & Ellison* warns all employees upon their hiring that the willful violation of any ethical rule is grounds for immediate termination and that the firm will not rule out criminal or civil remedies for serious violations.

The most relevant of these rules is the rule barring the disclosure of any "client information," even information that would not be considered confidential to the layperson. The Kentucky Bar Association's Committee on Ethics has advised that even the unauthorized disclosure of the names of current and former clients violates this ethical trust.* Therefore, it is the firm policy of *Gates, Jobs & Ellison* to immediately terminate any employee who intentionally discloses any client information to persons not authorized to receive such information. It is the responsibility of the network administrators, desktop support specialists and all other computing personnel to not only personally adhere to this policy, but to ensure that all reasonable security measures are in place to ensure that client information is not disclosed.

*A widely used treatise of legal ethics notes that the "general obligation" under Rule 1.6 "gives rise to a number of duties." Charles W. Wolfram, *Modern Legal Ethics* §6.7.5 (1986). Among these duties is a duty "to see that the client's interest in full confidentiality of information is adequately protected. ... The lawyer's files should be confidentially maintained, and nonlawyer employees should be instructed, and periodically reminded, to keep all office matters strictly confidential." Generally, all client communications, even those that are not "confidences," fall under this general obligation. See, KBA E-253 (1981) (committee advised that even the very existence of an attorney-client relationship should be held confidential).

II-3. Sample Computer Use Policy

Preface

To protect the integrity of the computer system against unauthorized or improper use and to protect authorized users from the effects of unauthorized or improper usage of the system, the law firm of *Gates, Jobs & Ellison* reserves the rights to limit or restrict any account holder's usage, and to inspect or remove any data, file, or system resources which may undermine the authorized use of that system, without notice to the user. The Firm also reserves the right to periodically check the system and any other rights necessary to protect the Firm's computer facilities.

Users of the Firm's facilities are required to comply with the Computer Use Policy, and by using the system, the user agrees to comply with and be subject to the Policy and these Conditions of Use. Serious violations of the Policy by nonlawyer employees are subject to immediate termination. Attorney-employees are also subject to dismissal or severance of the partnership relationship.

The Firm reserves the right to amend this statement at any time with or without notice.

Computer Use Policy

1. You must use only those computer accounts, files or directories that have been authorized for your use. The unauthorized use of another's account, files or directories, as well as the providing of false or misleading information for the purpose of obtaining access to computing facilities, is strictly prohibited and may be regarded as grounds for immediate termination of employment.
2. You may not authorize anyone to use your account for any reason. You are responsible for all usage on your account(s). You must take all reasonable precautions, including password maintenance and file protection measures, to prevent use of your accounts by unauthorized persons.
3. You must use your accounts only for the purposes for which they were authorized. Firm accounts must not be used for private consulting or any other commercial use without prior approval from the Managing Attorney. You must not use your accounts for unlawful purposes, such as the installation of fraudulently or illegally obtained software.
4. You must not access or copy files that belong to another account without prior authorization from the account holder. All requests for access to files or directories should go through the Managing Attorney who will request the Network Administrator to make such changes. Files may not be taken to other sites without permission from the managing attorney. **Improper use or disclosure of client files is grounds for immediate discharge.**

5. You must not use the system irresponsibly, or needlessly affect the work of others. This includes transmitting or making accessible offensive, annoying or harassing material; intentionally damaging the system; intentionally damaging information not belonging to you; or intentionally misusing system resources or allowing misuse of system resources by others.

6. You are responsible for reporting to the Network Administrator any violation of these guidelines by another individual, **especially any violation that may compromise client information**. You are also encouraged to report any information relating to a flaw in, or bypass of, computer facilities security.

Failure to comply with the above guidelines, or the unauthorized or illegitimate use of *Gates, Jobs & Ellison's* computing facilities or resources, shall constitute a violation of policy and will subject the violator to disciplinary action, including the possibility of immediate termination.

Employee Computing Account Agreement

Name _____

Position _____

Supervising
Attorney _____

I have read the **Computer Use Policy**. I agree to follow the rules contained in this Policy. I understand that if I violate the rules, I may face disciplinary action, including immediate termination.

Signature _____ - _____ Date _____

II-4. Disclaimer for E-mail Signature for Use on Law-Related Listservs

This email expresses only the generalized personal opinion of the writer and is not meant to be construed as legal advice. Nothing in this message is to be construed as creating a lawyer-client relationship. The views expressed are mine alone and are not be ascribed to the firm of *Hue, Due and Lue*.

APPENDIX III PASSWORD PROTECTION OF MICROSOFT WORD AND COREL WORD PERFECT

To assign a password to a Word Perfect 5.0, 5.1, 6.0, 6.1, 7.0, 8.0 file,

- 1 Click **File, Save As.**
- 2 Specify the file you want to password-protect.
- 3 Make sure the file format is Corel WordPerfect 5 or later.
- 4 Click **Password protect**, then click **Save.**
- 5 Type the password you want to use, then click **OK.**
- 6 Retype the password, then click **OK.**

To Require a password to open a Word file,

- 1 Open the document.
- 2 On the **File** menu, click **Save As.**
- 3 Click **Options.**
- 4 In the **Password to open** box, type a password, and then click **OK.**
- 5 In the **Reenter password to open** box, type the password again, and then click **OK.**
- 6 Click **Save.**

How to Avoid Losing your License

On The Information

Superhighway

Ethical Issues Raised by the Use of the Internet in the Practice of Law

by Kurt Metzmeier and Shaun Esposito

The last three years have seen a revolution in the way that Americans communicate with each other, entertain themselves, and research purchases and services. Millions of Americans have learned how to negotiate the expanding byways of the information superhighway. One of the most popular uses of the network of computers, collectively known as the Internet, is the transfer of written messages. Electronic mail, or email, is increasingly employed in the practice of law by small and large firms alike. A recent survey by the ABA's legal technology research center showed that 64% of responding small law firms reported using the Internet in 1997, up from 38% just one year earlier.¹ Some 54% of the respondents used email to communicate with colleagues, and 41% employed the Internet to communicate with clients.

