

# Richmond Journal of Law and Technology

---

Volume 6 | Issue 1

Article 4

---

1999

## Database Protection in a Digital World

Mary Maureen Brown

Robert M. Bryan

John M. Conley

Follow this and additional works at: <http://scholarship.richmond.edu/jolt>



Part of the [Computer Law Commons](#), and the [Internet Law Commons](#)

---

### Recommended Citation

Mary M. Brown, Robert M. Bryan & John M. Conley, *Database Protection in a Digital World*, 6 Rich. J.L. & Tech 2 (1999).

Available at: <http://scholarship.richmond.edu/jolt/vol6/iss1/4>

This Article is brought to you for free and open access by UR Scholarship Repository. It has been accepted for inclusion in Richmond Journal of Law and Technology by an authorized administrator of UR Scholarship Repository. For more information, please contact [scholarshiprepository@richmond.edu](mailto:scholarshiprepository@richmond.edu).



**Volume VI, Issue 1, Symposium 1999**

---

**Database Protection in a Digital World**

**Mary Maureen Brown**

**School of Information Technology**

**University of North Carolina at Charlotte**

**Robert M. Bryan**

**Robinson, Bradshaw & Hinson, P.A.**

**Charlotte, NC**

**John M. Conley**

**University of North Carolina at Chapel Hill**

**School of Law**

---

**Cite As:** John M. Conley et. al, *Database Protection in a Digital World*, 6 RICH. J.L. & TECH. 2, (Symposium 1999) <<http://www.richmond.edu/jolt/v6i1/conley.html>>. **[\*\*]**

---

**Table of Contents:**

**I. Introduction**

**II. The Nature of Databases**

### III. Non-Legal Solutions

### IV. Legal Protection: The Current State of U.S. Law

### V. The Available Legal Options

### VI. Conclusions: What Should We Do?

---

#### I. Introduction

{1} Digital Property and the Digital Marketplace Expenditures in the information technology arena indicate that digital property - defined as digitized information and the tools to use it - is generating astonishing wealth. Globally, expenditures in the information and communication technology markets exceed \$1.8 trillion annually and comprise six percent (6%) of aggregate global Gross Domestic Product ("GDP").<sup>[1]</sup> By 1997, such expenditures had escalated forty percent (40%) over 1992 levels.<sup>[2]</sup> Current spending on information and communication technologies is growing twenty-seven percent (27%) faster than the overall worldwide GDP, averaging roughly 5.5 percent annually.<sup>[3]</sup> Technological innovations have become the primary engine of economic growth. For example, according to a 1997 government report, the technology market accounted for seventy-six percent (76%) of economic growth in France, seventy-eight percent (78%) in Germany, seventy-three percent (73%) in the United Kingdom, and fifty-five percent (55%) in Japan.<sup>[4]</sup>

{2} In the United States, investment in information technology grew from \$55 billion to \$190 billion during the 1980's, an annual growth rate of just under fifteen percent (15%).<sup>[5]</sup> By 1997, the United States was spending roughly \$643 billion annually on information and communication technologies.<sup>[6]</sup> As of that same year, information technology industries accounted for an estimated 7.8 percent (7.8%) of U.S. GDP and 12.4 percent (12.4%) of its nominal growth, while for 1998 the preliminary comparable figures are 8.2 percent (8.2%) and 14.7 percent (14.7%).<sup>[7]</sup> In 1995, information technology's share of all research and development spending in the U.S. was 43.7 percent (43.7%) and rising,<sup>[8]</sup> and by 2000, business spending on information technology equipment should exceed half of all spending on capital equipment.<sup>[9]</sup>

{3} Much of the investment in information technology is directly related to the growth of the Internet. Between 1996 and 1998, Internet utilization grew from forty (40) to 100 million people.<sup>[10]</sup> Forecasters speculate that Internet use will escalate to 320 million people by 2002,<sup>[11]</sup> when Internet use for commerce between businesses alone may amount to \$300 billion.<sup>[12]</sup> Use of the Internet for delivery of goods and services and the retail sales of tangible items is also on the rise, and if the current trend continues, "information technology and electronic commerce can be expected to drive economic growth for many years to come."<sup>[13]</sup> Cost savings, increased consumer choice, and improved customer convenience are stimulating the expansion of the Internet retail sector. Advances in information and communications technologies have significantly improved the ease with which products or art forms can be created, reproduced, and disseminated. Trade on the Internet is thus equally attractive to consumers and suppliers. For the former, it is fast and convenient; for the latter, it reduces overhead costs at every stage, from production through sale and delivery.

{4} Despite this unprecedented growth, many observers see problems ahead. Issues such as proprietary rights, access, accuracy, privacy, confidentiality, responsibility, and equity pose challenges to the future scope and direction of the digital era. This paper focuses on one concrete problem that brings many of these issues

into especially sharp focus: the appropriate scope of proprietary rights in databases. The problem implicates, among other things, the structure of the digital marketplace, the nature of digital property, the current and future state of the law of intellectual property, and the sometimes conflicting demands for economic incentives to both intellectual creativity and the universal dissemination of knowledge. [14] Universal access to knowledge is the greatest benefit of the digital economy. Once digitized, any piece of information or any author's work can be made available to anyone, anywhere, at anytime. But the concept of universal accessibility challenges some of the foundational premises of intellectual property protection. As a result of the ease with which digital property can be modified, copied, and distributed, longstanding legal and practical assumptions about protecting ownership, guaranteeing authenticity, and balancing the rights of owners and users may no longer apply.

{5} In a market-based economy, products are assumed to be valued at their true worth when four conditions are met. [15] First, the marketplace must be competitive. In addition, the product, whether a good or service, must manifest transparency, exclusivity, and rivalry. Competition is that state in which producers, driven by fear of their competitors, work diligently to keep prices as low as possible while avoiding over-production. In a perfectly competitive marketplace, goods are priced at their true value, and production and consumption are in equilibrium. Historically, the absence of government intervention has been assumed to be the most effective guarantor of competition, [16] leaving the task to Adam Smith's "invisible hand." [17] When markets have exhibited such characteristics as unusual barriers to entry or susceptibility to collusion, government intervention in the form of antitrust legislation has been necessary. [18] Governments have, of course, often intervened directly to support particular activities and enterprises.

{6} Whereas competition is a general attribute of the marketplace, transparency, exclusivity, and rivalry are attributes of particular products. [19] Transparency refers to the ability of the consumer to understand fully the value of the good or service prior to purchase. When goods or services are transparent, their value is known in advance, allowing consumers to make a rational choice as to whether the product is worth the purchase price. Few goods or services are inherently transparent, prompting government intervention in the form of trademark, truth-in advertising, and unfair trade practice laws. Exclusivity refers to the seller's ability to limit or control access to the product. Traditional retail goods exhibit nearly-perfect exclusivity: the seller uses physical dominion over the goods to control distribution, thereby limiting access to those who pay the purchase price. Free-riding is virtually impossible. The related concept of rivalry, sometimes termed individual consumption, assumes that one person's consumption of a product depletes the supply available for others to use, either temporarily or permanently. Once again, retail goods are the perfect example: if I have a particular chair in my living room, you cannot have it in yours; if I eat that loaf of bread, then you cannot.

{7} As the retail examples suggest, little or no government intervention is necessary to insure the exclusivity and rivalry of most tangible, movable property. Real property has evoked such supports as title filing and registration systems, but intellectual property has proved to be the most difficult case of all. Ideas, inventive concepts, know-how, even literary texts once disclosed to anyone are inherently accessible to others. Intellectual property is also almost totally non-rival: I can produce your play in one theater at the same time you are producing it in another without affecting the play itself. The fundamental purpose of all intellectual property law is to create an artificial form of exclusivity (rivalry is nearly impossible). Although I can produce your play without having to "steal" a tangible object, the law of copyright empowers you to treat me like a thief.

{8} Governments have been restrained, however, in their support of exclusivity. Patent and copyright monopolies are limited in both time and scope, while the law of trade secrets is riddled with exceptions and defenses. The guiding principle has always been balance: dole out only as much exclusivity as is necessary "to promote the progress of science and the useful arts," [20] but otherwise, protect the public domain. [21] The assumption is that in the absence of the ability to exclude others from free-riding, entrepreneurs will not take the risks necessary to develop and market new and useful products. Where "real" exclusivity is inherent

in the product itself, the government largely stands aside and lets the market take its course, unless competitors act to suppress market forces. But where the government itself is the source of an artificial form of exclusivity, constant vigilance is required to make sure that the discouragement of free-riding does not also discourage the socially useful process of technological improvement.

{9} How adequately are these four conditions satisfied in the digital marketplace? First, the market appears to be fiercely competitive. The government's suit against Microsoft suggests concern about barriers to entry and the leveraging of market power in some sectors, but the statistics with which we began the paper are indicative of a market with unprecedented dynamism. Thus far, monopolizing a particular product or facility has hardly been worth the effort because technology has enabled others to leapfrog the bottleneck faster than the legal process could break it up. With respect to transparency, digital property may be more opaque to consumers than, say, clothes, but this is a question of degree. To most consumers, cars, and airfares are probably as impenetrable as digital products.

{10} With respect to exclusivity, digital property presents the same basic challenges as other forms of intellectual property, but at unprecedented levels of complexity. Like other forms of intellectual property, digital goods can be jointly consumed without being diminished in quality or quantity, presenting the consumer with the temptation to free-ride by exploiting them without compensation. In the case of digital property, however, the temptation is greater by many orders of magnitude than in the instance of, say, a patent on an industrial process or a copyrighted book. The ease with which digital property can be located, accessed, copied, modified, and distributed is utterly without precedent. The problems involved in using intellectual property law to create a form of artificial exclusivity that will have meaning in the real world are formidable. [22]

{11} The exclusivity issue takes on a further layer of complexity when the digital property in question is a database, especially one found on the Internet. Computers can, of course, archive, compare, manipulate, and distribute data with astonishing facility. But in addition, neither data itself, nor the labor involved in collecting, recording, and arranging it have a secure place in the current structure of intellectual property law. The law has hesitated to extend exclusivity in these areas because of concerns about the appropriate balance between the incentives needed to promote the creation of useful data compilations and the public's need for free access to information. The ultimate purpose of this paper is to consider whether the digital era's newfound ease of appropriation requires a rethinking of the current legal compromise and, if so, what form it should take. We turn next, however, to some necessary background on the nature of databases and the technical means available to create a measure of "real" exclusivity.

## **II. The Nature of Databases**

{12} As is true in all emerging and evolving fields, much of the vocabulary pertaining to the digital economy is ambiguous. As digital jargon has developed, the term "database" has taken on several definitions, covering everything from telephone books to the World Wide Web ("WWW"). Our intellectual preference would be to abandon "database" because of its lack of clarity and substitute "information system," which, as discussed below, better captures the nature of the entities that are the subject of the "database" debate. However, because the legal discourse has clung insistently to "database," [23] we will retain it as well. This section examines in some detail the various forms of digital property that are grouped under the database heading.

{13} A database, or information system, contains two primary forms of digital property: raw data, which can be a source of knowledge or entertainment value, and tools, which are programs that can be used to communicate, store, or manipulate raw data. A fully developed database is an interrelated set of components capable of generating value from the collection, processing, merger, storage, or dissemination of data. In



practice, databases are arrayed along a continuum according to where their primary value lies. At one end are those whose value depends on the data themselves. At the other end are those databases whose critical element is the system for manipulating the data. Most, of course, are found somewhere in the middle.

{14} The process of extracting useful knowledge from volumes of raw data is known as *knowledge discovery*. The potential economic benefits of knowledge discovery initiatives have opened new avenues for selling raw data, digital tools, and combinations of the two. A range of businesses find the "mining" of data economically fruitful in both producing and marketing goods and services. New patterns, trends, and associations can be identified through the merging of vast amounts of disparate data. The use of constantly expanding search capabilities can result in the discovery of knowledge or products that possess previously unappreciated market value. Data which is scattered among a variety of sources can be matched, collated, and reproduced in new formats that can give value to otherwise random facts. For example, many grocery stores today offer discount cards to customers who will provide identifying and demographic information. The checkout computer then creates a precise record of each individual's purchasing habits. When organized by residence pattern, income level, etc., and distributed in a usable format, this data can be of enormous value to a variety of retail interests. A chain thinking of opening an Italian restaurant in a particular neighborhood can find out exactly how much the residents spend on Italian food at the grocery store. What was once low market-value, or even useless, data - a wastebasket full of cash register receipts - has been transformed into a marketing goldmine.

{15} Over the past several years, the market has exploded with new tools for searching, matching, collating, updating, replicating, and distributing data. In much the same way that a builder employs many different tools to build a house, databases can be crafted through the use of multiple tools. These tools can be bundled together and provided as a "complete" package, or they can be subdivided to address specific tasks. The revolution in tool technology is an obvious threat to the exclusivity of digital property. Less obviously, because many of today's tools can easily alter data quality and integrity, they also threaten product transparency (knowledge of the worth of the commodity prior to purchase).

{16} A now-familiar example is that category of tools often lumped under the generic heading of "Internet search engine." In response to simple user requests, search engines can root out digital property irrespective of geographic location. The vast "snooping" power of these engines, coupled with weaknesses in security and detection controls, facilitates theft and allows unauthorized distribution. Additionally, advances in copying and editing capabilities can lead to recompilations and new derivatives beyond the imagination, let alone, the knowledge of the original owner.

