Who Owns the Customer? The Emerging Law of Commercial Transactions in Electronic Customer Data

Jane Kaufman Winn
University of Washington School of Law

James R. Wrathall

Follow this and additional works at: https://digitalcommons.law.uw.edu/faculty-articles

Part of the Commercial Law Commons, and the International Trade Law Commons

Recommended Citation


This Article is brought to you for free and open access by the Faculty Publications at UW Law Digital Commons. It has been accepted for inclusion in Articles by an authorized administrator of UW Law Digital Commons. For more information, please contact cnyberg@uw.edu.
Who Owns the Customer? The Emerging Law of Commercial Transactions in Electronic Customer Data

By Jane Kaufman Winn and James R. Wrathall*

INTRODUCTION

The Information Revolution is changing the way commerce is transacted and value is defined within transactions. Before the Internet and “e-business”1 took center stage, “electronic commerce” meant electronic data interchange, just-in-time inventory systems, supply chain automation, and corporate reengineering. But the rise of the Internet as a communications medium has coincided with a shift in management focus, from merely trying to improve the efficiency of business logistics systems to a more holistic perspective on improving customer relationships.2 Intangible assets such as intellectual property rights, human capital in the form of employee knowledge, and established relationships with customers and suppliers are playing an increasingly important role in both old economy and new economy businesses.3

Computer databases are one form of intangible asset that have played an important role in business for decades.4 The use of customer databases

* Jane K. Winn is a Professor of Law at Southern Methodist University in Dallas, Texas. She is the author of THE LAW OF ELECTRONIC COMMERCE (4th ed., 2001 forthcoming). Copies of other papers she has written on various electronic commerce law issues are available from her web site at http://www.smu.edu/~jwinn. James R. Wrathall is a partner with the firm of Wilmer, Cutler & Pickering in Washington, D.C., practicing in the areas of information law, litigation, and counseling.

1. “e-business (electronic business), derived from such terms as 'e-mail' and 'e-commerce,' is the conduct of business on the Internet, not only buying and selling but also servicing customers and collaborating with business partners.” Whatis.com, e-business, (visited Aug. 21, 2000), available at <http://www.whatis.com/WhatIs_Definition_Page/0,4152,212026,00.html>. IBM became one of the first to use the term “e-business” when “it launched a thematic campaign built around the term” in October, 1997. Id.
2. See, e.g., HARVARD BUSINESS REVIEW, MANAGING THE VALUE CHAIN (2000).
4. See, e.g., ALAN F. WESTIN & MICHAEL A. BAKER, DATABANKS IN A FREE SOCIETY (1972) [hereinafter WESTIN & BAKER].
is key to any strategy to build better relationships through electronic commerce. In recent years, there have been dramatic advances in the technology associated with building databases and analyzing the data they contain for competitive advantage. While data mining and customer profiling both antedate the rise of commercial Internet sites by many years, their use in business has become more visible and more controversial in recent years due to the ability of commercial Internet sites to collect new forms and greater quantities of customer data than was possible only a few years ago. As a result of their growing size and sophistication, and because of the pivotal role they play in managing business relationships, customer databases are becoming an ever more valuable asset for both "bricks and mortar" and Internet businesses.

The commercial law governing business-to-business transactions in customer databases has not kept up with the rapid pace of developments in business practice. Many interests in databases are not recognized as property rights under copyright or other intellectual property laws. Even a statute as newly-minted as the Uniform Computer Information Transactions Act (UCITA), which was finalized by the National Conference of Commissioners on Uniform State Laws in July 1999, is silent on many important issues raised by business transactions in data. In addition, the question of what rights, if any, individuals have to control the use of personally identifiable data has become very controversial in recent years as the ability to collect and analyze personal data continues to outstrip laws governing the privacy rights of individuals whose personal data is stored in databases.