Almost as popular as email is the use of the world-wide web.² The same ABA study found that most large firms have invested in Internet development: A majority of the larger firms had firm web pages; 60% of those who did not have pages planned

to create one in the near future.³ The ubiquitous web address has become as essential to American business as the toll-free number and the yellow page ad. The challenge for attorneys is to incorporate these new communication technologies into their practices without compromising the interests of their clients or falling afoul of the rules of professional ethics.

Using Email in the Practice of Law

The increasing use of email by law firms, as well as lingering doubts over the security of the Internet, has raised questions about whether the responsibility of lawyers to protect the confidentiality of client information is being unwittingly violated by the use of email to communicate with clients.⁴ Although the Kentucky bar has not yet visited the issue, the initial ethics opinions from other states have been mixed. Advisory boards in Iowa and South Carolina concluded early on that either encryption or the explicit consent of the client would be required to shield an attorney from ethics liability. The Illinois bar, on the

other hand, has taken the position that, because the likelihood of the interception of email is comparable to traditional communications and is heavily prohibited by federal law, no special protections are required. The split between these ethics advisory committees can, to a large degree, be explained by the varying degree of understanding that these bodies have of the technical processes involved in electronic communication over the Internet.

The increased use of email listservs and discussion groups has caused commentators to question whether the participation of attorneys in these forums is a form of advertising, or if it is more analogous to the participation of lawyers in public interest programs broadcast on radio and television.

How Email on the Internet Works

The Internet is, at its most basic level, a loosely interwoven network of computers connected by telephone lines that, by use of a variety of accepted rules, or protocols, can be

used to exchange information. It was reportedly designed by the defense establishment to withstand a nuclear war on the idea that an open network of computers, each able to pick up the tasks of another, would be better able to adapt to the loss of component parts than a closed network.⁵ The transfer of messages from one computer account owner to another was one of the earliest uses of the Internet.

One relevant characteristic of email over the Internet is that the path of a particular piece of email is unpredictable. Instead of being transferred whole from the sender to the recipient, each email document is broken up by the sender's host computer into small "packets" of data, each roughly the size of a paragraph. Each packet is then sent out onto the Internet and passed from computer to computer in a path determined by which computer is least busy at that millisecond. The packets are then reassembled by the recipient's host computer where the message remains until accessed and deleted by the recipient.⁶ The architecture of the Internet makes it extremely difficult to intercept a particular piece of email while the packets are on their journey. In fact, the majority of Internet email security breaches occur not on the Internet itself, but rather when a hacker gains access to the recipient's host computer or when a system administrator abuses his or her legitimate access rights. Tampering with electronic mail is a federal offense under the Electronic Communications Privacy Act and anyone who violates the ECPA risks both criminal and civil sanctions.⁷

Protecting Client Confidentiality

Neither Rule 1.6 of the Rules of Professional Conduct adopted by the Kentucky Supreme Court, nor the official Comments, explicitly provide



A member of the Kentucky Bar since 1981, Shaun Esposito received his J.D. from the University of Louisville School of Law.

Following a year as law clerk to Justice Marvin Sternberg of the Kentucky Supreme Court, Esposito spent five years with the Louisville Legal Aid Society. Turning to the legal academic world, he then spent three years as a Legal Writing and Research Instructor at Florida State University's College of Law. At Florida State, he also earned a M.S. degree from the School of Library and Information Studies there. His work as a professional librarian started at the University of Toledo's College of Law Library. Since 1994, Esposito has worked at the University of Kentucky's law library, where he is the Reference and Electronic Information Services Librarian.

guidance on the technical means used by lawyers to communicate with clients and share confidential client information with colleagues. The text of Rule 1.6 itself indicates only that "A lawyer shall not reveal information relating to the representation of a client unless the client consents after consultation . . ." By implication, the rule has been found to impose a responsibility on an attorney to prevent the inadvertent publication of client information,⁸ but there are currently no formal or informal ABA opinions or Kentucky formal ethics opinions that discuss the issue of email confidentiality. For guidance, the Kentucky lawyer must turn to the admittedly mixed message conveyed by the advisory bodies of other states



Kurt X. Metzmeier is a graduate of the University of Louisville School of Law and a member of the Kentucky Bar since 1995. He is

currently the Coordinator of Information Systems Services at the University of Kentucky College of Law, where he is responsible for integrating technology into the teaching of the law and for instructing students in the use of electronic resources in the practice of law. Metzmeier has an upcoming article appearing in the Kentucky Law Journal that analyzes the current and future state of Internet legal resources in Kentucky.

that have examined the issue.