{17} The popular term "search engine" actually encompasses five different categories of tools: directories, search engines, super engines, meta search engines, and special search engines.<sup>[24]</sup> The first category, *directories*, is exemplified by the WWW search tools Yahoo and Magellan. With a directory service, a search will yield any relevant website that is registered with that directory. The site is then reviewed by employees of the search directory, then placed in a category within the directory, and assigned a relevance ranking by the employees.

{18} *Search engines* in the narrow sense, for example Lycos, Infoseek, and Webcrawler employ "spiders" to locate sites. Spiders (also known as "robots," "bots," or "crawlers") are programs used by search engines to locate, retrieve, index, and update new websites. The new website information is then provided in response to search queries. Spiders follow links within webpages to continually gather more and more site information. Once a site is indexed, it becomes available for a research request. The index usually stores keywords found within a site's title, description, and "meta tags." Meta tags provide descriptive information about the contents and owner of the site. Website developers can aid search engines by placing the keywords they wish to be associated with a site within meta tags in the page's HTML (hyper text markup language). Website developers may also register their sites with most search engines in the same way as with directories.

{19} A third search tool is the *super search engine*. Some examples of super search engines are Hot Bot, Altavista, Excite, and Open Text. These super engines expand on the search engine concept by programming their spiders to search for keywords within the text of the webpages instead of just in page titles, descriptions, and meta tags. A fourth variety, the *meta search engine* (for example, Metacrawler, Dogpile, Cyber411, and Savvy Search), allows users to employ multiple search engines or even super search engines at once. Metacrawler, for example, allows users to search Lycos, Infoseek, Webcrawler, Excite, AltaVista, Thunderstone, and Yahoo. Meta search engines typically do not contain a site database of their own, but merely route requests to a variety of different engines, then compile and return the results to the requesting party. A final class of search tool, the *specialized search engine*, targets specific types of information such as Usenet newsgroups (DejaNews), phonebook listings (Infospace), and FTP (file transfer protocol) archive sites (i.e., FTP Search). These engines are all searchable by keyword, though the actual search logic depends upon the individual engine.

{20} The search engine concept is not limited to the Internet. In the grocery card example given earlier, the checkout information would be "searched" by software analogous to an Internet engine, then organized and formatted in a specified manner. Many law firms use a tool called "Goldmine" to store and organize coded data about clients and then to manipulate the data to produce, for example, mailing lists of clients with particular characteristics.

{21} Other information system elements may fall into a category that is intermediate between raw data and search software. Some systems are characterized by "database relationships." In such a system, facts are assigned to tables which are organized according to software-based rules. The data itself is not literally organized as it would be in a paper directory, but on the other hand, the process of organization is not dependent upon the application of an external tool.

{22} A user gathering information through any of these devices may see himself as simply using a "database." Yet, in each case both the logic and logistics of the search will be distinctive. Depending on the source of the data and the search tool or tools employed, different parties will be contributing to the value of the ultimate product in radically different ways. As we shall see in the remainder of this paper, these differences also have important implications for the application of existing intellectual property law and the evaluation of possible change.

{23} A final background thought concerns the variety of creative processes that contribute to the development of the hybrid entities popularly thought of as databases. These processes fall out along another continuum whose endpoints are effort and invention. In its most rudimentary form, the process of collecting and organizing information is a matter of raw human effort. The production of an old-fashioned database like a telephone book falls into this category. To borrow a cliché often used to describe science, this sort of process is ninety-nine percent (99%) perspiration and one percent (1%) inspiration. Courts long ago recognized this reality in developing the "sweat of the brow" doctrine to protect maps, simple directories, and the like. [25] At the other extreme is pure invention. The label "inventive" or "creative" would clearly apply to the development of an entirely new software tool to mine existing data resources.

{24} In the real world of databases, most things fall in the middle. Recall yet again, the example of the grocery discount cards that are a front for market research that can then be resold. [26] The individual items of information that are collected are straightforward. Presumably, they could have been compiled and collated in the past through a vast amount of human sweat, with drones sorting cash register receipts. That sweat has been replaced almost entirely by new search technology. The realization that this previously useless data now has economic value was insightful, if not inventive, and the tools which do the work of compilation are themselves inventive products. But how should one characterize the enterprise as a whole - that thing that is loosely-termed a "database?"

{25} Most digital data-based products result from a combination of effort and invention. This reality gives rise to a number of practical questions that have legal significance. Where, for example, is the boundary between mere effort on the one hand, and invention and creativity on the other? Where does ownership reside? Does it reside with the original collector of the data, the individual who conceived of the new combination, the inventor of the search tools, or some combination of them? And what of the people to whom data pertain? As more and more data goes online, as our tools become more advanced, and as digital property becomes an ever-larger component of our collective wealth, issues like these will only become more vexing.

### **III. Non-Legal Solutions**

{26} Lawyers who deal regularly with technology clients know of their pervasive belief that the law is slow, outdated, and inconsistent. It is therefore, not surprising that the database industry has pressed ahead with non-legal, technological solutions to some of the present and future problems with exclusivity, rivalry, and transparency that we have reviewed. This section provides a brief introduction to some of the more widely used technical measures. It is intended only as an introduction; the field is in fact, both wider and deeper than our remarks suggest, with these and many other measures used in a bewildering array of combinations.

{27} The field of technological protection for digital property is developing very rapidly, but at the moment the most common approaches include server and file controls, encryption, complementary keys, and digital signatures.[27] Server and file controls restrict unauthorized access and thus enhance exclusivity, and indirectly, rivalry.[28] Access can vary from completely uncontrolled (the full contents of the server are available without restriction) to partially-controlled (unrestricted access is granted to only certain data on the server) to completely controlled (no uncontrolled access in any form is permitted).[29] Access control is effected through user identification and authentication procedures that deny server or file access to unauthorized users. "Call back" control provides additional access security by calling back the requestor when log on is initiated. When the user makes a connection, the server immediately terminates the connection and reestablishes it to a location that has been previously registered and authenticated. Alternatively, hardware key systems require the user to verify the connection by inserting a hardware device similar to a credit card into the computer system. The device sends an indecipherable code to the server to verify the identity of the user. Without the hardware key, data or tools on the server cannot be accessed.

{28} A second level of control over access to, and use of, digital property can be exerted through the electronic file containing the work. "Rendering" software allows restriction at the file level. For example, a provider can incorporate code that will control by whom, and to what extent, a protected file can be used. Such code can also establish which rights (read, write, delete, or copy) any given individual may exercise.

{29} Various forms of encryption can promote exclusivity, by limiting access, and transparency, by facilitating authentication, thereby enabling the user to know he is getting what he expected. Encryption amounts to using mathematical algorithms both to "scramble" and "unscramble" the data. It is in essence a high-tech version of the manual encoding and decoding systems familiar to readers of spy novels (for example, move each letter five places down the alphabet, so that "A" is read as "F"). Authorization in the form of a "decryption key" is required to decrypt the encrypted file and to restore it to its original malleable format. In early encryption technologies, only a single key was used. The sender encrypted the message with one key and the receiver decrypted the message with its ancillary key. The sender had one key, and every receiver had an identical ancillary key to decrypt the message. Problems soon resulted with this method. The stealing and changing of keys compromised, respectively, security and access. To resolve these threats, the industry turned to a "complementary key" or "public key" system.

{30} Public key encryption requires two specific keys - a public and a private key. Each person has one



private and one public key. Any number of authorized people may know a person's public key, while each individual's unique private key should indeed be private. Encryption is done with the public key, but decryption can only be done with the private key. At the time of encryption, the sender encrypts the data with the sender's public key, and sets the decryption method according to the recipient's public key, obtained from the recipient or a directory. But without the private key of the intended recipient, the work cannot be read, manipulated, or otherwise deciphered by other parties. Interestingly, it is at present computationally infeasible (within thousands of years) to determine private keys from encrypted messages by brute force trial-and-error methods. However, once a file is decrypted, if other security measures are not included, nothing prevents it from being reproduced and redistributed.<sup>[30]</sup>

{31} Recent advances in digital signatures are also proving to offer substantial security benefits. Digital signatures allow the receiver of a communication to authenticate the source. Digital signatures can also verify that the original contents of the file have not been altered. By exposing fraudulent data transfers, signatures aid in the policing of exclusivity, while the verification function enhances transparency. In one common model, an algorithm called a "hash function" is applied to the message being sent to produce a shorter, scrambled statement, or message digest, which becomes a fingerprint of the message. The sender then encrypts the message digest using the complementary key system discussed above, but in reverse, with the sender's private key used to encrypt and the public key to decrypt. The result is a digital signature. The recipient of the message decrypts the signature and then applies the same hashing algorithm to the message to produce another message digest. A comparison of the two message digests verifies that the message originated from the expected sender and has not received tampering. While digital signatures use encryption in the signature and hashing functions, they do not actually encrypt the work. But digital signatures and encryption can be used simultaneously to optimize security. Some electronic correspondents also append "electronic certificates" to their messages. These are issued by a mutually agreeable, trusted third party and certify that the public key which decodes the signature is in fact, that of the presumed sender.

{32} According to a recent American Bar Association report, digital signatures offer four related advantages.<sup>[31]</sup> First, they minimize the risk of dealing with imposters or persons who attempt to escape responsibility by claiming to have been impersonated. Second, digital signatures minimize the risk of undetected message tampering and forgery, and false claims that a message was altered after it was sent. Third, they are more secure than handwritten signatures, with the threat of forgery virtually negligible. Finally, digital signatures insure a high degree of information security, even for information sent over open, insecure, inexpensive, and widely used channels.

{33} Despite their sophistication, self-help technological approaches like these have not eliminated the demand for legal protections. In some contexts, they are technologically infeasible. In other situations, they would impose a burden on existing and potential users that would be unacceptable from a business perspective. We turn now to a review of the currently available legal protection, identifying along the way some of the instances in which legal and extra-legal measures may interact.

## **IV. Legal Protection: The Current State of U.S. Law**

### **A. The Nature of the Potentially Protectable Rights**

{34} The variety of entities lumped under the heading of "database" comprise a complex array of potentially protectible intellectual property.<sup>[32]</sup> The principal categories include the data elements themselves; the effort used in locating them; the effort and any originality involved in selecting among and arranging the available elements; and the tools for search and organization, together with all aspects of their creation. In this section, we consider the available *legal* strategies to protect these various categories of intellectual property. As

discussed, a lack of confidence in legal protections may drive some database proprietors to use technological means to prevent certain user activities.<sup>[33]</sup> Here, however, we assume the proprietor wishes to enable a full range of uses and to assess the efficacy of the applicable legal strategies.

{35} The objectives of a rationally self-interested database owner will be: (1) to permit authorized persons to use the database fully; (2) to prevent unauthorized persons from using it; and (3) to prevent competitors from copying it in order to create a competitive product. A database owner will judge the adequacy of any form of legal protection according to its capacity to advance these three interrelated objectives. The legal principles of protection are the same whether the subject is a simple paper database like a telephone book or a complex aggregation of data dispersed through cyberspace. However, the way in which those principles are applied will be heavily dependent on the nature of the product. In particular, the appropriate focus of protection for a given database will depend in large part on whether its creators placed primary value in the underlying data structure or in the search and organization tools.

## 1. The Data Elements

{36} The intellectual property status of the data elements to be compiled is typically beyond the control of the compiler. As a general rule, the legal status of the data elements is unaffected by the process of compilation; the rights appurtenant to the constituent elements are passed through from compiler to end-user.<sup>[34]</sup> The raw materials will often be in the public domain, as in the case of telephone book entries,<sup>[35]</sup> the names of cable system operators,<sup>[36]</sup> or the statistics of Major League baseball pitchers.<sup>[37]</sup> A compilation can also include copyrighted works, whose use would require the permission of the copyright holders. A database might even contain trade secret material. In such a case, a law-abiding compiler would seek a license from the trade secret proprietor. Because unrestricted dissemination of the material to innocent third parties might vitiate its trade secret status,<sup>[38]</sup> the proprietor would presumably demand that end-users be placed under contractual obligations of confidentiality. It is difficult to imagine circumstances in which a data element would itself *be* a patented invention, the unauthorized making, using, or selling of which would constitute infringement.<sup>[39]</sup> However, it is conceivable that the inclusion of information about a patented invention could amount to active inducement of infringement, which is itself a form of infringement.<sup>[40]</sup>

## 2. The Research Effort

{37} Prior to the Supreme Court's 1991 decision in *Feist Publications, Inc. v. Rural Telephone Service Co., Inc.*,<sup>[41]</sup> courts occasionally granted copyright protection for the *effort* involved in finding and assembling a body of collected data. Under what came to be called the "sweat of the brow" doctrine,<sup>[42]</sup> a long line of cases protected the "industrious collection" of a compiler, regardless of "whether the materials he has collected consist or not of matters which are of public juris, or whether such materials show literary skill or originality, either in thought or in language."<sup>[43]</sup> In order to avoid copyright infringement, a second user of previously-compiled public-domain information had to make the redundant effort to root it out from the original sources.<sup>[44]</sup> Copyright protection for a compilation thus depended on the quantity, rather than the quality of the work done by both the original collector and subsequent users of the compiled information.