Uncertainty also results where there is no express agreement among interested parties governing the collection and use of the data, or where one of the parties with an interest in the data seeks to change the rights of interested parties unilaterally by modifying an existing agreement or practice. The number of parties claiming commercial interests in the same data is growing as electronic commerce marketing strategies become more interdependent and interconnected. With the trend towards “coopetition”—including vertical hubs, partnerships, strategic alliances, and other

7. Some are skeptical about the value to businesses of profiling notwithstanding the overall uproar over the practice among privacy advocates. See, e.g., Saul Hansell, So Far, Big Brother Isn’t Big Business, N.Y. TIMES, May 7, 2000, at 3, 1.
9. See infra notes 178-99 and accompanying text.
licensing arrangements—it may be difficult for transacting parties to de-
termine whether they have obtained good title to database assets or are
taking them subject to competing claims of ownership or claims in in-
fringement of the rights of third parties.

These uncertainties are compounded by the rapid globalization of elec-
tronic commerce and the inconsistent legal standards applied in different
jurisdictions. For example, current U.S. law governing commercial use of
customer data may be incomplete and highly uncertain with regard to
many issues raised by new applications for customer databases. European
Union (EU) law, by contrast, is often quite unambiguous in simply pro-
hibiting or sharply curtailing a wide range of business practices U.S. firms
consider unproblematic. Global transactions often are subject to these and
other potentially conflicting bodies of law, creating additional legal risks
with respect to database assets.

This Article explores the new business models and technological ad-
vances driving the growing business interest in customer databases and
the uncertain and fragmentary state of the law applicable to these practices
and technologies. The Article also discusses practical strategies businesses
should consider to minimize the risks they face from collecting and using
customer data for competitive advantage in electronic commerce markets.

In recent years and months, many businesses have become involved in
disputes with regulators, competitors, and customers as a result of changing
conditions for the collection and use of customer data. As context for the
discussion of law and technology that follows, this Article summarizes
seven case studies involving actual or potential conflicting claims in cus-
tomer data. These cases illustrate the variety and significance of the legal
issues being created by the ongoing shifts in practice and technology.

Next, the Article provides an overview of the evolving business tech-
nologies fueling the explosive growth in the development and exploitation
of customer databases. Computer networking, data capture opportunities,
and data storage and analysis technologies are expanding rapidly. The
pace of technological change is far exceeding the ability of the lawmakers
to keep up, and indeed, some new technologies threaten to impair or even
eliminate the practical ability to enforce legal rights in data.

This Article then summarizes the current U.S. legal framework for pro-
tection of database assets and the divergent EU data protection framework,
respectively.

Finally, the Article concludes with analysis and practical suggestions for
managing risks in commercial transactions in data. Given the uncertainty
in the law regarding new commercial applications for customer data, con-
tract provisions will often assume paramount importance in establishing
the parties’ intentions regarding the value being created in new databases.
However, the complexity of Internet commerce technologies and the in-
terdependence of Internet businesses and their marketing strategies, com-
bined with the unsettling impact bankruptcy law could have on such “vir-
tual alliances,” will limit the certainty any contract provisions can provide. Accordingly, businesses should carefully evaluate legal risks arising from significant transactions involving data and take practical as well as legal measures to avoid or reduce the risks created in the new electronic commerce environment.

CASE STUDIES IN DATABASE RIGHTS AND DISPUTES

When the legal and economic implications of computer databases were first subjected to critical scrutiny and public debate in the late 1960s and early 1970s, networking was almost irrelevant to the analysis. By the middle of the 1970s, however, computer networking came to play a more important role in transaction settlement and clearing in banking and securities markets. One of the first examples of creating legal frameworks to resolve competing interests in transaction data collected and analyzed by multiple parties (including competitors) was the establishment of a regulatory system governing use of airline computer reservation systems.

When the Internet took center stage in the 1990s, one of the first major public conflicts to arise involved the “WHOIS” database created by Network Solutions, Inc. when it had the exclusive right to register Internet domain names. As a new Internet governance structure was created, legislators, businesses, and the public asserted widely divergent views as to the legal status of data collected in the process of registering domain names.

In 1999 and 2000, a series of legal actions were filed against electronic commerce companies challenging their collection and use of consumer data. A number of other recent cases have raised claims between businesses, asserting breach of contract and related claims to databases. In addition, several “dot-com” companies have become insolvent, resulting in conflicting claims to customer data and related privacy concerns in the context of bankruptcy proceedings. Finally, the emergence of business-to-business e-Hubs presents even more complicated issues relating to rights in shared customer data. These case studies are discussed below in turn.