One of the first state ethics bodies to take up the issue of the ethics of email communication was the South Carolina bar. In a 1995 opinion, the South Carolina Ethics Advisory Committee determined that "the confidentiality requirements of Rule 1.6 are implicated by any confidential communication which occurs across electronic media, absent express waiver by the client."⁹ The committee found what it believed was a cogent analogy to email communications in cellular telephony and noted three state ethics advisory opinions barring the use of cellular telephones to communicate confidential client information without that client's consent.¹⁰ Ignoring the possibility that perhaps another wire-based means of communications, like ordinary telephony, was more analogous than the cellular technology, which broadcasts

signals over the air, the advisory committee found:

“Thus, it is the opinion of the committee that unless certainty can be obtained regarding the confidentiality of communications via electronic media, that representation of a client, or communication with a client, via electronic media, may violate Rule 1.6, absent an express waiver by the client.”¹¹

The South Carolina opinion was followed in May 16, 1996 by a formal opinion of the ethics committee of the Iowa bar association that advised that: “Pure inter-exchange of information or legal information with clients [need not conform to advertising rules], but sensitive material must be encrypted to avoid violation of DR4-101 . . .”¹² Apparently the ruling was later found to be too restrictive and was slightly revised three months later in an August 29, 1996 opinion:

“[I]f sensitive material is to be transmitted via e-mail, the lawyer must have written acknowledgment by client of the risk of the violation of Rule 4-101 [i.e. client confidentiality] and obtain consent for the communication via Internet or non-secure Intranet or other forms of proprietary networks. Otherwise the communication must be encrypted or protected by a password/firewall or other generally accepted equivalent security system. Opinion 95-30 is rescinded.”¹³

The Iowa body did not go into its rationale in requiring either encryption or explicit consent, but it was no doubt

influenced by the perception that email communication was somehow less safe than traditional forms of communication such as fax, telephone, courier and ordinary mail. The implicit assumption of the South Carolina and Iowa opinions was that email communication is inherently so unsafe as to require an assurance of “certainty” regarding confidentiality not required for other means of communication. Under this theory, only encryption or explicit waiver could satisfy Rule 1.6.

In stark contrast with the initial response of the South Carolina and Iowa ethics bodies (both of which later revised their opinions), the Illinois State Bar Association, in an intelligent and well-reasoned advisory opinion, found that attorneys may communicate with clients using ordinary, unencrypted email, unless unusual circumstances dictated otherwise.¹⁴ The Illinois committee began its opinion by noting the implied duty of lawyers to prevent the inadvertent publication of confidential client information, and recalled its opinion barring the transmission of client secrets over cordless and mobile telephones because of the susceptibility of that medium to interception. It then briefly discussed the opinions of the Iowa and South Carolina bodies, but decided those opinions were in error. The committee noted that “courts and ethics committees have uniformly held that persons using ordinary phones for confidential communications have a reasonable expectation of privacy. The three common types of electronic mail messages appear no less secure.”¹⁵ The committee then examined three common types of email, finding them more analogous to wire-based telephony than over the air cellular and wireless technologies. The committee admitted that dishonest persons could intercept email at a host machine, but that same type of threat

could occur using ordinary telephonic communication, and that, in each case, the Electronic Communications Privacy Act¹⁶ made criminal such activities: “The committee does not believe that the possibility for illegal interception by the personnel of an ISP (Internet Service Provider) makes it unreasonable to expect privacy of the message.”¹⁷ The Illinois committee thus found:

“In summary, the Committee concludes that because (1) the expectation of privacy for electronic mail is no less reasonable than the expectation of privacy for ordinary telephone calls, and (2) the unauthorized interception of an electronic message subject to the ECPA is illegal, a lawyer does not violate Rule 1.6 by communicating with a client using electronic mail services, including the Internet, without encryption. Nor is it necessary, as some commentators have suggested, to seek specific client consent to the use of unencrypted email. The committee recognizes that there may be unusual circumstances involving an extraordinarily sensitive matter that might require enhanced security measures like encryption. These situations would, however, be of the nature that ordinary telephones and other normal means of communication would also be deemed inadequate.”¹⁸

Since the Illinois decision, those state ethics bodies examining the issue of client communications via electronic mail have generally avoided requiring encryption or written

waivers in all circumstances.¹⁹ Recently, both Iowa and South Carolina have revised their previous opinions to allow greater freedom for unencrypted email.²⁰ Iowa shifted ground slightly to require a written waiver from the client, but South Carolina turned full circle recognizing a "reasonable expectation of privacy" in email communications that satisfied Rule 1.6.²¹ North Dakota, the latest state to take up the issue, refused to require encryption for "routine matters with clients, and/or other lawyers jointly representing clients."²²

So, Should a Kentucky Lawyer Avoid Email?

Although it is clear that recent decisions by ethics committees in other states indicate a strong trend toward the view that routine email communications are as safe as other ways attorneys maintain contact with clients, the absence of a state advisory opinion leaves a lawyer in Kentucky that chooses to use email with the legitimate fear that he or she will be second-guessed down the road. Some attorneys have decided to avoid the issue by refusing to use email, but the prevalence of email use makes this a short-term solution for most lawyers. Increasingly, potential clients will expect and, in many cases demand, the opportunity to communicate with their lawyer by email. Attorney's Liability Assurance Society (ALAS), a large attorney malpractice insurance firm, has carefully examined the issue and perhaps offers the soundest course. The ALAS insists that it is not necessary for its insured attorneys to encrypt ordinary client communications over the Internet to protect confidences. Nonetheless, it urges its clients to use "great caution" because of the possibility that courts and ethics committees "will be tempted to

bypass a careful analysis" and hold that unencrypted email "either violates ethics rules or waives the [attorney-client] privilege."²³ Until the KBA offers any guidance on email communication, the prudent lawyer wishing to use email to communicate with his client should seek the client's written consent and perhaps investigate one of the email packages that includes encryption. Fortunately, several easy-to-use email packages with encryption capabilities are now beginning to enter the market.²⁴

Solicitation by Email

Persons using email often subscribe to interactive discussion groups and listservs. Listservs or discussion groups are independently organized electronic forums where participants "post" email messages concerning the discussion topic around which the listserv or group has been organized. The participation by attorneys in public electronic forums may implicate ethics rules concerning advertisement and solicitation, especially when the topic of discussion explicitly involves legal issues. The Kentucky Rules of Professional Conduct regulate the way a Kentucky lawyer can broadcast information about his or her practice to the general public. There are specific rules concerning advertisements, direct and indirect solicitation, professional cards, telephone listings, announcements, signs, and letterheads. There is no discussion of the participation of lawyers on electronic discussion groups or listservs. However, Rule 7.02 which defines an advertisement, also notes exceptions to the advertising rules that are relevant to the activities of lawyers on listservs and online discussion groups. Rule 7.02(1)(f) states that:

"Any communication by a lawyer to third parties that is

published or broadcast by a third party who is not in any way controlled by the lawyer, and for which publication or broadcast the lawyer pays no consideration, shall be exempt from all the provisions of these Rules except Rule 7.10 [Rule 7.10 bars "false, deceptive or misleading communication about the lawyer or the lawyer's service"]."