{38} *Feist* explicitly repudiated the "sweat of the brow" doctrine.<sup>[45]</sup> In rejecting copyright protection for a white-pages telephone directory, the Court held that requiring subsequent users to duplicate the original compiler's effort was exactly backwards: far from demanding redundant effort, copyright law - by denying protection to isolated facts and ideas<sup>[46]</sup> - sought to discourage it.<sup>[47]</sup> Henceforth, copyright protection would depend upon the quality of the compiler's work: "originality, not 'sweat of the brow', is the touchstone of copyright protection in directories and other fact-based works."<sup>[48]</sup>

{39} The *Feist* Court did leave open the possibility that unoriginal effort alone might be eligible for legal protection other than copyright.<sup>[49]</sup> Suggesting the availability of unfair competition protection, the Court

mentioned its 1918 decision (never overruled) in *International News Service v. Associated Press*.<sup>[50]</sup> There, the defendant was enjoined from repackaging news items originally reported by the Associated Press and then selling them to its own subscribers. While the Court acknowledged that the factual items that comprise the news are not literary works eligible for copyright protection,<sup>[51]</sup> it found that the common law of unfair competition would not allow a competitor "to reap where it has not sown."<sup>[52]</sup> Although *INS* was decided on the basis of federal general common law, a category extinguished by the Court's 1938 decision in *Erie Railroad v. Tompkins*,<sup>[53]</sup> a few courts have recognized non-copyright protection for facts amounting to "hot news" in state laws of misappropriation.<sup>[54]</sup>

{40} A prospective plaintiff's enthusiasm for the *INS* cause of action must be tempered by the realization that misappropriation theories that purport to prohibit copying of compiled information are usually held to be preempted by the Copyright Act.<sup>[55]</sup> A state-law cause of action will survive preemption only if it protects intellectual property not within the subject matter of copyright and/or asserts rights not equivalent to copyright.<sup>[56]</sup> Cases decided under the Copyright Act of 1976 have uniformly held compilations of facts to be within the subject matter of copyright <sup>[57]</sup> and have allowed misappropriation claims only when they include the "extra elements" (that is, in addition to proof of copying) that were present in *INS* itself: the time-sensitive value of the facts, free-riding by the defendant, and a threat to the existence of the plaintiff's product or service.<sup>[58]</sup>

{41} Another avenue for protecting industrious collection is to enter into contracts with users. An agreement with a database user might, for example, allow access only for research purposes and prohibit dissemination of the contents to others. There are both practical and legal problems with this approach, however. On a practical level, it is difficult to establish, police, and enforce contractual relations with users of a database that is widely available, such as one on the Internet. The proprietor's options include demanding that users assent to a "click-on" license, with or without user identification, as a condition to access and/or downloading capability, and even charging for these privileges. Such steps will deter some casual abusers, and a fee will insure some return on the proprietor's effort. But the material passes out of the proprietor's control once downloaded, and a list of thousands of prospective shallow-pocket defendants would be of little practical value. Moreover, the more onerous the restrictions, the more potential users are driven away, which will have consequences for generating revenue through advertising.<sup>[59]</sup>

{42} The principal legal concerns are contract enforceability and possible copyright preemption. Presumably, old-fashioned, face-to-face contracting will be possible only in the case of specialized users of high-end, limited-access databases. For the majority of Internet situations, something analogous to software shrinkwrap licenses will have to suffice. Few cases have dealt with the enforceability of shrinkwrap licenses, but in the most recent and perhaps most authoritative of these, *ProCD, Inc. v. Zeidenberg*,<sup>[60]</sup> the Seventh Circuit held that a shrinkwrap license is an ordinary contract that is enforceable under the Uniform Commercial Code ("U.C.C"). Writing for a unanimous panel, Judge Frank Easterbrook relied largely on the accepted economics of the software market.<sup>[61]</sup> The court also ruled that state-law enforcement of such contracts is not preempted by the Copyright Act. This is because a copyright, which "is a right against the world," is in no sense "equivalent to" a contract, which binds only its parties.<sup>[62]</sup>

{43} The *ProCD* decision is not, however, a guaranty that contractual limits on the use of mass-marketed databases will be uniformly enforceable. First, *ProCD* dealt with traditional shrinkwrap packaging for software, and treated it as a "sale" governed by Article 2 of the U.C.C. Other courts might take a different analytical perspective on click-on contracts intended to limit database use. Second, however persuasive its analysis might be, *ProCD* is a single case applying the contract law of a single state. The status of shrinkwrap licenses and analogous contracts is undecided in most states.<sup>[63]</sup> Finally, the *ProCD* court's view of preemption is not universally shared. In 1988, in *Vault Corporation v. Quaid Software, Ltd.*, the Fifth Circuit held that a Louisiana statute which made shrinkwrap licenses enforceable was preempted.<sup>[64]</sup> Although *Vault* has attracted little positive attention in the subsequent case law,<sup>[65]</sup> David Nimmer, who succeeded his late



father as the principal author of the influential treatise *Nimmer on Copyright*,<sup>[66]</sup> argues vigorously in the current edition that *ProCD* was wrongly decided and that similar contractual attempts to limit database use are preempted.<sup>[67]</sup> Nimmer's point is that *Feist* has declared facts to be unprotectible elements of works that are generally within the subject matter of copyright. Therefore, any attempt to protect facts by other means must run afoul of either Section 301 of the Copyright Act or a general theory of preemption that, he claims, operates independent of Section 301.<sup>[68]</sup> Passing judgment on Nimmer's argument is beyond the scope of this article. Suffice it to say that contractual protection of the research effort is not a sure thing from a legal perspective. Even if it were, one comes inevitably back to the practical problem: with apologies to P.T. Barnum, a million clicks of assent to a restrictive license are probably not worth the electrons by which they are transmitted.

### 3. The Selection and Arrangement of the Data

{44} It is abundantly clear that legal protection for the intellectual process of selecting and arranging data in a compilation must come, if anywhere, from copyright law. Section 103 of the Copyright Act expressly includes within the subject matter of copyright contributions made by authors of compilations.<sup>[69]</sup> The definitions section then sets the standard for a protectible compilation: "a work formed by the collection and assembling of preexisting materials or of data that are selected, coordinated, or arranged in such a way that the resulting work as a whole constitutes an original work of authorship."<sup>[70]</sup> A state-law attempt to protect the process of compilation upon some lesser or different showing would amount to a "junior" copyright - an obvious violation of Section 301.

{45} *Feist*, of course, is the authoritative statement of how much originality is required for copyright purposes. In theory, the requirement is minimal: "[o]riginal, as the term is used in copyright, means only that the work was created by the author (as opposed to copied from other works), and that it possesses some minimal degree of creativity. . . . [T]he requisite level of creativity is extremely low; even a slight amount will suffice."<sup>[71]</sup> The white-pages phonebook at issue in *Feist* fell well short of even this minimal standard. Although the plaintiff might have invested substantial effort into collecting its listings, the arrangement followed the standard alphabetical scheme, and thus involved no creativity at all.

{46} Once the "sweat of the brow" doctrine had been abrogated, *Feist* was an easy copyright case - too easy, perhaps, in light of the difficulty that subsequent courts have had in applying in it. A white-pages phonebook is perhaps the least creative compilation imaginable. Consequently, virtually every other reported compilation case involves a stronger case for copyright protection than *Feist* itself. By choosing the weakest possible case to articulate the originality standard, the Supreme Court offered no guidance to the lower courts on the question of how much more creative than the white-pages a compilation must be in order to qualify for copyright protection. Several recent decisions illustrate the ensuing confusion.

#### a. *Sufficient originality found*

{47} One of the first reported cases to cite *Feist* also involved a telephone directory. In *Key Publications, Inc. v. Chinatown Today Publishing Enterprises, Inc.*,<sup>[72]</sup> the plaintiff published a directory of New York's Chinese business community. Plaintiff Key collected business cards from business and professional people, copied some restaurant listings from another directory, and ultimately produced a "yellow pages" that included about 9,000 listings organized into 260 business categories. Each consisted of an English and Chinese name, an address, and a telephone number.<sup>[73]</sup> The defendant's directory contained 2,000 listings, 1,500 of which also appeared in the Key directory, organized into twenty-eight categories, only three of which were also used by Key.

{48} The Second Circuit affirmed the district court's finding that the Key directory was sufficiently original to warrant copyright protection, but reversed its judgment of infringement. On the first issue, the court of



appeals agreed that the process of selection undertaken by Key's president was sufficiently creative to satisfy *Feist*. It cited her initial judgment to select only those New York businesses that would be of interest to the Chinese-American community, and her testimony that she subsequently exercised discretion in excluding individual businesses that she thought would not remain open for very long. These acts of "thought and creativity" distinguished the Key directory from the typical white-pages, whose compiler "slavishly" includes every available listing.<sup>[74]</sup> The Second Circuit reversed the judgment of infringement, however, on conventional substantial similarity grounds. The court emphasized that the defendant had duplicated only three of Key's twenty-eight categories, had omitted 7,500 of Key's 9,000 categories, and had not duplicated any significant groupings of listings. The court concluded as a matter of law that "the principles of selection determining the listings"- the only "copyrightable" element of the Key directory - were not sufficiently similar in the two works to support a finding of infringement.<sup>[75]</sup>

{49} A more recent post-*Feist* case that applies a minimal originality standard is *Oasis Publishing Company v. West Publishing Company*,<sup>[76]</sup> the latest in a string of home-court victories for the Minnesota-based legal publisher. In the pre-*Feist* case of *West Publishing Company v. Mead Data Central, Inc.*,<sup>[77]</sup> West had established a compilation copyright in the arrangement of cases in its National Reporter System. In *Oasis*, a competitor intended to convert the decisions (but not the headnotes, synopses, or syllabi) in West's *Florida Cases* to CD-ROM format.<sup>[78]</sup> Oasis planned to display parallel citations to *Florida Cases* at the start of each case, and also to "star paginate" its cases - that is, to show the internal page breaks and page numbers as they appear in *Florida Cases*. West claimed that both the citations and the page numbers were aspects of its copyrighted case arrangements. West conceded that the use of parallel citations would be fair use,<sup>[79]</sup> but insisted that Oasis's star pagination would infringe upon West's compilation copyright.<sup>[80]</sup>

{50} *Mead* had previously held that West's internal pagination was the expression of its copyrighted case arrangement, and thus could not be copied by a competitor. Oasis now contended that *Mead* had relied on the "sweat of the brow" doctrine, and was thus overruled by *Feist*, but the court rejected this contention out of hand.<sup>[81]</sup> Tracking *Mead's* analysis, the court recited the acts of creativity involved in West's arranging of cases: West first divides cases by state, then by court level; next, within each state and court level, it orders the decisions according to whether they are opinions, memoranda, or table dispositions; finally, it orders table dispositions alphabetically and other cases by date. The court emphasized that West's attorney-editors frequently exercise discretion to override the system, as by taking a case out of chronological order to pair it with a related case in the same volume.<sup>[82]</sup>

{51} Oasis attacked West's position on two fronts. First, Oasis contended that if a citation to the first page of a case was concededly fair use, then the subsequent page numbers could not command copyright protection because their determination was a rote process. In other words, given the first page number of a case, the setting of the rest of the page numbers involved no creativity. The court brushed this argument aside on the authority of *Mead*, holding that the arrangement process just described was sufficiently creative to merit copyright protection, and that internal pagination was an integral part of the arrangement.<sup>[83]</sup>

{52} Oasis's second argument was closely related to the first, but was directed at infringement rather than copyrightability. Oasis contended that internal pagination revealed nothing more about West's arrangement than initial pagination did.<sup>[84]</sup> Therefore, if, as West conceded, it was lawful to copy initial page numbers, it could not be infringement to copy subsequent page numbers, as well. The court was no more receptive to this argument than it had been to the first, but its logic was obscure. The critical fact in the court's view was that "by determining an internal page from each case in a given volume, the user could sort and determine West's arrangement with Oasis' CD-ROM product."<sup>[85]</sup> But what about Oasis' contention that the user could do exactly the same thing with the first-page parallel cites, which concededly were unprotected? The court's unsatisfying response was that the publication of parallel cites would not supplant the need for West's product, whereas the internal cites would. It is not clear why market effects are relevant to deciding whether a given work is an infringing copy. It is even less clear why the disclosure of the nature of West's arrangement

constitutes an infringing reproduction of that arrangement.[86]

b. *Insufficient originality found*

{53} West Publishing has fared less well on the road. In two cases captioned *Matthew Bender & Company, Inc. v. West Publishing Company*,[87] the Second Circuit denied copyright protection to many of the selection and arrangement aspects of West's case reports. In the first *Bender* case, the defendant published HyperLaw, a CD-ROM compilation of federal decisions.[88] It copied the text of the opinions from West, but deleted West's syllabi, headnotes, and key numbers. However, HyperLaw did copy certain other enhancement features that West adds to the judicial text: information about parties, counsel, court, and date of decision; annotations about subsequent procedural developments; and the editing of parallel citations in the reported cases to insure uniformity of style. West asserted that each enhancement feature reflected creative choices. The Second Circuit disagreed, affirming the district court's grant of declaratory relief to HyperLaw. The court held that all of the information was factual in nature, and that the information had not been compiled or arranged with even the minimal creativity required by *Feist*. On the contrary, every decision that West made about format or arrangement was dictated by convention. While West's work "entails considerable scholarly labor and care," the court observed, "creativity in the task of creating a useful case report can only proceed in a narrow groove." [89] In fact, a competitor seeking to produce its own reports would be hard-pressed to do anything differently.[90]

{54} In the second case, the Second Circuit rejected claims identical to those that been endorsed in *Oasis* and the earlier *Mead Data* decision. Here, as in those cases, the issue was whether a competing publisher could include "star pagination" in its compilation of case reports - that is, to display the internal page numbers and breaks that appear in West reporters.[91] West had again conceded that copying initial page numbers was fair use. West asserted "an indirect infringement theory" to the effect that Bender's star pagination would infringe by allowing users to perceive West's arrangement of cases, to page through them as arranged, and ultimately to print cases exactly as published by West.[92]