AIRLINE COMPUTER RESERVATION SYSTEMS

Among the most successful Internet commerce sites are travel services sites such as Expedia.com and Travelocity.com. Part of the reason these services have enjoyed success as Internet services is that the Internet is

11. In Westin & Baker, the term “network” does not appear in the index. In a 500 page book published in 1972, there are two paragraphs on “communications systems” that speculate that satellite, cable television channels, and laser communication networks will play a more important role in computer technology in the future. Westin & Baker, supra note 4, at 329.

merely providing a new interface for one of the largest, most complex, and most successful electronic commerce systems developed before Internet commerce was possible. Airline computer reservation systems (CRS) operate globally and permit tens of thousands of individuals to access systems that execute millions of transactions daily.

In the United States, the airline industry is one of the most sophisticated users of data profiling technology. By carefully monitoring booking data, airlines are able to make continuous modifications in schedules and fares to maximize their return on their operations. In the airline industry, carriers are often forced to rely on competitors' CRS to receive bookings. In addition, a single trip may be the product of flight segments provided by different carriers, each of which have an interest in accessing marketing data about the entire trip, not just data about the segment the carrier provided. As a result, the competitive significance of control over access to marketing data is well established in the airline industry.

Some of the controversies surrounding access to airline CRS marketing data clearly foreshadow current controversies surrounding access to Internet commerce marketing data and, in part, share a common cause: the collaborative, multiparty structure of the network communication system through which transactions are executed and from which data is generated. Unlike Internet commerce, however, in the United States and in almost all countries around the world, the airline industry is subject to direct government regulation, substantially reducing uncertainty surrounding rights and obligations in marketing data.

In 1992, the U.S. Department of Transportation (DOT) issued a rule designed to enhance competition in the airline and CRS industries. The rule regulated the association between individual airlines and computer reservation systems that gave independent travel agents access to the schedules of all airlines. The rulemaking was aimed at eliminating "architectural bias" which gave a competitive advantage to the airline that owned a CRS. The kind of bias that concerned the DOT would permit an airline that owned a major CRS to obtain a larger number of bookings than other carriers accepting bookings through its system. Modifying the way flight availability or prices are displayed or the ease with which reservations can be made or tickets issued can create architectural bias. American Airlines and United Airlines each controlled a major CRS, and other carriers were concerned that independent travel agents subscribing to either CRS would have difficulty learning what seats were available on other carriers and booking them.

In addition to addressing the problems of "display bias" and discriminatory fee structures, the DOT rulemaking also addressed who should have access to marketing data generated from CRS transactions. If a CRS

vendor chose to generate any marketing, booking, or sales data from the bookings made on its system for domestic travel, it was required to make that data available to all participating U.S. carriers on nondiscriminatory terms.\textsuperscript{14} This rule did not extend to bookings for international travel because there was no assurance that foreign carriers would make comparable data from their systems available to U.S. carriers.\textsuperscript{15} At the time of the 1992 rulemaking, some EU carriers objected to the reciprocity standard established by the DOT because they were concerned that more rigorous data protection requirements in European countries might prevent European CRS vendors from meeting a reciprocity requirement.

The regulations in effect required CRS vendors to make marketing data available to other carriers that was as accurate and as complete as the data it provided to its own carrier. They allowed a CRS vendor's parent carrier to enjoy real time access to the marketing data, while competing carriers could obtain a copy of the data on tape. The DOT noted that although CRS vendors were allowed to charge for access to the data, and to provide it in a manner that made its use by other carriers difficult, it appeared that the carriers associated with CRS vendors did not gain substantial competitive advantage in the market for air travel as a result.\textsuperscript{16} The DOT also rejected claims from the American Society of Travel Agents that the data generated from agent booking belonged to the agency and that CRS vendors should be required to provide agencies with data generated from an agency’s bookings.