The rule seems to indicate that ordinary postings by an attorney to a listserv or discussion group would not be subject to advertising and solicitation rules so long as the group was independent of the lawyer and the lawyer not pay to post his message. However, if the posting did not flow from the topic of the group and/or explicitly solicited clients, this narrow exemption would likely not apply. Four KBA formal ethics opinions relating to other media seem to support this theory. In Opinion KBA E-50, the committee said an attorney could appear on a commercially sponsored radio program in a "public service context" to discuss legal problems involved in real estate transactions. In Opinion KBA E-78, an attorney was allowed to write a series of articles for a local newspaper discussing probate and estate law. In 1975, a local bar association was allowed to place a series of articles in newspapers on legal issues by Opinion KBA E-110. Finally, Opinion KBA E-270 allowed a local bar association to sponsor a television show and allowed lawyers to participate. A number of states have also explicitly allowed the participation of attorneys in email discussion groups, so long as their participation does not cross over from discussion to solicitation,²⁵ but others have found it to be subject to rules regulating advertisements.²⁶

A few additional cautionary notes for attorneys using email. When using listservs and other electronic forums, lawyers need to be cautious that their replies are made publicly to the listserv, not privately to individuals. Answering questions "off-list" could inadvertently establish an attorney-client relationship or lead to a charge that the attorney is practicing law in a state where he or she is not licensed.

Also, attorneys should take every means to ensure that email is properly addressed. Finally, lawyers must take care that their firm's technical support staff²⁷ and email service provider are competent and trustworthy.

Advertising on the World-Wide Web

An information explosion in the last few years has changed the Internet

from a scholarly back road to a major marketplace for information, ideas and products. The web provides the opportunity for those using it to obtain graphically rich and visually appealing information with the click of a mouse. A major part of the web now deals with the marketing of products and services. Businesses ranging from auto dealers to book sellers have set

up stalls on the information superhighway. Given these marketing opportunities, it is not surprising that lawyers have begun to promote themselves and market their services in this new marketplace.²⁸ The marketing of lawyers' services naturally raises questions of the propriety of lawyer advertising and the ethical questions inherent in such activity. Kentucky's rules on lawyer advertising make no specific reference to the web, but a number of other states have issued rules regarding this issue that may be instructive.

Basic Mechanics of the Web

Information on the web is provided through specific locations on the Internet known as home pages. Attorneys using the web for marketing will have a home page with a unique address. That address, known as an URL (Uniform Resource Locator) follows a standard naming convention that typically begins with <http://www>. and includes the name of the host computer and ends with a three-letter code that indicates whether the site is educational, governmental or commercial. Information consumers view these home pages through the use of a web browser, such as Netscape Navigator or Microsoft Internet Explorer. An interested person might reach the site by typing a known URL directly into the browser, or by "hyper linking" to it by clicking on a link to that site in another home page. Several web search engines also provide access to specific pages in response to a search query entered by the person seeking information. On a web browser the pages display in a graphical mode providing colorful packaging for the information conveyed. The underlying program language for a web page, Hypertext Markup Language (HTML) looks like gibberish to most

web users, but provides a wealth of information about the home page creator's desired audience.

Attorney Web Pages As Advertising

Kentucky provides no specific guidance on whether attorney home pages fall under the general rules of attorney advertising. An examination of the rules dealing with lawyer advertising would seem to include this type of communication within their scope. Concerning applicability of the rules, Kentucky Rule of Professional Conduct 7.01 states that the rule "shall apply to advertisements related to or concerning legal services . . ." Under the definitions provided in Rule 7.02, "advertise or advertisement means to furnish any written, printed or broadcast information or any other communication containing an attorney's name or other identifying information" [with certain exceptions]. These provisions seem to strongly imply that Kentucky's rules cover web-based marketing. Few states' rules provide explicit mention of the web- or computer-based activities, but the ethics committees of a number of state bars have provided guidance through ethics opinions or commentaries.²⁹

Reporting Requirements As Applied to Web Advertising

Kentucky Rule of Professional Conduct 7.05 provides the procedural mechanism required of all attorneys wishing to advertise. In particular, section 7.05(1)(b) requires that "simultaneously with the publication of any advertisement under this subsection, the attorney shall mail to the Commission . . . a copy of the advertisement, or if by radio or television, a fair and accurate representation of the advertisement plus a typed transcript of the words spoken.

... A list of all persons or firms or groups to whom the advertising has been sent shall be maintained in the principal office in Kentucky of the advertising lawyer or firm for a period of two (2) years . . ."

Just what is required of a Kentucky attorney using the web is not clear from this rule. Would a notification of the home page's address (its URL) be enough? What about a printed copy of the home page? And, if so, how much of the home page—the opening screen, or every screen? Some law firms provide a wealth of information on various topics, and providing copies of all this material could become burdensome for both the attorney and the Commission. Nearly every home page provides links to other sites maintained by third parties. Would hard copies of these sites also be necessary? Web pages require constant updating and changing. Are Kentucky attorneys under a continuing duty to disclose any changes to the web page by providing additional hard copies of the whole web site or just the changes? Do any changes trigger the reporting requirement or just material ones, and if so, what is a material change?