{55} Explicitly repudiating both *Oasis* and *Mead Data*,[93] the Second Circuit rejected West's theory on several grounds. First, it held that a work which simply permits a user "to rearrange the material into the copyright holder's arrangement" does not amount to an infringing copy - an issue never addressed in *Oasis*. [94] An alternative phrasing of this conclusion is that Bender's work was not substantially similar to West's. [95] Nor could Bender be charged with contributory infringement, because West had failed to identify any primary infringer.[96] Finally, the court disparaged the *Oasis-Mead-Data* notion that a work which can supplant the original, is by definition, a copy. Those cases, the Second Circuit held, had no basis, other than the defunct "sweat of the brow" doctrine, for equating a "reflection" of West's arrangement with a "copy." [97]

{56} A recent Eleventh Circuit en banc decision, *Warren Publishing, Inc., v. Microdos Data Corporation*, [98] is an interesting counterpoint to the *Key Publications* directory case. The work at issue in *Warren* was the plaintiff's *Television & Cable Factbook* - as the title suggests, a compilation of information about the cable industry. In publishing its own computerized cable database, defendant Microdos allegedly copied elements from *Factbook*, in particular, an extensive directory of U.S. cable systems. Warren's claim of originality in its directory rested on what the district court called "a system for selecting communities which is unique in the industry." [99] Rather than listing cable systems by the name of the system or the name of each community it served (as the official Federal Communications Commission ("FCC") compilation does), Warren chose the principal community served by each system, and listed all information under that heading. The district court found that the selection and arrangement of the various communities was "an obvious, mechanical, or routine task which required no creativity." [100] However, it held that the underlying decision to organize by principal community was a sufficiently creative choice to render the directory protectable.[101]

{57} The court of appeals found a fatal flaw in the lower court's use of the word "system," holding that copyright protection for a system of selection "is contrary to the plain language of 17 U.S.C. § 102(b), and is clearly wrong." [102] Moreover, the court found, even if the system were somehow subject to protection, it would fail the originality test, since Warren "selected" and included every cable system listed by the FCC. It compared this - unfavorably - to the selection made in *Key Publications*, where "the compilation copyright holder did not include the entire relevant universe in her directory." [103] The final nail in the coffin was the fact that the designation of principal communities was made not by Warren, but by cable operators responding to a survey. Even if Warren were the first to do such a survey, primacy would "not translate these acts of discovery into acts of creation entitled to copyright protection." [104]

{58} A final variation on the originality theme is presented by *Kregos v. Associated Press*, [105] decided by the Second Circuit two years after *Key Publications*. The work at issue in *Kregos* was a "pitching form," a compilation of statistics about the starting pitchers in upcoming baseball games that is primarily of interest to gamblers. [106] The Second Circuit's final opinion was actually the fourth reported decision in this protracted litigation. [107] Previously, the district court had held that *Kregos*' form was not copyrightable as a matter of law because it lacked sufficient originality and creativity; the court relied in part on the "blank forms" doctrine, which has barred protection for things like check stubs. The court of appeals reversed and remanded for reconsideration of the amount of originality and creativity present in the pitching form, holding the blank form doctrine inapplicable because the pitching form conveyed information. On remand, the district found sufficient originality, but held that there was no substantial similarity between *Kregos*' form and those used by the defendant wire service.

{59} In affirming the finding of no infringement, the Second Circuit approached the problem from multiple complementary angles. First, it reiterated that the pitching form was a sufficiently original work to merit some measure of copyright protection, at least in the abstract. [108] The court then took note of the merger doctrine, which can render meaningless the copyright in simple functional works whose ideas can be expressed in essentially only one way. [109] Here, however, merger did not apply because "there are a variety of selections *Kregos* could have chosen for his form." [110] Comparing the plaintiff's and defendant's forms, the court observed that six of the ten statistics presented on the two forms were identical. However, it concluded, much of the overlap was influenced by the common purpose of the two forms - a weak version of the merger doctrine that it had just rejected. In light of this rationale, the defendant's selection of four different statistical categories was enough to avoid a finding of substantial similarity. [111]

{60} The principal relevance of *Kregos* to database protection is its emphasis on the potential role of functional constraints. Think of *Kregos*' pitching form as a very simple statistical database. Its selection of data was sufficiently creative to yield a nominal copyright. That copyright was robust enough to survive an abstract legal challenge. Yet it had no practical value for its owner because it could not support a finding of substantial similarity: those similarities that were observed were written off to function, while even minimal differences were enough to avoid substantiality.

### c. Conclusions for databases

{61} The post-*Feist* compilation cases prompt several inferences about the copyright status of databases:

\**Feist has raised the originality bar.* The standard may be minimal, but it is a standard, nonetheless. Courts are no longer free to ignore the originality requirement, or to substitute "sweat of the brow."

\**We still know very little about the principles to be applied to computerized databases.* *Feist* itself, of course, involved the most primitive sort of paper database, a telephone book. In some of the other cases (*e.g.*, *Warren* and the *West* cases), at least one of the competing works was in digital form. However, the courts treated even these works as if they were simply alternative versions of such familiar paper compilations as case reporters



and directories. Thus, when we speculate about the legal fate of things like Internet databases accessed with powerful search engines, we should remember how little we actually know at this point.

*\*The more comprehensive the database, the less copyright protection may be available.* The keys to protection are selection and arrangement. As the *Warren* cable directory case reminds us, if everything is included, then there is no selection. The existence and depth of any copyright will rest entirely on the originality of the arrangement. This principle may be especially problematic for digital databases such as those accessed through the Internet, since their very appeal is their all-inclusiveness.

*\*The form of the selection and arrangement must be original to the database creator and separable from the dictates of function.* As several of the post-*Feist* cases illustrate, it is fatal to copyright if the selection and arrangement either (1) follow principles already developed, or (2) are constrained by function. "Function" can mean a variety of things, including established convention (the alphabetical listings in *Feist* itself), the demands of the user market (the pitching forms in *Kregos*), or the data themselves (the attorney and court information in the *West* cases). The merger doctrine is a variation on this theme, applicable when the underlying idea is capable of only a narrow range of expression. These also may be particularly difficult issues for Internet databases, given the rapid growth of search conventions and the need of database creators to satisfy mass user audiences.

#### 4. Search and Organization Tools

{62} The tools for searching and organizing data enjoy the same level of protection as other computer programs. The scope of and limitations on software copyrights are massive topics well beyond the scope of this article. Although individual cases continue to pose difficult questions of application, there is now a general consensus about the applicable legal principles, as a result of the near-universal acceptance of the "abstraction-filtration-comparison" test promulgated by the Second Circuit in *Computer Associates International, Inc. v. Altai, Inc.*<sup>[112]</sup> In addition, the Federal Circuit's recent decision in *State Street Bank & Trust Co. v. Signature Financial Group, Inc.*<sup>[113]</sup> appears to have eliminated any doubt that software-based processes and systems comprise patentable subject matter as long as they manipulate data for some useful purpose. Indeed, *State Street* all-but invites claims in the form of "a data processing system for [doing almost anything useful]."<sup>[114]</sup> Thus, information systems whose value lies primarily in their search and organization tools will find protection under the well-established principles of both copyright and patent law.

#### 5. Technical Measures and the Digital Millennium Copyright Act<sup>[115]</sup>

{63} The Digital Millennium Copyright Act ("DMCA"), a massive piece of legislation enacted in October 1998, may have a significant if unintended impact on the protection of databases. The relevant portion of the DMCA implements the 1996 World Intellectual Property Organization Copyright Treaty by adding to the Copyright Act a new Chapter 12 entitled "Copyright Protection and Management Systems."<sup>[116]</sup> Subject to a number of exceptions, it is now a copyright offense to "circumvent a technological measure that effectively controls access to a work protected under [Title 17]," or to manufacture, sell, or traffic in products whose only significant purpose is circumvention.<sup>[117]</sup> The new chapter provides a full range of civil remedies and criminal penalties.<sup>[118]</sup>

{64} As a result of Chapter 12, technological protections for copyrighted works, formerly referred to as "non-legal," are transformed into legal protections as well. A logical question is whether the DMCA has effectively closed all remaining gaps in the wall of legal protection for digital databases. The argument that it has is simple: regardless of the scope of copyright or other existing protection, the proprietor of a database can achieve fool-proof protection by employing technical barriers to unauthorized copying. If the barriers work, there will be no unauthorized copying; if they fail and are circumvented, the act of circumvention will itself violate the Copyright Act.



{65} As superficially appealing as it may be, this reasoning has several possible flaws. The first problem is that, for reasons discussed earlier, some database proprietors will not want to use technological measures. [119] Many proprietors tolerate or even encourage small-scale copying by ordinary users; their only concern is massive appropriation and remarketing of their data by competitors.

{66} The second problem involves the legal meaning of the phrase "a work protected under this title." If the DMCA is to fill in the gaps in existing copyright protection, then this phrase must be interpreted to mean "a work falling generally within the subject matter of copyright." If this is the meaning, then circumventing a measure designed to protect a database - a compilation, clearly within the subject matter of copyright - would be illegal, regardless of how thin that copyright might prove to be. A court hearing a Chapter 12 case would never reach the sort of issues that have been dispositive in the post-*Feist* cases.

{67} It is also possible to interpret the phrase to mean "a work protected under this title, *but only to the extent of such protection*." Under this interpretation, a court in a Chapter 12 case would first have to determine the extent of the traditional copyright protection in the work in question. Circumventing technological measures would then be illegal only to the extent that those measures protected copyrightable expression. It would not violate Chapter 12, for example, to circumvent measures protecting unoriginal arrangements of raw facts, as in *Feist* itself. If this were the proper interpretation, then Chapter 12 would do little more than add a new remedy to existing copyright law.

{68} As a matter of common sense, the latter reading seems strained. The more straightforward approach is to take "work protected under this chapter" as inviting a general consideration of the nature of the work, not full-blown copyright litigation. Nonetheless, the question of interpretation will remain open unless and until authoritatively answered by the courts.

{69} A final potential issue is a species of the "gray market" problem. That is, what happens if a technological protection for a database is disabled abroad? Can the database then be freely used outside of the United States, or even imported back into this country? The answer to both questions is certainly "no." First, recall that the DMCA technological measures legislation was intended to implement a WIPO treaty. This means that most other countries will have similar legislation in place, and will offer reciprocal national treatment to authors from other signatory countries. [120] In addition, the U.S. Copyright Act already prohibits the importation, without authority of the copyright holder, of any copies of a protected work that have been acquired outside the United States. [121] A separate provision forbids the importation of copies made under circumstances that would have constituted an infringement if U.S. law had applied. [122]

## B. The Perceived Shortcomings in U.S. Law

{70} Each of the past two United States Congresses has seen a failed attempt to create non-copyright, *sui generis* protection for databases more or less on the European Union model. [123] Comparable legislation is pending in the current Congress. [124] This activity reflects a perception that is widespread, at least among the proprietors of information systems, that the current level of protection is inadequate. [125] Among the principal concerns are the following, each of which has been identified in the legal discussion above.

1. Post-*Feist* copyright protection is too "thin." Although the *Feist* standard is low, it is working to eliminate or at least vitiate protection for many databases that are the product of substantial "sweat" (and investment), but little creativity. Moreover, even when copyright protection does exist in theory, it is often nominal in application.

2. Unfair competition and misappropriation remedies are likely to face preemption. To survive, such remedies cannot be merely "copyright lite" causes of action, but must include extra elements such as time-sensitivity of the data or free-riding. However, what many database proprietors really want is precisely what the

preemption doctrine forbids: a simple prohibition against copying compilations that are insufficiently original for copyright purposes. In addition, even those state-law protections that do survive are too spotty and inconsistent to be relied upon in a global marketing environment like the Internet.

3. Contract protection is often infeasible, both practically and legally. For many database proprietors, it will be impossible to obtain assent to restrictive contracts, or inconsistent with their business objectives. Notwithstanding some recent positive developments, there are still lingering questions about the enforceability of "click-on" licenses, and even contract law faces possible preemption problems.

## **V. The Available Legal Options**

{71} Those in the database industry who take these concerns seriously have been promoting a European-style solution for the last several years. The key element is a non-copyright, *sui generis* form of protection. In this section we review the European approach, and then describe the ongoing effort to enact such legislation in the U.S. Congress.

### A. The European Response

{72} In 1996, the European Union ("EU") enacted a Directive (the "Database Directive")<sup>[126]</sup> for the purpose of bringing more uniformity to the protection of databases within the EU, while ensuring that there would be a level of protection adequate to encourage their continued creation.<sup>[127]</sup> Each member state was required to enact a law consistent with the Database Directive by 1998.<sup>[128]</sup>

{73} The Database Directive limited the availability of copyright protection for databases,<sup>[129]</sup> and to fill the gap resulting from that limitation, created a new *sui generis* right protecting the makers of databases.<sup>[130]</sup> The Database Directive specifically provided that the existing Directive on the protection of computer programs (the "Software Directive")<sup>[131]</sup> would continue to specify the appropriate level of copyright protection for search engines and related software tools.<sup>[132]</sup> The Database Directive made no change in either trade secret or patent law. The remainder of this section describes in more detail the current level of database protection in the EU.