The regulation of the airline CRS system is an early example of the importance of data warehousing and customer profiling to competition in global markets. In addition, it shows the importance of policing the behavior of market intermediaries who are also competitors in resolving such technical matters as how output from databases is to be displayed to prospective customers and how broadly or narrowly a transaction record is defined.

\textbf{THE WHOIS DATABASE DISPUTE}

One of the most significant new customer databases to emerge in recent years is the “WHOIS” database of Internet domain name registrants, which grew from less than 500,000 names in 1995 to more than 8.1 million names by February 2000.\textsuperscript{17} In 1999, the issue of rights to the WHOIS

\begin{itemize}
\item \textsuperscript{14} 14 C.F.R. § 255.10(a) (2000) (requiring that “[t]he data made available shall be as complete and accurate as the data provided a system owner”).
\item \textsuperscript{15} See 14 C.F.R. § 255.11(b) (2000) (stating that “[t]he obligations of a system under this part shall not apply to any foreign carrier . . . .”)
\item \textsuperscript{16} CRS Regulations, supra note 13, at 43,820.
\item \textsuperscript{17} Ariana Eunjung Cha, Network Solutions Antitrust Probe Ends; No Action Taken; Va. Firm’s Stock Jumps, WASH. POST, Feb. 2, 2000, at E2.
\end{itemize}
database became the subject of a legal and political controversy that was global in scope.

Since the early 1990s, Internet domain name registration services have been provided and coordinated by Network Solutions, Inc. (NSI), in cooperation with the National Science Foundation (NSF). On December 31, 1992, NSF awarded to NSI a federal cooperative agreement (Cooperative Agreement) to provide exclusive Internet administration and domain name registration services.18 During the next five years, NSI and its shareholders invested tens of millions of dollars to build up processing capabilities and operational infrastructure to meet the exploding demand for domain names and registration services.

As questions of Internet governance and domain name administration gained global attention, many objected to NSI's rights in the customer data it collected in providing domain name registration services. By 1997, a number of constituencies argued for increased control and more formal governance. Major corporations with overarching interests in trademark protection, and related entities, including the World Intellectual Property Organization (WIPO), advocated a new framework that would create and enforce standards to curtail perceived trademark abuses arising out of the use of Internet domain names.19 European governments argued for greater regulatory control over Internet communications, particularly in connection with alleged violations of privacy standards, and for a greater role in setting Internet policy generally.20 In addition, a number of companies expressed interest in competing with NSI as registrars of non-military domain names.21

The U.S. Department of Commerce (DOC) initiated a proceeding on February 20, 1998, to address these and related Internet governance issues. Following notice and review of more than 650 comments, DOC proposed that a non-profit corporation—subsequently named the Internet Corporation of Assigned Names and Numbers (ICANN)—be formed in cooperation with government and private parties.22

On February 8, 1999, ICANN published for comment a draft document entitled “Guidelines for Accreditation of Internet Domain Name Registrars” (proposed Guidelines).23 The proposed Guidelines went far beyond the development of a shared registry system. They included, among other

20. Id.
21. Id.
things, a proposal that domain name registrars (principally NSI) be required to submit to ICANN, as the "registry administrator," a number of customer "data elements" beyond the customer name and domain name.\textsuperscript{24} ICANN also proposed to prohibit domain name registrars (principally NSI) from making any use of these customer data elements beyond that strictly necessary for operation of the domain name systems.\textsuperscript{25} ICANN's proposed Guidelines were supported in a number of comments that concurred in the suggestion that NSF's customer database should be turned over in its entirety to ICANN.\textsuperscript{26} Members of the U.S. Congress expressed similar objectives.\textsuperscript{27}

NSI responded that its customer database—which NSI had named under the trademark "Dot-Com Directory"—consisted of NSF's proprietary data, generated from the company's business operations as a registrar.\textsuperscript{28} NSI strongly opposed the efforts to restrict use of what had by then arguably become its most important asset.