While Kentucky has remained silent on these points, other states have offered some guidance to attorneys attempting to comply with these type of requirements. Florida's Bar Ethics Department advised that a hard copy must be filed with the department, as well as a statement explaining when and where it will appear.³⁰ Although Florida provides some guidance with this bit of advice, it still provides little insight into the amount of material that must be filed. And, the advice seems to be ignorant of how the web is used. Any web user anywhere could view the page with the click of a mouse. It would be impossible for an attorney to know who will view the page. Texas has provided more guidance on the

amount of material to be filed, limiting it to the first page viewed and any subsequent screens primarily dealing with client solicitation.³¹ Iowa has also provided that the first screen and biographical screens must contain required disclosures.³² Recently, the Utah State Bar Ethics Advisory Opinion Committee advised attorneys to keep copies of all pages of the web site (not just the initial home page) for the required two year period.³³ Recognizing that web pages are frequently updated, the Committee approved the retention of electronic rather than hard copies of the changes to web pages. The North Carolina Bar's Ethics Committee, also recognizing the frequency of web page updates, requires hard copies be retained only of any "material changes in format or content" to the original pages.³⁴

Jurisdiction and Choice of Law on the World-Wide Web

By its very nature, the web spans the globe; it is, after all, the world-wide web. Thus, persons anywhere in this country or around the world might access a given home page. This raises troublesome questions for both the advertising attorney and the bar's governing ethical body. Which state's ethical rules apply: the attorney's home state, or any state where someone can access the home page?³⁵ Must an attorney licensed in more than one state meet requirements in all states in which the attorney is licensed? And for those states where the attorney is not licensed, does contact with potential clients in those states resulting from web pages give rise to unauthorized practice of law problems?³⁶

Although no reported cases deal specifically with attorney web advertising, conflicting decisions have been issued by courts concerning jurisdictional issues related to web pages.³⁷

Many commentators believe that attorneys should list those jurisdictions in which they are admitted to practice, in order to avoid any confusion and to remain consistent with those ethical rules requiring the avoidance of false, deceptive or misleading communications (see Kentucky Rule of Professional Conduct 7.10). Cautious attorneys will at a minimum provide disclaimers about the limits of their practice and provide information about states in which they are licensed to practice. At minimum, attorneys should be certain to comply with the requirements for each state in which they are licensed.³⁸ Finally,

some commentators suggest that the conflicting state rules are so confusing, some national standards need to be developed.³⁹

Web Pages As Solicitation

For the most part, states examining the topic consider web home pages with proper disclaimers to be akin to advertising rather than solicitation.⁴⁰ Solicitation rules are much stricter than those governing advertising (see Kentucky Rule of Professional Conduct 7.30). By their nature, web pages are viewed only when someone

purposely chooses to seek out and view them. This makes a charge of improper solicitation very unlikely. Some commentators, though, have noted that with developing technology, such as interactive web pages, concerns about solicitation might grow.⁴¹ Even now, some have raised concerns about banner advertising (where a firm or company ad will appear, unsolicited, on a web search engine's page following entry of a research query). Additionally, web page creators can put keywords in fields used by Web search engines to determine whether a given site matches the search query entered by the user. Some web page designers "pack" this field with every possible relevant term, many duplicated or triplicated to increase possible hits. If a lawyer uses these tactics this could be held to border on solicitation depending upon the index terms used and how accurately they reflect the contents of the home page.⁴²

While existing ethical rules in Kentucky may seem to cover attorneys' activities on the web, the questions raised here, and the activities of the bar governing authorities in several other states, suggest the need for clarification of exactly how these rules apply to web activities. To craft meaningful new rules or commentaries on existing rules, the bar's governing authority must consult those who are knowledgeable about the workings of the web. If rule drafting in the area is left to persons without an understanding of how the web works, more rather than less confusion will likely result.⁴³

Conclusion

The information superhighway may be fraught with dangers for attorneys, particularly those who are apt to skirt the rules. Unwary lawyers may risk losing their license for inadvertently betraying client confidences, by

soliciting clients on listservs and in chat rooms, or by passing over unclear ethical lines with a flashy web page. Despite these road hazards, attorneys will find that in the very near future a web page will be as essential as a shingle and a yellow page listing, and that clients will insist on using email to communicate with their lawyer, just as they use it to manage their businesses and to stay in touch with their kids. ■