#### 1. Copyright Protection

{74} Prior to the enactment of the Database Directive, the scope of copyright protection for databases varied significantly from country to country. The United Kingdom and Ireland had very low originality requirements and routinely protected works with minimal creativity,<sup>[133]</sup> such as the telephone directory at issue in *Feist*. The rest of the EU countries were more focused on the level of the author's original creative work, and generally did not provide copyright protection for a work, like a telephone directory, that had minimal originality.<sup>[134]</sup>

{75} The Database Directive rejected the approach being used in the United Kingdom and Ireland and raised the threshold for copyright protection by specifying that there would be no copyright protection unless "by reason of the selection or arrangement of the contents of the database, the database constitutes the author's own intellectual creation."<sup>[135]</sup> This standard is very similar to the standard that is applied in the United States after *Feist*<sup>[136]</sup> with one additional limitation: under the Database Directive, there must be intellectual creation by a human author<sup>[137]</sup> for copyright protection to exist, raising questions about the extent to which a database can be protected under copyright law if the selection and arrangement of data is accomplished by a computer program with minimal human contribution.

{76} As a result of the Software Directive, copyright law in the EU will continue to provide meaningful protection for software, so it will remain important in the protection of search tools. However, in the case of most databases, it seems unlikely that the compilation itself will exhibit the type of intellectual creation required for copyright protection. Thus, as a result of the Database Directive, copyright law is likely to play a less significant role in the protection of databases.

## 2. Trade Secret Protection

{77} EU law does not deal in a uniform manner with the protection of commercial trade secrets.<sup>[138]</sup> Rather, each member state retains its own laws in this area. While the laws vary to some extent, most countries provide some type of civil and criminal protection against the misappropriation of confidential commercial information, whether by breach of a contract or other wrongful conduct.<sup>[139]</sup> The Database Directive specifically provides for the survival of national laws concerning, among other things, trade secret rights in the data elements contained in a database.<sup>[140]</sup> With respect to electronic databases in which the access to data is restricted by technical means, the EU is in the process of adopting a directive that will prohibit the circumvention of technical protections in the same manner as the U.S. Digital Millennium Copyright Act.<sup>[141]</sup> This new provision, working in concert with existing national trade secret law, should be broad enough to protect against most kinds of "data dumps." Trade secret law should also provide at least some protection against the misuse of confidential information relating to the manner in which the data in a database has been selected, verified and arranged. Thus, trade secret law in the EU can provide partial, but often very useful, protection for databases.

## 3. Patent Protection

{78} Article 52(2) of the European Patent Convention <sup>[142]</sup> provides that "programs for computers" are not to be regarded as patentable "inventions." In practice, patents have been routinely granted for software-based inventions under conditions similar to those obtained in the United States prior to the *State Street* decision. <sup>[143]</sup> "Thus inventions for a technical process which are implemented by a computer program are considered patentable, providing the claims are directed to method steps performed by the program, or to a computer system including both hardware and the computer program." <sup>[144]</sup> Claims directed to the program itself are unpatentable. <sup>[145]</sup> Since a patent claim on a typical database -- an unlikely prospect in any event -- would be more likely to fall into the latter category than the former, patent law is not currently a realistic source of database protection in the EU. At least one practitioner has argued that European law can and should be modified in a manner consistent with *State Street*,<sup>[146]</sup> so it is possible the patent law will play at least some role in database protection in the EU in the future.

## 4. The New *Sui Generis* Right

{79} The Database Directive created a new *sui generis* right <sup>[147]</sup> that protects the economic investment of the "maker" of a database by prohibiting third parties from extracting or re-utilizing the contents of the database without the consent of the maker. The right is subject to certain exceptions that resemble, but are narrower than the fair use exceptions under copyright law. The *sui generis* right supplements, but does not replace copyright protection.

{80} The "maker" of a database is the individual or company who takes the initiative in creating the database and who assumes the financial risk. <sup>[148]</sup> The maker may be different from the "author" of the database, so different persons or companies may hold the copyright and the *sui generis* right in a particular database. <sup>[149]</sup> To qualify for protection under the *sui generis* right, the maker must have made a substantial investment in "the obtaining, verification or presentation" of the data. <sup>[150]</sup> In the case of an individual, he or she must be a national or resident of one of the member states of the EU. <sup>[151]</sup> A company will qualify if (1) it is created under the laws of one of the member states and has a substantial presence in a member state, or (2) it has a

registered office within the EU and "its operations [are] genuinely linked on an ongoing basis with the economy of a Member State." [152] This latter provision is clearly biased against smaller companies in the U.S. and other non-EU countries, since, even if they do establish an EU office, they are less likely than their multinational counterparts to be able to show ongoing economic linkage.

{81} Not every compilation of information will be considered a "database" for the purpose of the *sui generis* right. To qualify for protection, a database must be "a collection of independent works, data or other materials arranged in a systematic or methodical way, and individually accessible by electronic or other means." [153] The requirement of independence is intended to exclude works such as a film, which literally is composed of a collection of still frames, but in which the still frames are not independent of each other. [154]

{82} The requirement that the data be "arranged" does not specify any physical storage arrangement, [155] and it should be sufficient that specific attributes be assigned to each item of data. It should be enough, for example, for data to be organized into fields, or for facts to be assigned to tables which are then related by rules. However, the requirement of arrangement would presumably exclude protection for a database that is no more than an unorganized compilation of data that can be searched and retrieved by a search engine.

{83} If a database qualifies for the *sui generis* protection, no third party will have the right to extract or reutilize "all or a substantial part" [156] of the contents of the database for a fifteen year period. [157] This right is much broader than it would at first appear, since the Database Directive expressly provides that the repeated and systematic extraction or re-utilization of insubstantial parts of a database may amount to the extraction or re-utilization of a substantial part. [158] This is an important distinction, since the typical use of a database involves this very type of access. Each member state is free to determine its remedies for the infringement of the *sui generis* right. [159]

{84} The *sui generis* right is not absolute. A maker of a database that is made available to the public cannot prevent a lawful user of the database from extracting or re-utilizing insubstantial parts of it. [160] In addition, the *sui generis* right is subject to certain exceptions for non-commercial uses related to teaching, scientific research, and public security. [161] These exceptions are narrower than the similar fair use exceptions under copyright law. [162] For example, the *sui generis* right has no exceptions for criticism, news reporting, satire, or library use.

## 5. The Impact of the Privacy Directive

{85} The underlying premise of the Database Directive is the notion that the development of databases should be encouraged because they are an essential tool in the development of an information market. [163] The Database Directive seeks to provide a level of protection that will be adequate to encourage the financial investment and risk inherent in the creation of databases. However, any assessment of the adequacy of database protection in the EU must take into account the provisions of the Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Movement of Such Data [164] (the "Privacy Directive"). The Privacy Directive established a fundamental individual right of privacy that is far broader than any comparable notion in the United States. Each member state was required to adopt a law prior to October 28, 1998 that established a national regulatory body for the protection of personal data, [165] required the prior consent of an individual for the collection and use of personal data, [166] required disclosure to the individual of the purposes for which the data was being collected, [167] and prohibited the transmittal of personal data to other countries that lack "adequate laws" for the protection of personal data. [168] The United States is presumably in danger of being so categorized, with unrealized consequences that are still difficult to predict. [169]

{86} Taken together, the provisions of the Privacy Directive may significantly increase the costs of creating and maintaining databases in the EU while decreasing their usefulness, with the net effect of raising the level



of protection that a business may demand before investing the time and money required to create one. It is too early to tell whether the EU has struck an appropriate balance between creating economic incentives for the creation of databases and protecting the privacy of individuals.

## B. The U.S. Legislative Response

{87} In this country, the database industry's first major initiative was the Database Investment and Intellectual Property Antipiracy Act of 1996, introduced in the 104th Congress in the spring of 1996 as H.R. 3531. The bill proposed a *sui generis* database right essentially on the European model.<sup>[170]</sup> However, it went beyond the EU Database Directive by establishing a twenty-five year (versus fifteen) term of protection and by giving database proprietors a broader right of exclusion. Whereas, the EU Database Directive prohibits only extraction and reuse of data, H.R. 3531 would have limited any use - even certain uses of insubstantial portions of the protected database - that might affect the proprietor's market or conflict with the owner's normal exploitation of the data. The bill also lacked a fair use or public interest exception. Largely because of the latter shortcoming, it was attacked by the scientific and academic communities as portending the monopolization of pure knowledge. H.R. 3531 died in the House Judiciary Committee.<sup>[171]</sup>

{88} Two major initiatives, each less expansive than H.R. 3531, were launched during the 1997-98 Congressional session. The Information Technology Association of America ("ITAA"), an Arlington, Virginia-based trade association, argued for legislation based on state laws of misappropriation.<sup>[172]</sup> The ITAA proposal would have created a cause of action in favor of a database producer against a person who made unauthorized use of information generated by a substantial investment of time or money, if the use competed directly with the producer's authorized products and served as a disincentive to the creation of such products.

{89} The second approach was that taken by H.R. 2652, introduced in October 1997 by Rep. Howard Coble (R-N.C.).<sup>[173]</sup> H.R. 2652 was considerably more aggressive in its protection than the ITAA proposal. Like the previous year's H.R. 3531, H.R. 2652 followed the EU model in broadly prohibiting the use of "all or a substantial part of a collection of information gathered, organized, or maintained by another person through the investment of substantial monetary or other resources, so as to harm that other person's actual or potential market for a product or service."<sup>[174]</sup> H.R. 2652 departed from the EU model in imposing no time limit on the protection. However, unlike its predecessor, the 1997 bill enumerated a number of "permitted acts," including the extraction or use of individual items of information or insubstantial parts of a protected collection, or using protected information for purposes of verifying independently gathered data, conducting non-profit research in a manner that does not hurt the actual or potential market for the database, or reporting the news.<sup>[175]</sup> Notwithstanding these limitations, H.R. 2652 was the subject of a protracted lobbying struggle between the database industry, and academic and scientific communities.<sup>[176]</sup> Among the specific concerns of the latter group were the absence of a time limit, the ambiguous phrase "collection of information," which could extend to bodies of knowledge well beyond the conventional definition of a database, and the limitation of the research exemption to uses that do not threaten the market for the protected database. Along these lines, of particular concern was the argument that any injection of information into the public domain would be viewed as a threat to the market for a proprietary database. Although the bill seemed to have been drafted almost entirely from the proprietors' perspective, both sides were dissatisfied with the indeterminacy of the phrase "substantial part." The Justice Department also entered the dispute with questions about the constitutionality of the bill.<sup>[177]</sup>

{90} The House passed H.R. 2652 in May 1998, and then passed it again as part of the House version of what was to become the Digital Millennium Copyright Act. However, the Senate deleted the provisions of H.R. 2652 from the DMCA before both houses passed that legislation in October 1998. While this was going on, Senator Orrin Hatch (R-Utah) attempted to reach a compromise between industry and research interests, but his efforts proved unavailing.<sup>[178]</sup>

{91} Rep. Coble, Sen. Hatch, and the ITAA all promised renewed efforts in the 106th Congress. On January 19, 1999, Rep. Coble introduced a new Collections of Information Antipiracy Act ("CIAA") as H.R. 354. The bill is almost identical to the failed H.R. 2652, with two potentially significant differences: H.R. 345 includes a fair use exemption<sup>[179]</sup> and limits protection to a period of fifteen years after the misappropriated portion of the database was first offered in commerce.<sup>[180]</sup> An ITAA representative has indicated that its proposal will move from a misappropriation to an unfair competition model.<sup>[181]</sup> The organization's bill will protect "databases" rather than "collections of information," and the cause of action will require a showing of both duplication and competition in commerce leading to commercial harm.<sup>[182]</sup> Although Sen. Hatch has not yet introduced legislation, he has read into the Congressional Record three illustrative bills: his final 1998 compromise draft, the new Coble proposal, and a bill on the unfair competition model that fits the ITAA description.<sup>[183]</sup> As we conclude this article, the only formal action on any new legislation has been the approval of H.R. 354 by the House Judiciary Committee.<sup>[184]</sup>

## **VI. Conclusions: What Should We Do?**

{92} Before launching into recommendations for legal action, it may be beneficial to take a step back and ask the prior question of what our policy objective is. Presumably, it is to advance the constitutional goal of promoting the progress of science and the useful arts through the granting of exclusive rights. In our particular context, that means to use legal exclusivity to promote the creation of databases, especially those that are in some sense the most "useful." But, the constitution also emphasizes that exclusivity must be employed in a limited way, giving away no more of the public domain than is necessary to achieve the desired promotional effect.

{93} Arriving at a perfect utilitarian balance between incentives for knowledge producers and access for knowledge consumers has always been the Holy Grail of intellectual property law. Just like the original Holy Grail, this one is still at large, of course. This is due in substantial part to the lack of a clear distinction between producers and consumers. Since few if any producers start from scratch, the process of knowledge production inevitably begins with the consumption of what is already there. This reality is sometimes conveniently overlooked by the database industry and its advocates. Their position is a variation on the pull-up-the-drawbridge argument made by opponents of suburban growth: now that I'm comfortably ensconced in my subdivision, development has to stop. The database version is: I may have stood on the shoulders of those who came before, but no one is going to stand on mine.<sup>[185]</sup> While this form of argument may occasionally make sense in the development context, it has no place in the world of knowledge production.