The debate continued for several more months, until in September 1999, ICANN, DOC, and NSI reached an agreement pursuant to which NSI retained control of the Dot-Com Directory, and was allowed to implement the "shared registry system" that it originally had proposed to further open up competition in domain name registration services.\textsuperscript{29} To accomplish the settlement, however, NSI agreed to recognize formally ICANN and to pay ICANN $1.25 million.\textsuperscript{30}

NSF's rights to its customer database were premised on the terms of its Cooperative Agreement with NSF and on the common law governing

\textsuperscript{24} Id.
\textsuperscript{25} Id.
\textsuperscript{27} In June 1999, the House Commerce Committee held a hearing regarding ICANN, at which Department of Commerce Counsel Andy Pincus stated that he had "serious reservations" about whether NSF could retain the rights to its customer database. See Robert MacMillan, House Commerce Grills NSI, ICANN, Administration, NEWSBYTES, July 29, 1999. Counsel Pincus wrote to James Rutt, CEO of NSF, stating that Commerce "strongly objected" to NSF's restrictive use of the WHOIS database, and that "[n]othing in the [NSF] Cooperative Agreement nor in existing law gives NSF the right to restrict access to this information." Robert MacMillan, Database Is "Company Property"—Network Solutions, NEWSBYTES, July 26, 1999.
\textsuperscript{28} Robert MacMillan, Database Is "Company Property"—Network Solutions, NEWSBYTES, July 26, 1999.
\textsuperscript{30} See David McGuire, Network Solutions, ICANN Create New Plan, NEWSBYTES, Sept. 28, 1999. The ICANN agreement was successfully implemented in the first quarter of 2000, opening up additional competition with five new domain name registration services based on the NSF shared registry. On March 8, 2000, NSF announced that it would merge with VeriSign in a stock-for-stock deal valued at approximately $17 billion. Don Clark & Julia Angwin, For the Keeper of Web Names, a $17 Billion Deal, WALL ST. J., Mar. 8, 2000, at B1.
The Emerging Law of Commercial Transactions in Electronic Customer Data

protection of business trade secrets. The federal Cooperative Agreement Act provides that where a party enters into a Cooperative Agreement with a government agency, it is entitled to retain any assets generated in performing under the Cooperative Agreement. Trade secret law has traditionally protected customer lists and other information generated by businesses against disclosure and use by competitors and third parties. Under those legal authorities, there was no serious question that NSI’s rights to its customer data should have been honored.

However, the lack of express terms in the Cooperative Agreement itself and the ambiguity regarding data rights, in general, resulted in conflicting interpretations. Many government officials and private parties concerned with Internet governance and domain name registration argued that NSI should not retain the rights to its customer data. Some asserted that because NSI generated its database under a federal agreement, the data should belong to the U.S. government. Others argued that the data was proprietary to the individual domain name registrants, and therefore that no single party could claim rights to exclude others from access to the data. While the issue was resolved by agreement among the government, NSI, and ICANN, the parties and commentators ultimately did not concur with respect to the legal framework governing NSI’s rights in the Dot-Com Directory.

**REALNETWORKS**

RealNetworks dominates the market for audio and video delivery over the Internet, including the use of streaming media with an estimated 100 million users for its primary software products, RealJukebox and RealPlayer. RealNetworks was founded in February 1994, and went public in November 1997. Within days of the publication of a story in the New York Times detailing its surreptitious data collection practices, RealNetworks had been named in more than a dozen federal and three state class actions which are being consolidated for multidistrict litigation in the Northern District of Illinois.

32. See infra notes 171-77 and accompanying text.
33. See ICANN Mail Index, supra note 26.
34. Id.
35. Id.
37. Id.
Plaintiffs in these cases allege that the company's RealJukebox software, "which plays music on a computer, snooped on them once they installed it on their computers, and it reported back to the company over the Internet." Each time an individual user ran the RealJukebox program, information from the individual user's personal computer was surreptitiously transmitted back to RealNetworks. "Such information [allegedly] included the type of computer format the music is stored in; the quality level of the recordings; [the individual user's] musical preferences; and the type of portable music player, if any, the [individual user had] connected to the computer." The complaints point out that this data, once collected, was then available for RealNetworks to use for commercial purposes.

The company has disputed the charges and asserted that it never did anything improper with regard to the collection or about its individual user's listening habits or any other personal information. Nevertheless, "immediately after the alleged practice was publicized, RealNetworks altered its [published] privacy [policy] and began making available fixes that users could deploy to block the tracking technology."