ENDNOTES

1. American Bar Association, Legal Technology Resources Center, *1997 Small Firm Technology Survey* (July, 1997); American Bar Association, Legal Technology Resources Center, *1997 Large Firm Technology Survey* (July, 1997).
2. *Id.*
3. *Id.*
4. See, generally, William Freivogel, *Communicating with or About Clients on the Internet: Legal Ethical and Liability Concerns*, 1 ALAS LOSS PREVENTION J. 17 (Jan. 1996).
5. A good description of the origin of the Internet, as well as its current architecture, can be found in Paul Gilstar's *NEW INTERNET NAVIGATOR* 19-43 (1995).
6. *Id.* at 19.
7. 18 U.S.C. § 2510 *et seq* (1994).
8. A widely used treatise of legal ethics notes that the "general obligation" under Rule 1.6 "gives rise to a number of duties." CHARLES W. WOLFRAM, *MODERN LEGAL ETHICS* §6.7.5 (1986). Among these duties is a duty "to see that the client's interest in full confidentiality of information is adequately protected. Conferences with clients should be arranged to avoid the presence of third parties. ... The lawyer's files should be confidentially maintained, and nonlawyer employees should be instructed, and periodically reminded, to keep all office matters strictly confidential." *Id.* Generally, all client communications, even those that are not "confidences," fall under this general obligation. See, KBA E-253 (1981) (committee advised that even the very existence of an attorney-client relationship should be held confidential).
9. S. C. Ethics Advisory Op. 94-27 (1995). This opinion was substantially revised in 1997 to allow unencrypted lawyer-client email communications. S. C. Ethics Advisory Op. 97-08 (1997).
10. Mass. Advisory Op. 94-5 (1994); N.Y.City Advisory Op.1994-11 (1994); N. H. Advisory Op. 1991-92/6 (1991).
11. S. C. Ethics Advisory Op. 94-27 (1995).
12. Iowa Formal Op. 95-30 (1996)
13. Iowa Formal Op. 96-1 (1996). The Iowa bar group further amended its opinion by adding the following language:
 - III. Pure exchange of information with clients is an exception to Division I of this opinion, but with sensitive material to be transmitted on email counsel must have written acknowledgment by client of the risk of violation of DR 4-101 which acknowledgment includes consent for communication thereof on the Internet or non-secure Intranet or other forms of proprietary networks to be protected as agreed between counsel and client.
 Iowa Formal Op. 97-1 (1997) Iowa attorney David A. Hirsch, whose appeal of 96-1 prompted the revision, argues that this "revision" only stated explicitly what was implied in its prior decision and, by adding the undefined phrase "sensitive materials" muddled the issue even further. Listserv discussion on legaethics-1@lawlib.wuacc.edu listserv (October 22-25, 1997).
14. Ill. State Bar Assoc. 96-10 (1996).
15. *Id.*
16. 18 U.S.C. §§ 2510-2520 (1998). The ECPA also makes any illegally intercepted communication inadmissible as evidence in any "trial, hearing or other proceeding" held under the authority of "the United States, a State, or a political subdivision thereof." 18 U.S.C. § 2515 (1998).
17. Ill. State Bar Assoc. 96-10 (1996).
18. *Id.*
19. Pa. [Informal] Op. 97-130 (1997); Mass. Bar Assoc., Inquiry Response No. 1997-T30 (1997). Internet legal ethics commentator Peter Krakaur sees a trend away from encryption that will grow as bar ethics bodies become more educated about the Internet. Peter Krakaur, *E-mail Emancipation*, 1.1 INTERNET LAW PRACTICE NEWS 1 (Oct. 20, 1997).
20. Iowa Formal Op. 97-09 (1997); S. C. Ethics Advisory Op. 97-08 (1997).
21. *Id.*
22. State Bar Assoc. of N. D. Ethics Comm. Op. 97-09 (1997).
23. William Freivogel, *Communicating with or About Clients on the Internet: Legal Ethical and Liability Concerns*. 1 ALAS