{94} With this as background, we turn to four questions that frame the dilemma facing lawmakers:

{95} *1. Is the current law really inadequate?* As we have discussed, those who argue for new federal legislation allege numerous inadequacies in the current law.<sup>[186]</sup> But the adequacy of current law cannot be judged in the abstract. It depends, rather, on what kind of database one is talking about, and how it will be used. It is important to remember that the claims of inadequacy derive from *Feist* and its heightened standard for protection. *Feist*, however, focused on wholesale copying of the most vulnerable kind of database, a paper telephone book. Most of the subsequent cases that have found little or no copyright protection have dealt with comparable compilations, or straightforward digital copies thereof.<sup>[187]</sup>

{96} To evaluate the adequacy of existing legal protections for compilations of data, it is necessary to consider three distinct scenarios. In the first, the database consists of an unoriginal compilation on the phone book model, and the users seek unrestricted access to the entirety of the information. The second scenario involves the "full service" database, where the proprietor both collects, arranges, and manages the raw data and provides the search tools. The user does not take possession of (or have disclosed to him) the entirety of

the database, as in the phone book model, but is granted controlled access in order to create some subset of information. The Lexis/Nexis and Westlaw legal databases are examples. The third scenario is illustrated by the typical Internet search. The user brings to bear search and organization tools from one or more sources in order to access an unlimited range of data sources and create a compilation customized to fit his own needs.

{97} The second situation is the easiest to evaluate from a legal perspective. Here, existing protections seem adequate. There is a measure of real exclusivity, to which the law makes significant enhancements. Technical measures are readily available to deny access or impose conditions, thereby diminishing the likelihood of wholesale theft of the database. Since access is understood to be limited from the outset, there is little market resistance to such measures. Moreover, where the raw data are themselves proprietary, the availability of technical restrictions makes trade secret protection of the database both legally and practically feasible, thus dodging the whole preemption problem.<sup>[188]</sup> Even some level of copyright protection may be available for the raw data if their selection and arrangement involve a modicum of creativity.<sup>[189]</sup> In addition, the circumvention of technical measures is now itself a copyright infringement.<sup>[190]</sup> Search and organization tools are subject to copyright and, increasingly, patent protection. On balance, neither a European-style *sui generis* right, nor a national misappropriation or unfair competition law would seem to add significantly to what is already available to database producers in this category of circumstances.

{98} The third scenario is conceptually similar to the second, but with the added wrinkle that there are now a plurality (if not an infinity) of data sources. The conclusions reached above concerning search and organization tools apply here as well. Some of the data sources may be suitable for technical protection and/or merit a meaningful level of copyright, contract, or trade secret protection. But many--perhaps most--will not. Some will lack the market appeal to support any kind of restrictions;<sup>[191]</sup> others, by their nature, will not command a meaningful level of intellectual property protection; many will have both sets of problems. Further, the management of the whole situation is complicated, of course, by the multiplicity of players. Consequently, for those who expose more or less raw and non-proprietary data to Internet searches, both real and artificial exclusivity are absent and a *sui generis* right would add significantly to their ability to control usage.

{99} The first scenario -- the phonebook-type database made available for unrestricted use -- is the most difficult. There is substantial market demand for simple compilations, particularly if the compiler has had to expend "sweat" by mining the data from other sources. Users of raw data are likely to be resistant to technological measures. If I have to do the work of selection and collation, I probably will not accept significant technical impediments; I am likely to decide fairly quickly to forgo purchase of the database and collect the information myself. Even here, however, if the subject data have been "mined," there may be enough originality to generate significant copyright protection. Contractual arrangements may also be feasible in some situations, subject to the vagaries of preemption. But, in the true *Feist* case and its corollaries, involving complete access to phonebooks and other primitive compilations, the "goods" are plainly non-exclusive, and current law offers little help. Any form of *sui generis* right would significantly alter the present legal landscape.

{100} 2. *Assuming that we can enhance protection for simple databases, should we?* To address this question, it is useful to ask how the market would respond if the law did nothing further to promote database exclusivity. The current law is not inert, but is clearly discriminatory. It encourages reliance on search tools and sophisticated (creative, and thus original) data mining techniques while discouraging the production and sale of bulk databases.

{101} Is this a good or a bad thing? The word "discrimination" has negative connotations, but not all discrimination is invidious. In our semi-free-market system, certain classes of producers are regularly disadvantaged by the law's failure to intervene on their behalf. For example, the current law offers no encouragement to the production of ideas that are not transformed into a operable invention or a copyrighted



work. One who submits a raw idea to industry for possible exploitation has little to rely on beyond the good faith of the recipient.<sup>[192]</sup> But this is not widely viewed as problematic; on the contrary, it is assumed that unrefined ideas have insufficient social utility to be worth the law's intervention.<sup>[193]</sup>

{102} The database issue requires a similar kind of analysis. Thus, we might ask whether the *Feist* end of the database industry is producing something of such value to society that the law should lend artificial exclusivity to the product. To take a specific instance, would it be a good or bad thing if most directories were provided on a diskette together with a search program (the whole entity having a meaningful mix of copyright, contract, and even patent protection), rather than in written form? Would this make society more efficient? Or, would it magnify the gap between the haves, who could afford and utilize the more sophisticated database, and the have-nots, who might lose access to the information in any form? Before jumping to any conclusions, recall that library catalogs have undergone this very transformation, with adverse consequences only for irredeemable luddites.

{103} A related issue is whether the proprietors of *Feist*-type databases actually need enhanced protection. Despite the arguments of Senator Hatch and others,<sup>[194]</sup> we see no evidence that a raw information shortage is developing. On the contrary, experience says that all of us are overwhelmed by information, and its proliferation is accelerating. The evidence suggests that proprietors are finding alternative avenues to profitability (that is, through means other than exclusivity);<sup>[195]</sup> advertising is currently the most important of these. Moreover, technical measures improve daily, offering the hope for subtler compromises between the free access that attracts advertisers and the wholesale misappropriation that frightens producers. As *Feist* itself suggests, it is dangerous to predicate tomorrow's law on yesterday's - or even today's - technology.

{104} Our conclusion is that the problem of inadequate protection, however serious in the abstract, is, in the real world of digital property, (1) limited in scope and (2) having little discernible effect on the pace of the digital revolution. At most, some kinds of low-end databases can legitimately claim inadequate legal protection. In addition, any restrictions on access to information have real social costs, a topic we explore further below. We are therefore hesitant to advocate novel and broadly applicable *sui generis* legislation.

{105} 3. *If we nonetheless conclude that we do want to protect all types of databases, what form should the protection take?* The form of protection has two components: the nature of what is to be protected and the conduct that is to be prohibited. With respect to the first, there seems to be no realistic alternative to the European model of predicating protection on the investment of substantial time or money in the compilation effort<sup>[196]</sup>-sweat of the brow, in other words. It has never been seriously proposed that information itself should be protected (except under trade secret law), and the compilations seeking protection are by definition unoriginal. Sweat equity is all that is left.

{106} The second component is more complex. The European prohibitions are very broad, covering "extraction and/or re-utilization of the whole or a substantial part" of the database,<sup>[197]</sup> subject to some fair use-type exceptions.<sup>[198]</sup> But this approach conflates two categories of misappropriation that should be kept separate. The first is the individual who wants to use data for personal purposes without paying for it. (The European Database Directive exempts some, but by no means all, personal uses.<sup>[199]</sup>) This is roughly comparable to a home user who copies a friend's software. Experience has shown that the law is of limited value in limiting this risk. Legal protection would be of largely theoretical value, and the owner of the database should therefore be left to fight this battle by other, technical means. Even in cases where no such alternatives are available, the law ought not to invest its credibility and resources in this ultimately futile endeavor. Software producers have, after all, survived the home copying problem. It is commercial misappropriation that should be the focus of any legislation. This focus might be achieved either through a European-style *sui generis* right with a blanket exemption for non-commercial use or a federal law of unfair competition that required a showing of actual or intended commercial advantage.<sup>[200]</sup> If the *sui generis* right is limited by a broad non-commercial exemption, there seems little to choose between the two.<sup>[201]</sup> With



either, the principal point of contention is likely to be the meaning of "commercial." It is easy to foresee such disputes as whether the copying of a database by research scientists at a drug company is a forbidden commercial use or a protected research use. Its immediate purpose may be purely scientific, but the ultimate objective of the whole endeavor is to generate profits. A related question would involve research in a university laboratory which produces patentable inventions that generate revenue to further the university's non-profit mission. Copyright cases that have attempted to apply the fair use doctrine in contexts just like these hint at the difficulties to be expected.[202]

{107} A final consideration is the general advisability of following a novel European Union approach. One reaction might be that if the whole continent of Europe has adopted the *sui generis* approach then it must be sensible. But recall that the Database Directive was adopted in early 1996, when the Internet was in its relative infancy. For European nations adopting conforming legislation, the basic policy questions we have been discussing were already moot. Is there any indication that the U.S. database industry has suffered relative to its EU counterpart in the three-plus years since the Directive was promulgated?

{108} Remember also that EU legislation is sometimes enacted to advance agendas beyond its nominal subject matter. For one thing, in a Europe that is federalizing self-consciously and often awkwardly, the very adoption of a continent-wide legal regime can be viewed as a worthy accomplishment. The United States, whatever its other problems, does not suffer from a paucity of federal law. Note as well that the Database Directive works in concert with the Privacy Directive[203] to provide a level of central control over the digital industry that goes far beyond anything ever advanced in this country. This control reflects a very different relationship among government, citizens, and private businesses than has been customary in the United States, and a very different experience with government monitoring of individuals.[204] Finally, a cynic might suggest that every EU initiative must be searched for hidden protectionism.[205]

{109} None of this is to say that the European solution is wrong. It has, however, emerged in a different political and cultural context. Consequently, the United States Congress should be reluctant to adopt European policy assumptions without questioning them at a fundamental level.

{110} Overall, it is our judgment that new legislation is neither necessary nor desirable. With respect to necessity, the information industry is growing explosively under the present dispensation. To the extent that certain segments of the industry are disfavored by current law and technology, they are segments that economic Darwinism has probably already doomed to extinction. Moreover, the pace of technological change is such that any "novel" legislation might be obsolete before it took effect. With respect to desirability, it should be emphasized that relatively free access to information has been a cornerstone of the digital revolution. To threaten this growth with novel and aggressive restrictions on access would be risky indeed; this is not, after all, a situation where a dying industry is desperate to be saved. In more technical terms, all the evidence suggests it ain't broke, so don't fix it.

---

**[\*\*]NOTE:** All endnote citations in this article follow the conventions appropriate to the edition of THE BLUEBOOK: A UNIFORM SYSTEM OF CITATION that was in effect at the time of publication. When citing to this article, please use the format required by the Seventeenth Edition of THE BLUEBOOK, provided below for your convenience.

John M. Conley et. al, *Database Protection in a Digital World*, 6 RICH. J.L. & TECH. 2, (Symposium 1999), at <http://www.richmond.edu/jolt/v6i1/conley.html>.

[1]. See World Information Technology Services [WITSA], *Executive Summary, Digital Planet: The Global Information Economy* 1 (visited Mar. 26, 1999) <<http://www.witsa.org/press/dpexsumm.pdf>>.

[2]. *See id.*

[3]. *See id.*

[4]. U.S. Department of Commerce, *The Global Context for U.S. Technology Policy* 4 (visited Mar. 23, 1999) <<http://www.ta.doc.gov/OTPolicy/Reports.htm#USTPS>>.

[5]. *See* Peter G.W. Keen, *Shaping the Future: Business Design Through Information Technology* 1 (1997).

[6]. *See* WITSA, *Digital Planet Press Release* 3 (visited Mar. 23, 1999) <<http://www.witsa.org/press/digplanpr.htm>>.

[7]. U.S. Department of Commerce, *The Emerging Digital Economy* A1-2 (visited Mar. 23, 1999) <<http://www.ecommerce.gov/emerging.htm>>.

[8]. *See* U.S. Department of Commerce, *supra* note 4, at 8.

[9]. *See* U.S. Department of Commerce, *supra* note 7, at A1-7.

[10]. *See id.* at 2.

[11]. *See* WITSA, *supra* note 6, at 2.

[12]. *See* U.S. Department of Commerce, *supra* note 7, at A1-7.

[13]. *Id.* at 2.

[14]. *See generally* Anne Wells Branscomb, *Who Owns Information?* 7-8 (1994) (raising questions about the adequacy of current incentives).

[15]. *See generally* Nicholas Henry, *Public Administration and Public Affairs* 259-62 (1986); Emmanuel Savas, *Privatizing the Public Sector: How to Shrink Government* 29-52 (1982) (for a discussion of market structure).

[16]. *See generally* Rondo Cameron, *A Concise Economic History of the World* 319-23 (1993) (on the historical role of government).

[17]. Adam Smith, *The Wealth of Nations* (Prometheus Books ed. 1991, orig. 1776).

[18]. Martin J. Sklar, *The Corporate Reconstruction of American Capitalism, 1890-1916* 179ff. (1993).

[19]. *See* Robert Cooter & Thomas Ulen, *Law and Economics* 108-113 (discussing exclusivity, rivalry, and free-riding).

[20]. U.S. Const. Art. I, sec. 8, cl. 9.

[21]. *See* Cooter & Ulen, *supra* n. 19, at 112-116 (discussing government's role in protecting property rights in information); William M. Landes & Richard A. Posner, *An Economic Analysis of Copyright Law*, 18 J. LEGAL STUD. 328 (1989) (assessing economic need for copyright protection); Steven Breyer, *The Uneasy Case for Copyright: A Study of Copyright in Books, Photocopies, and Computer Programs*, 84 HARV. L. REV. 281 (1970) (questioning whether artificial stimulus of copyright law is economically necessary).