- LOSS PREVENTION J. 17, 19 (Jan. 1996).
24. One easy means of encryption is available to all attorneys worried about the transfer of confidential information: both Corel WordPerfect or Microsoft Word allow the password protection of documents. An attorney can simply password-protect the document, send it as an email attachment, and transmit the password by other means.
 25. Ill. State Bar Assoc. Op. No. 96-10 (1996).
 26. S. C. Ethics Advisory Op. 94-27 (1995); Mich. State Bar Comm., Informal Op. RI-276 (1996).
 27. Prudent lawyers should treat those persons managing their computers and electronic networks as nonlawyer assistants subject to Rule 5.3 and "should give such assistants appropriate instruction and supervision concerning the ethical aspects of their employment, particularly regarding the obligation not to disclose information relating to the representation of the client, and should be responsible for their work product." Comment to SCR 3.130, Rule 5.3.
 28. For an introduction to web marketing by a couple of savvy lawyers who know how to play by the rules, see GREGORY H. SISKIND & TIMOTHY J. MOSES, THE LAWYERS GUIDE TO MARKETING ON THE INTERNET (1996), distributed by the American Bar Association's Law Practice Management section.
 29. Most opinions that have considered attorney web marketing consider the pages to be no different than other forms of print and electronic advertising. See Pa. Informal Op. 96-17 (determining that "a web page qualifies as 'public media'"); N.Y. Cty. Law. Assn. Comm. Prof. Eth. Op. No. 721 (1997)(determining that web page information is not prohibited by the Code of Professional Responsibility and constitutes advertising); Conn. Bar Assn. Informal Op. 97-29 (finding that "the same rules apply to Internet advertising that apply to advertising in other media"); Mich. Prof. Jud. Eth. Op. RI-276 (1996)(distinguishing among types of internet information and finding that where the user "initiates the contact with the posted information" normal rules concerning advertising, rather than those related to solicitation, apply); Cincinnati Bar Assn. Eth. Prof. Resp. Comm. Op. 96-97-01 (finding that ordinary rules of professional conduct apply to internet sites); Florida Bar Assoc., Standing Comm.on Advertising. Internet Guidelines (1997)(available at the FBA web site: <http://www.flabar.org/Regulation/AdReg/adguide.html>) (advising that web pages fall under general advertising rules); Iowa Formal Op. 96-1 (1997)(determining that web pages fall under usual advertising rules); Utah Eth. Op. 97-10 (1997)(finding attorney web sites to be a form of advertising).
 30. Florida Bar Assoc., Standing Comm.on Advertising. Internet Guidelines (1997). Available at the FBA web site: (<http://www.flabar.org/Regulation/AdReg/adguide.html>).
 31. Texas Disciplinary Rules of Professional Conduct, Part 7, Interpretive Comment 17. For an extensive analysis of this Comment, see Mitchel L. Winick, ET AL, *Attorney Advertising on the Internet: From Arizona to Texas—Regulating Speech on the Cyber-Frontier*, 27 TEX. TECH L. REV. 1487 (1996).
 32. Iowa Formal Op. 96-1 (1997).
 33. Utah Eth. Op. 97-10 (1997).
 34. North Carolina State Bar Assn. Eth. Comm. Op. 239 (1997).
 35. One Iowa ethics opinion has gone so far as to suggest that two distinct, unlinked web sites be maintained, one for Iowans, one for all others. Iowa Formal Op., 96-14 (1997). *But see*, Pa. Informal Op. 96-17 (warning that it may not be possible to comply with all advertising rules throughout the country due to their contradictory requirements).
 36. For a discussion of one possible solution to the myriad of interstate problems, see Peter Krakaur, *Internet Advertising: States of Disarray?: Are Uniform Rules a More Practical Solution*, N.Y. LAW J. (Sept. 15, 1997). See also Kathryn N. Fenton, *Legal Ethics and the Internet*, 11-SUM ANTITRUST 43 (1997)(discussing unauthorized practice of law issues).
 37. In a series of cases dealing with the use of state long-arm statutes and the constitutional limits of personal jurisdiction, conflicting rulings have been handed down. See *Compuserve, Inc. v. Patterson*, 89 F.3d 1257 (6th Cir. 1996)(finding personal jurisdiction appropriate in Ohio over Texas defendant whose only contact had been electronic with Ohio plaintiff Compuserve), see also *Hall v. Laronde*, 56 Cal. App. 4th 1342, 66 Cal. Rptr. 2d 399 (1997)(holding personal jurisdiction appropriate where contacts with California were only electronic) and *Telco Communications v. An Apple A Day*, 977 F. Supp. 404 (E.D. Va. 1997)(finding personal jurisdiction appropriate under Virginia long-arm statute over Missouri defendant that placed material on web site that allegedly defamed Virginia corporation); *but see Cybersell v. Cybersell*, 130 F.3d 414 (9th Cir. 1997)(holding that mere use of trademark on Internet advertisements by Florida defendant did not establish personal jurisdiction in Arizona); *Bensusan Restaurant Corp. v. King*, 126 F.3d 25 (2d Cir. 1997)(finding no jurisdiction under New York long arm statute over Missouri defendant where only contact with New York was web advertisement concerning defendant's Missouri establishment).
 38. For a handy checklist of ethics considerations related to web advertising, see John B. Kennedy, *Legal Advertising and Ethics on the World Wide Web*, N.Y.L.J. S1 col. 5 (1/27/97); see also J.T. Westemeier and Leonard T. Nuara, *Ethical Issues for Lawyers On the Internet and World Wide Web*, 14 COMPUTER LAWYER 8 (1997).
 39. H. Geoffrey Moulton, Jr., *Federalism and Choice of Law in the Regulation of Legal Ethics*, 82 MINN. L. REV. 73, 171 (1997)(stating, in regard to internet advertising, "we may have reached the point that effective state-based regulation of lawyer advertising and solicitation is a practical impossibility"); see also Peter Krakaur, *Internet Advertising: States of Disarray?: Are Uniform Rules a More Practical Solution*, N.Y. LAW J. (Sept. 15, 1997).
 40. See Mass. Bar Assoc. Op.1997-130 (Advising that not only are attorney web pages not solicitation but they are also not advertising under the rules) and Michigan Ethics Op. RI-276 (1996)(contrasting the posting of a web page with the direct solicitation involved with sending email to specifically targeted potential clients).
 41. See Kennedy, *supra*, n. 38 (noting the continued development of "push" technology makes web pages much more interactive and much less like a "passive" television or radio advertisement).
 42. In its interpretive comment concerning the application of ethics rules to internet activity, *supra* n. 31, the Texas disciplinary body included in its list of examples of activities generally not considered to be solicitation the following: questionnaires and survey forms, E-mail and E-mail response forms, online registration for seminars and events, and links to other internet sites.
 43. Readers interested in monitoring further developments in this area should consult a new Kentucky legal ethics web page, the result of a joint effort of the Kentucky Bar Association and the University of Kentucky College of Law Library www.uky.edu/Law/kyethics. This site contains the text of recent KBA Ethics Opinions as well as other information of interest to Kentucky practitioners.

Appendix to "How to Keep Your License on the Information Super-Highway"
 prepared by Shaun Esposito, Reference & Electronic Information Service Librarian, University of
 Kentucky College of Law Library

Articles Related to Attorney Web Pages & Internet Use

Advertising on the Net, The Young Lawyer, <<http://www.abanet.org/yld/tyl/julyad.html>>
 (points out ethical questions raised by attorney internet use and provides links to relevant sites)

Fisher, Vance A. *Practicing Law on The Internet: The Virtual Law Firm*
 <<http://209.69.6.126/~wpoff/michbar/V19AA02.htm>> (well footnoted exploration of ethical
 dilemmas of the internet law firm)

Hankins, Mark. *Ambulance Chasers on the Internet: Regulation of Attorney Web Pages*,
 1 J. Tech. L. & Pol'y 3, <<http://journal.law.ufl.edu/~techlaw/1/hankins.html>> (1996)(practitioner
 offers extensive analysis of ethical considerations for attorney web pages)

Kennedy, Dennis M. *Marketing Your Legal Practice on the Internet: Successful, Safe and
 Ethical Ways to Use the Internet to Market and Promote Your Practice While Staying Within the
 Ethical Boundaries for Practicing Law*, <<http://www.bamsl.org/inet/dkmark01.htm>> (outline
 of seminar on topic presented to St. Louis Bar Association, extensive discussion of technologies
 and legal issues involved)

Kennedy, John B. *Legal Advertising and Ethics On the World Wide Web*,
 <<http://www.ljx.com/internet/0127webethics.html>> (Law Journal Extra article provides
 citation to numerous articles and bar rules)

Kennedy, Dennis M. *Hanging Out Your Shingle on the World Wide Web: Promoting Your
 Practice in a Digital Era* <<http://members.aol.com/dmk58/slbjart.html>> (a general "how to"
 column on setting up a firm web page, includes links to legal ethics sites in the footnotes)

Kennedy, Dennis M. *The Practice of Law in a Digital Era*,
 <<http://members.aol.com/dmk58/praclaw.html>> (provides and extensive list of links to sites
 dealing with ethical issues related to the internet)

Lanctot, Catherine J. and James Edward Maule. *The Internet -- Hip Or Hype? Legal Ethics and
 the Internet* <<http://www.law.vill.edu/vcilp/MacCratc/mcle/lanctot.htm>> (two Villanova
 professors discuss ethical issues related to internet advertising; also provides sample disclaimers
 for use on attorney web pages)

Legal Websites: Creation, Marketing, Disintermediation and Ethics in Web Counsel Notes,
 <<http://www.pli.edu/arts/pliethc9.htm>> (part of a summary outline of a PLI course on web
 creation and marketing, this section addresses ethical considerations)

Luce, Charles F. Jr., *Ethics In Attorney Advertising & Solicitation*,
<<http://www.mgovg.com/ethics/11advert.htm>> (in general discussion on attorney advertising includes extensive consideration of internet advertising)

Luce, Charles F. Jr., *On Legal Ethics and the Practice of Law*,
<<http://www.mgovg.com/ethics/index.html>> (general discussion of ethical issues by long-time Colorado practitioner, includes discussion of internet based ethical problems)

Maher, Stephen T. *The Practical Professor: Legal Ethics in Cyberspace*,
<<http://www.usual.com/article9.htm>> (provides a list of points to consider in determining whether to advertise on the internet)

Marsh, Stephen R. *Web Site Design for Small Firms: A Primer*,
<<http://www.collegehill.com/ilp-news/marsh.html>> (a straightforward how to guide for setting up a web page, this article includes references to relevant ethics materials)

Morgan, Laura W. *Ethics Spotlight: Attorney Malpractice for Web Site Content*,
<<http://divorcenet.com/famlaw/famlaw-ethics03-99.html>> (examines possible malpractice complications for attorneys with web sites)

Orsinger, Richard R. *Cyber Hazards: Legal & Ethical Pitfalls in Using the Internet*,
<<http://www.txdirect.net/users/rrichard/hazard.htm>> (this article, prepared for a CLE presentation, examines ethical issues including advertising and unauthorized practice of law)

Pruner, Mark. *The Internet and the Practice of Law*, 19 Pace L. Rev. 69 (1998)(examines use of web by law firms and considers ethical implications involved)

Rappaport Jordan, *Attorney Advertising on the Internet*,
<<http://www.law.miami.edu/~froomkin/seminar/papers/rappaport.htm>> (law student seminar paper explores ethical issues involved and provides extensive citations to other materials)

Read, T.K. *Pushing the Advertising Envelope: Building Bill Boards In The Sky Along The Information Superhighway*, <<http://www.computerbar.org/netethic/read.htm>> (copiously footnoted examination of mechanics of and issues involved in internet advertising)

Rogers, Joan C. *How Do Advertising Rules Apply to Lawyers on the 'Net?*
<http://www.bna.com/prodhome/bus/mopc_adnew.html> (from ABA/BNA Manual on Professional Conduct, this article reviews issues raised by net advertising and summarizes general trends in state bar ethics rulings on the topic)

Welch, Mark J. *Creating a Lawyer's Web Site; Results of My Web Site*,
<http://www.markwelch.com/probate_results.htm> (good explanation of nuts and bolts of putting up a web site, includes discussion of ethical problems)

Sample Law Firm Web Pages From Kentucky and Beyond

Becker Law Office <<http://www.beckerlaw.com/>>

Bowles Rice McDavid Graff & Love <<http://www.bowlesrice.com/>>

Bricker & Eckler <<http://www.bricker.com/welcome.htm>> (Ohio firm, an early web page developer and award-winning web site)

Brown, Todd & Heyburn <<http://www.bth-pll.com/>>

Bryan Gowin <<http://www.bryangowin.com/>>

Dinsmore & Shohl <<http://www.dinshohl.com/index.cfm>>

Faegre & Benson <<http://www.faegre.com/>> (web site award-winning Midwest multi-state firm)

Frost & Jacobs <<http://www.frojac.com/>>

Goldberg & Simpson <<http://www.gsatty.com/welcome.html>>

Jewell & Lemke <<http://www.bluegrass.net/~mcl/jewelem.html>>

LexTech's List of Top Ten Law Firm Web Sites
<<http://www.lextechinc.com/topten/firms.html>> (includes Kentucky's own Brown, Todd & Heyburn)

Miller, Griffin & Marks <<http://www.kentuckylaw.com/mgm.html>>

Poston, Seifried & Schloemer, <<http://www.nkymall.com/ps&slaw/>>

Publishing Law Center <<http://www.publaw.com/>> (informational/advertising page dealing with legal issues in the publishing industry)

Stites & Harbison <<http://www.stites.com/>>

Stout Law Office <<http://www.stoutlaw.com/>>

McAdam's Home Page <<http://members.aol.com/TAMCADAM3/lawyer.html>>

Siskind Susser & Haas <<http://www.visalaw.com/>> (a true web pioneer, this immigration law firm has been cited many times as an example of an effective web page producer)

Taft, Stettinius & Hollister <<http://www.taftlaw.com/overview/>>

Watson, Farley & Williams <<http://www.wfw.com/>> (multi-national international law firm with award-winning web site)