[22]. Consider, for example, the challenges to the long-established music copyright regime presented

suddenly by the availability of digitized music over the Internet. *See, e.g.*, Jupiter Communications, Music Industry and the Internet: Usage, Retail and Digital Distribution Projections (1998); Mark Plotkin, *The Times They Are A Changin'*, 1 VAND. J. INT'L L. & PRAC. 46 (1999).

[23]. *See infra* notes 170-84 and accompanying text.

[24]. *See* Rick Darnell, et al., *How Search Engines Work* (last modified Sept. 29, 1997) <<http://www.webreference.com/dlab/books/html-pre/43-1-1.html>> (discussing tool categories generally).

[25]. *See infra* notes 41-48 and accompanying text.

[26]. *See supra* notes 22-23 and accompanying text.

[27]. *See generally* White House Information Infrastructure Task Force, Working Group on Intellectual Property, *Intellectual Property and the National Information Infrastructure* (visited Mar. 26, 1999) <<http://www.uspto.gov/web/offices/com/doc/ipnii/index.html>> (discussing technological protections).

[28]. Digital property can never take on the rivalry characteristics of a loaf of bread, which can be used only by one consumer at a time. Access control can move data in this direction, however, by preventing universal simultaneous use.

[29]. *See infra* notes 59-68 and accompanying text (discussing the legal aspects of access control).

[30]. A "key escrow" system adds another level of protection by placing the private key needed to decrypt an encrypted transmission in escrow with a mutually trusted third party; this party can then supervise the distribution of the message.

[31]. *See* American Bar Association, *Digital Signature Guidelines Tutorial* (visited Mar. 17, 1999) <<http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html>>.

[32]. *See* John M. Conley & Kelli Bemelmans, *Intellectual Property Implications of Multimedia Products: A Case Study*, 6 INFO. & COMM. TECH. L. 3 (1997) (discussing these intellectual property implications in detail).

[33]. *See supra* notes 27-32 and accompanying text.

[34]. This proposition is explicit in the Copyright Act. *See* 17 U.S.C. Section 103(b) (1994) (copyright in compilation "does not affect or enlarge the scope, duration, or subsistence of, any copyright protection in the preexisting material"). It is self-evidently implicit in the Patent Act. An infringer is one who, without authority, makes, uses, or sells the patented invention, *see* 35 U.S.C. Section 271(a) (1994), and there is no exception remotely applicable to the context of a database. (On the contrary, a database maker who actively induced the infringement of an invention could be held liable for contributory infringement. *See infra* note 38 and accompanying text.) The exceptional case is trade secret law, where, as discussed in the text, a pass-through to an innocent end user could undercut trade secret protection.

[35]. *See* Feist Pubs., Inc. v. Rural Telephone Serv. Co., 499 U.S. 340 (1991).

[36]. *See* Warren Pub., Inc. v. Microdos Data Corp., 115 F. 3d 1509 (11th Cir. 1997).

[37]. *Kregos v. Associated press*, 3 F. 3d 656 (2d Cir. 1996).

[38]. *E.g.*, N.C. Gen. Stat. Section 66-154(a)(2)(1992)(Uniform Trade Secrets Act; under some

circumstances, innocent purchaser of trade secret may have right to continue to use it).

[39]. *See* 35 U.S.C. Section. 271(a) (1994). Since patented inventions must be fully disclosed on the public record, 35 U.S. C. Section. 112 (1994), disclosure does not violate the patentee's rights.

[40]. *See id* at Section. 271(b) (1994).

[41]. 499 U.S. 340 (1991).

[42]. *Id.* at 354.

[43]. *Jeweler's Circular Pub. Co. v. Keystone Pub. Co.*, 281 F. 83, 88 (2d Cir. 1922) (granting copyright protection to compilation of trademarks in jewelry). *See also* *Leon v. Pacific Telephone & Telegraph Co.*, 91 F.2d 484 (9th Cir. 1937) (telephone directory entries); *Northwestern Bell Tel. Co. v. Bedco of Minn.*, 501 F.Supp. 299 (D. Minn. 1980) (same); *Rand McNally & Co. v. Fleet Management Sys., Inc.*, 591 F.Supp. 726 (N.D. Ill. 1983) (map).

[44]. *See Jeweler's Circular*, 281 F. at 88-89.

[45]. *See* 499 U.S. at 354.

[46]. *See* 17 U.S.C. Section 102(b)(1994).

[47]. *See* 499 U.S. at 354.

[48]. *Id.* at 359-60.

[49]. *See id.* at 353-54.

[50]. 248 U.S. 215 (1918).

[51]. *See id.* at 234.

[52]. *Id.* at 239.

[53]. 304 U.S. 64, 78 (1938) (stating "there is no general federal common law").

[54]. *See, e.g., National Basketball Association v. Motorola Inc.*, 105 F. 3d 841, 845 (2d Cir. 1997) (noting that New York common law can be used to protect time-sensitive data from free-riding under limited circumstances); *Nash v. CBS, Inc.*, 704 F. Supp. 823, 834-35 (N.D. Ill. 1989), *aff'd*, 899 F. 2d 1537 (1990) (suggesting availability, under Illinois law, of unfair competition protection for hot news and other, unspecified, "valuable stored information").

[55]. *See, e.g., National Basketball Association*, 105 F.3d at 848-53 (claims intended to prohibit real-time reporting of scores from NBA broadcasts held preempted, because broadcasts were within scope of copyright and protection sought was equivalent to copyright); *Nash*, 704 F. Supp. at 835 (on similar reasoning, striking as preempted claims intended to protect ideas contained in historical work).

[56]. *See* 17 U.S.C. Section 301.

[57]. The respected Nimmer treatise suggests that only compilations that have not been fixed in a tangible medium of expression, 17 U.S.C. Section 102(a), will fall outside the subject matter of copyright. *See generally* 1 Melville B. Nimmer & David Nimmer, *Nimmer on Copyright* § 3.04[B][3][b] at 3-34.15 (1997)



[hereinafter cited as Nimmer].

[58]. See, e.g., *National Basketball Association*, 105 F.3d at 853. The House Report accompanying the Copyright Act of 1976 suggests that an unpreempted misappropriation claim might lie "against a consistent pattern of unauthorized appropriation by a competitor of the facts (i.e., not the literary expression) constituting 'hot' news, whether in the traditional mold of [*INS*], or in the newer form of data updates from scientific, business, or financial data bases." H.R. Report No. 1476, 94th Cong., 2d Sess. 132, reprinted at 1976 U.S.S.C.A.N. 5659, 5748 (footnote and citations omitted). This seems identical to the New York cause of action recognized in *National Basketball Association*. As another example of a surviving misappropriation claim, the Report mentions the case of one who breaches an electronic security system in order to gain access to a database. Here, the extra element of the unauthorized invasion of the secured domain results in a right not equivalent to copyright. *Id.* One court has quoted this language from the House Report, but in circumstances where it did not apply. *Mayer v. Josiah Wedgwood and Sons, Ltd.*, 601 F. Supp. 1523, 1534 (S.D.N.Y. 1985) (rejecting unfair competition claim to protect design).

[59]. Hardcore baseball fans (like co-author Conley) have encountered this whole panoply of strategies in their ongoing quest for the weekly columns of Peter Gammons, the demigod of baseball journalists. Formerly, the columns were freely available at the website of *The Boston Globe*, Gammons' home paper. Recently, however, the *Globe* used technological means to disable downloading, and then on December 13, 1998 (Conley's birthday-an especially cruel blow) stopped posting them entirely. The *Globe* has thus protected its direct investment in Gammons, but presumably at some cost to the advertising value of its entire website (aside from an occasional, pruriently motivated peek at Boston political news, Conley has no other use for the site). An alternative is ESPN Sportzone. Here, one must register and pay to read Gammons. Aside from the cost, this process puts the reader's credit card number in cyberspace and exposes the reader to unwanted solicitation. Even for a Boston-born fanatic like Conley, this is too high a price to pay. (Update: Just prior to submission of this article, the Gammons column began to appear again at the *Globe* Website, and it sometimes can be downloaded.)

[60]. 86 F.3d 1447 (7th Cir. 1996).

[61]. See *id.* at 1451-52. Interestingly, *ProCD* was a high-tech version of *Feist*. The protected work was a CD-ROM version of nationwide phonebook, containing millions of entries and packaged in a shrinkwrap license. Pro-CD charged a low price to consumers and a much higher one to commercial users of the product. The defendant "bought" a consumer package and then, in violation of the license, sold the information contained over the Internet. On such facts, a copyright claim was impossible under *Feist*.

[62]. See *id.* at 1454. In support of its reasoning, the court cited two Supreme Court decisions: *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470 (1974) (holding that trade secret protection not preempted), and *Aronson v. Quick Point Pencil Co.*, 440 U.S. 257 (1979) (holding that contract to pay for use of invention which is expected to be patented is enforceable even after patent fails to issue).

[63]. See *Ballas v. Tedesco*, 41 F. Supp. 2d 531, 536 (D.N.J. 1999) (characterizing law regarding preemption of contract remedies as "unsettled"). The death of the proposed UCC Article 2B, which would have governed licenses, suggests that uniformity may be a long time coming. See *Effort to Develop UCC Article 2B Abandoned in Favor of New Uniform Computer Data Law*, 67 U.S.L.W. (Legal News) 2615 (May 20, 1999).

[64]. *Vault Corp. v. Quaid Software, Ltd.*, 847 F.2d 255 (5th Cir. 1988). *Vault's* preemption analysis was convoluted. The license in question would have prohibited the defendant from taking advantage of limited rights to copy software for archival or technical purposes granted by Section 117 of the Copyright Act. The court held that section 117 was the exclusive source of law with respect to such copying, and that *it* therefore preempted any state law that purported to be more restrictive.

[65]. *Vault* was cited but not followed in *ProCD*. However, one recent district court decision has followed *Vault* and characterized *ProCD* as the minority view. *Novell, Inc. v. Network Trade Center, Inc.*, 25 F. Supp. 2d 1218 (D. Utah 1997). For a discussion of *Vault* and its implications, see John M. Conley & Vance F. Brown, *Revisiting Section 117 of the Copyright Act: An Economic Approach*, 7/11 COMP. LWYR. 1, 4 (Nov. 1990).

[66]. *See Nimmer* .

[67]. *See* 1 *Nimmer*, Section 3.04[B][3][a](1997).

[68]. *See id.* at 3-34.2. As discussed elsewhere in the treatise, the non-section 301 theory is the general constitutional law of preemption, applied to state laws that implicate copyrighted works. *See id.*, Section 101[B][3]. Ironically, David Nimmer's argument rests on the proposition that section 301 does not "preempt" the subject of preemption in the field of copyright.

[69]. *See* 17 U.S.C. Section 103.

[70]. 17 U.S.C. Section 101.

[71]. *See Feist*, 499 U.S. at 345.

[72]. 945 F.2d 509 (2d Cir. 1991).

[73]. *See id.* at 511.

[74]. *Id.* at 513.

[75]. *Id.* at 516.

[76]. 924 F. Supp. 918 (D. Minn. 1996)

[77]. 799 F.2d. 1219 (8th Cir. 1986), *cert. denied*, 479 U.S. 1070 (1987).

[78]. 924 F. Supp. at 921. The *Florida Cases* series is simply the *Southern Reporter*, less the non-Florida (Alabama, Louisiana, and Mississippi) cases.

[79]. 17 U.S.C. Section 107.

[80]. 924 F. Supp. at 921. Oasis had originally filed suit in the Southern District of Florida, seeking antitrust damages and a declaratory judgment of copyright invalidity and/or non-infringement. West successfully moved for transfer to Minnesota, and the case came before the court on cross-motions for summary judgment on the copyright count as well as a count based on Florida's public records law.

[81]. *Id.* at 923.

[82]. *Id.* at 924.

[83]. *Id.* at 925.

[84]. *Id.* at 926. Oasis' point was presumably that one who knew all the initial page numbers would know exactly how the cases were arranged. If arrangement was the key to the copyright, then West's concession on initial page numbers, or citations, effectively conceded everything.

[85]. *Id.*

[86]. The court also rejected Oasis' fair use defense. *Id.* at 926-29.

[87]. 158 F.3d 674 (2d Cir. 1998) and 158 F.3d 693 (2d Cir. 1998), *cert. denied*, 119 S. Ct. 2039 (1999).

[88]. *See* 158 F.3d at 677.

[89]. *Id.* at 688.

[90]. *Id.* In dissent, Judge Sweet contended that the court should have focused on the totality of West's effort, rather than looking at the case reports element-by-element. *Id.* at 690. He also emphasized the very undemanding nature of the *Feist* test.

[91]. 158 F.3d at 696-98.

[92]. *Id.* at 697 n.5. That footnote quotes West's counsel's detailed description of how the process would work.

[93]. *Id.* at 701, 707, 708.

[94]. *Id.* at 702.

[95]. *Id.* at 704-06.

[96]. *Id.* at 706.

[97]. *Id.* at 708. Judge Sweet dissented once again, adopting the *Oasis-Mead Data* equivalence of reflection and copy.

[98]. 115 F. 3d 1509 (11th Cir. 1997).

[99]. *Id.* at 1516 (italics in original).

[100]. *Id.*

[101]. *Id.*

[102]. *Id.* at 1517.

[103]. *Id.* at 1518.

[104]. *Id.* at 1520. Three judges dissented, arguing at length that the originality requirement had been met. *Id.* at 1521 (Godbold, Hatchett and Barkett, JJ., dissenting). The majority made reference to its earlier en banc decision in *BellSouth Advertising & Pub. Corp. v. Donnelley Info. Pub., Inc.*, 999 F.2d 1436 (11th Cir. 1993) (en banc), *cert. denied*, 510 U.S. 1101 (1994), in which it held that the yellow pages listings lacked sufficient originality, in part because the subscriber chooses the heading under which it will appear.

[105]. 3 F.3d 656 (2d Cir. 1993).

[106]. *Id.* at 659.

[107]. The previous three opinions are summarized at 3 F.3d at 660. A number of other issues were dealt

with, including trademark and state-law claims and the copyright statute of limitations. The only copyright claim to survive the statute of limitations was that concerning Kregos' 1986 pitching form.

[108]. *Id.* at 663.

[109]. *Id.* Consider, for example, the instructions for a rudimentary device like a picture hook.

[110]. *Id.*

[111]. *Id.* at 663-64.

[112]. 982 F.2d 693 (2d Cir. 1992).

[113]. 149 F.3d 1368 (Fed. Cir. 1998).

[114]. *Id.* at 1371-72.

[115]. Pub. L. No. 105-304 (October 28, 1998) (codified at various sections of 17 U.S.C.).

[116]. 17 U.S.C. Sections 1201-05 (1998). Other provisions of the DMCA limit copyright infringement liability for online service providers, create rights to operate licensed software for maintenance purposes, and protect boat designs.

[117]. *Id.* Section 1201(a)(1-2) (1998). The most important exception may be that for reverse engineering. *Id.* § 1201(f).

[118]. *Id.* Sections 1203-04 (1994).

[119]. *See supra* note 59 and accompanying text.

[120]. Reciprocal national treatment means that each signatory country will afford the same rights to nationals of other signatories that it offers to its own citizens. WIPO Copyright Treaty, Articles 3, 11, & 14 (Article 3 incorporating reciprocal national treatment provision of Berne Convention).

[121]. 17 U.S.C. Sections 602(a) (1994). The Supreme Court has recently held, however, that the first sale doctrine, *id.* Section 109, trumps this provision, meaning that Section 602(a) will not apply to a copy which was legitimately sold abroad and then imported back into the United States. *Quality King Distributors, Inc. v. L'anza Research International, Inc.*, 118 S.Ct. 1125 (1998).

[122]. *Id.* Section 602(b).

[123]. *See infra* notes 170-84 and accompanying text.

[124]. *See id.*

[125]. The industry concerns were concisely articulated by Sen. Orrin Hatch (R-Utah), Chairman of the Senate Judiciary Committee, in remarks at the start of the current session of Congress. 145 Cong. Rec. S316-01 (Jan. 19, 1999)(statement of Sen. Hatch). For further discussion of this perspective, see John Tessensohn, *The Devil's in the Details: The Quest for Legal Protection of Computer Databases and the Collections of Information Act*, H.R. 2652, 38 IDEA 439, 464-87 (1998)[hereinafter Tessensohn]; Jennifer Lucas, *Database Protection Could be at Forefront of the 106th Congress' Legislative Efforts*, 67 U.S.L.W. 2355 (Dec. 22, 1998) (quoting Washington, D.C. attorney Jonathan Band, who has been involved in the drafting and



lobbying efforts for the current congressional session on behalf of the Information Technology Association of America)[hereinafter Lucas]. Mr. Band elaborated on these issues in a Jan. 4, 1999 telephone interview with co-author Conley.

[126]. Council Directive 96/9/EC of Mar. 11, 1996, 1996 O.J. (L. 77) 20 [hereinafter cited as "Database Directive"].

[127]. The 1996 Diplomatic Conference that adopted the WIPO Copyright Treaty, considered but did not adopt a database protection provision.

[128]. Database Directive, art. 16. For a review of the implementation process in the United Kingdom, see Simon Chalton, *The Copyright and Rights in Databases Regulations 1997: Some Outstanding Issues on Implementation of the Database Directive*, 1998/5 EUR. INT. PROP. REV.178.

[129]. Database Directive, arts. 3-6.

[130]. *Id.*, arts. 7-11.

[131]. Council Directive 91/250/EC of May 14, 1991, 1991 O.J. (L. 122) 42.

[132]. Database Directive, recital 23, art. 1.

[133]. See John Adams, "*Small Earthquake in Venezuela*": *The Database Regulations 1997*, 1998/4 EUR. INT. PROP. REV. 129.

[134]. See *id.*

[135]. Database Directive, art. 3, ¶1. See Adams, *supra* note 133, at 130.

[136]. See *id.*

[137]. *Database Directive*, art. 4, ¶ 1.

[138]. Article 85(3) of the Treaty Establishing the European Community of Mar. 25, 1957 (Treaty of Rome) exempts from the EU's generally strict prohibitions against agreements in restraint of trade those agreements that promote technological progress and do not unreasonably burden consumers or threaten competition. Subsequent regulations have specifically extended the exemption to "know-how" licenses and have defined know-how in a way that is similar to the American understanding of trade secrets. *E.g.*, Commission Regulation 556/89, art. 1, 1989 O.J. (L. 61) 7; Commission Regulation 240/96, 1996 O.J. (L. 31) 2. There is no substantive EU trade secrets law.

[139]. For example, under article 311-1 of the French Criminal Code, the illegal taking of a trade secret embodied in a fixed medium, such as a computer disk, constitutes theft. It is a general principle of French and other Continental law that an aggrieved party can seek private compensation through the criminal justice system. Bernard Rudden, Otto Kahn-Freund & Claudine Levy, *A Source-Book on French Law* 206-07 (rev. 3d ed. 1991). While the French Civil Code does not expressly provide a cause of action for the misappropriation of trade secrets, a victim of misappropriation may, under the appropriate circumstances, be able to maintain a cause of action for unfair competition under general tort principles, French Civil Code, arts. 1382-83, or for breach of contract. *Id.*, arts. 1101 *et seq.* Under German law, it is illegal for a person, without authorization and for personal or business gain, to misappropriate a commercial secret through the utilization of technical devices or means or the physical reproduction of the secret information. Statute Against Unfair Competition of 1909, § 17, ¶ 2. The same statute's general prohibition against unfair

competition has also been held to cover the disclosure of business secrets. *Id.*, § 1; *see* Norbert Horn, Hein Kotz & Hans G. Leser, *German Private and Commercial Law: An Introduction* 286 (Tony Weir trans., 1982). A trade secret owner could enforce its rights under this statute by an application to the public prosecutor or by the initiation of a private cause of action seeking to enforce criminal penalties. In a private cause of action, the claimant can add a claim for damages and equitable remedies, such as an injunction.

[140]. Database Directive, art. 13.

[141]. Proposal for a European Parliament and Council Directive on the Harmonization of Certain Aspects of Copyright and Related Rights in the Information Society, COM (97) 628 final, 1998 O.J. (C. 108) 6. On the U.S. DMCA, *see supra* notes 115-22 and accompanying text.

[142]. The European Patent Convention was adopted in 1973 to create a uniform set of standards for issuing national patents within the eighteen countries that are parties to the convention.

[143]. *See* notes 113-14 and accompanying text.

[144]. Simon Davies, *Computer Program Claims*, 1998/11 EUR. INT. PROP. REV. 429.

[145]. *Id.*

[146]. *Id.* Davies argues that the European Patent Convention is merely procedural in nature, and that the underlying substantive patent law does not require that computer programs be treated as unpatentable subject matter.

[147]. Database Directive, arts. 7-11.

[148]. *Id.*, recital 41.

[149]. *See* Chalton, *supra* note 123, at 181.

[150]. Database Directive, art. 7, ¶ 1. There are no specific standards for determining when an investment has been substantial. The test is both quantitative and qualitative.

[151]. *Id.*, art. 11, ¶ 1.

[152]. *Id.*, art. 11, ¶ 2.

[153]. *Id.*, art. 1, ¶ 2.

[154]. *Id.*, recital 17.

[155]. *Id.*, recital 21.

[156]. *Id.*, art. 6, ¶ 2.

[157]. *Id.*, art. 10. The period of protection expires fifteen years from the first day of January of the year following completion of the database, but may be extended by making the database available to the public, or by making any substantial change in the database.

[158]. *Id.*, art. 6, ¶ 4.

[159]. *Id.*, art. 12.

[160]. *Id.*, art. 10, ¶ 1.

[161]. *Id.*, art. 9.

[162]. The U. S. law of fair use is codified in 17 U.S.C. Section 107 (1994).

[163]. Database Directive, recitals 9 -12.

[164]. Council Directive 95/46/EC of Oct. 24, 1995, 1995 O.J. (L. 281) 31.

[165]. *Id.*, art. 28.

[166]. *Id.*, art. 7.

[167]. *Id.*, art. 10.

[168]. *Id.*, art. 25. Article 26 creates some limited exceptions based on consent or necessity.

[169]. The United States and the EU are currently engaged in delicate negotiations over U.S. non-compliance. *See Privacy Issue Hits a Nerve: Europeans See U.S. as Naive to the Dangers of E-Commerce*, Raleigh News & Observer, July 11, 1999, at A1.

[170]. *See* Tessensohn, *supra* note 125, at 466-69.

[171]. *See id.*

[172]. Lucas, *supra* note 125, at 2355.

[173]. H.R. 2652, 105th Cong., 1st Sess. (1997). *See* Lucas, *supra* note 125, at 2356-57; Tessensohn, *supra* note 125, at 471.

[174]. H.R. 2652, § 1201.

[175]. *Id.* § 1202.

[176]. *See* Lucas, *supra* note 125, at 2355-56.

[177]. The drafters of H.R. 2652 intended to rely on the interstate commerce clause as authority to legislate, rather than the intellectual property clause. U.S. Const. Art. I, § 8, cl. 3 & 8. Justice questioned whether, after *Feist*, the intellectual property clause would prohibit the enactment of copyright-like protection for unoriginal compilations. *See* Lucas, *supra* note 125, at 2357.

[178]. *See id.* at 2356-57.

[179]. H.R. 354, 106th Cong., 1st Sess. (1999), Section 1403(a)(2).

[180]. *Id.* Section 1407 (c).

[181]. *Id.* at 2355.

[182]. The ITAA's proposals are embodied in a new bill introduced on May 20, 1999 by Rep. Tom Bliley (R-Va.), the Consumer and Investor Access to Information Act of 1999, H.R. 1858, 106th Cong., 1st Sess. (1999). *See* 54 BNA Pat., Copyr. & Trademark J.129 (May 27, 1999).

[183]. 145 Cong. Rec. S316-01 (Jan. 19, 1999) (statement of Sen. Hatch).

[184]. *See House Committee Approves Database Protection Measure*, 67 U.S.L.W. (Legal News) 2728 (June 8, 1999).

[185]. Einstein is reputed to have said, with absurd if sincere modesty, that he was but a dwarf standing on the shoulders of giants.

[186]. *See supra* note 125 and accompanying text.

[187]. *See supra* notes 90-114 and accompanying text.

[188]. *See supra* notes 27-32 and accompanying text.

[189]. Recall that West has had some success with this position. *See supra* notes 76-88 and accompanying text.

[190]. *See* notes 115-22 and accompanying text.

[191]. In other words, when users are confronted by a proposed restriction, either technical or legal, they will simply go elsewhere.

[192]. *E.g.*, *Lueddecke v. Chevrolet Motor Co.*, 70 F. 2d 345 (8th Cir. 1934).

[193]. *E.g.*, *Richter v. Westab, Inc.*, 529 F. 2d 896, 902 (6th Cir. 1976).

[194]. *See supra* note 125 and accompanying text.

[195]. *See*, for example, the figures reported at notes 1-9 and accompanying text *supra*.

[196]. *See supra* notes 147-62 and accompanying text.

[197]. Database Directive, art. 7, ¶ 1.

[198]. *Id.*, art. 9.

[199]. The Database Directive creates a general exception for personal use, but only in the case of paper databases. Otherwise, the use must be for non-profit teaching or research purposes. Personal use of electronic databases for business, entertainment, or other casual purposes is not exempted.

[200]. This is the form of the legislation being proposed in the current Congress by the Information Technology Association of America. *See supra* note 182 and accompanying text.

[201]. If commercial exploitation by the defendant is made either an element of the claim for relief or the basis for a blanket exception, the whole issue of the drafting of specific exceptions is avoided. Subject to the caveats raised in the text, the commercial exploitation rule should exempt all personal non-commercial and "pure" research uses.

[202]. *E.g.*, *Williams & Wilkins Co. v. U.S.*, 487 F.2d 1345 (Ct. Cl. 1973), *aff'd by an equally divided court*, 420 U.S. 376 (1975) (fair use for government lab to photocopy articles from medical journals for distribution to researchers); *American Geophysical Union v. Texaco Inc.*, 60 F.3d 913 (2d Cir. 1994), *cert. dismissed*, 116 S.Ct. 692 (1995) (not fair use for corporate scientist to photocopy journal articles).



[203]. See *supra* notes 163-692 and accompanying text.

[204]. A similar difference can be seen in a comparison of the American and European health care systems. Reasonable minds might differ as to which is better, but they are surely built on different sets of assumptions.

[205]. For a witty exposition of the cynical view, see David Pryce-Jones, *Bananas Are the Beginning*, Nat'l Rev., Apr. 5, 1999, at 34.