The class actions against RealNetworks assert a variety of legal theories, including allegations of unauthorized access to computer data in violation of the Computer Fraud and Abuse Act, and unlawful interception of electronic communications in violation of the Electronic Communications Privacy Act. The actions also assert common law claims based on breach of contract, fraud, promissory estoppel, invasion of privacy, and negligence. In addition, RealNetworks may have violated state or federal deceptive trade practices statutes.

The RealNetworks cases demonstrate the legal risks of moving too quickly to implement data technology without regard for the basic notion of fair information practice principles.

DOUBLECLICK

"DoubleClick Inc. [Doubleclick], based in New York, is the leading Internet advertising provider, delivering 1.5 billion [banner] ads a day on

41. Id.
42. Id.
43. Id.
behalf of 1800 customers to 750 web site publishers."48 Beginning in late 1999, DoubleClick came under attack in a variety of arenas for alleged violations of privacy rights.49 DoubleClick uses “cookies” to identify the computers of individual users and to monitor the individual user’s movements around the Internet in order to better target banner advertisements. By collecting information about individual users’ interests, DoubleClick is able to tailor advertising content to improve the likelihood that an individual user will make a purchase. Cookies are small text files that are placed on a user’s computer when a user visits a particular web site. A “cookie” allows Web sites to recognize particular users on future visits, enabling Web sites to provide personalized information or to automate the log in process. On some sites, cookies are essential for navigation. Cookies were originally designed to be contained within a specific site; however, when set by an ad server, such as DoubleClick, they can be read by any server in the ad company’s domain, no matter what URL the browser is displaying or what site is on the screen. Thus, one company can collect information on a particular individual’s activities on any number of sites.50

When DoubleClick announced a plan to attach data collected on-line with consumers’ real names and addresses collected off-line, in order to better target advertisements, a major public outcry ensued.51 “The off-line information comes from a data base amassed by Abacus Direct Corp. [(Abacus)], with whom DoubleClick merged in 1999. The merger between DoubleClick and Abacus allows DoubleClick to offer a program whereby web sites can link personal information they collect to cookie information collected by DoubleClick, and the off-line [catalog-shopping] information in the Abacus data base.”52 It was this merger and the plan to combine the data that sparked concern among privacy activists such as the Electronic Privacy Information Center.53 In response to the public controversy, DoubleClick has announced that the integration of the two databases is on hold until government and industry have agreed upon adequate privacy standards.54 Nevertheless, DoubleClick is now defending itself in more than a dozen class action lawsuits, both in federal and state court, is being

50. Id.
51. Id.
52. Id.
53. Id.
54. Id.
investigated by the Attorneys General of several states, and is the subject of an inquiry by the Federal Trade Commission (FTC).\textsuperscript{55}

The DoubleClick case demonstrates that even in the absence of an obvious legal obstacle to making such changes, there may be serious practical limitations on revising posted privacy policies due to a change in business plan when a business is not prepared to notify and seek the consent of the individuals whose personal information will be affected by the change.

DoubleClick’s aggressive pursuit of marketing data through the use of cookies placed by its banner ads is causing problems for more than just DoubleClick, however. In its May 2000 report on online privacy, the FTC expressed concern over the failure of Internet sites to disclose in their privacy policies that “third-party cookies”\textsuperscript{56} were being placed on users’ computers.

\textbf{FIRST UNION}

In December 1999, First Union filed suit against Secure Commerce Services, an Internet account aggregator.\textsuperscript{57} Account aggregators permit consumers to collect information from more than one retail financial institution’s web site and present it to the consumer in a single location. Consumers must provide the aggregator with the user names and passwords they have established to access their personal account information from the web sites of financial institutions where they maintain accounts.\textsuperscript{58} The aggregator is then able to do a “screen scrape” of the consumer’s account information. Screen scraping requires a program that can translate data from the formats used by older “legacy” systems to display it and convert that data into newer formats that permit it to be displayed in graphical interfaces such as Internet browsers.\textsuperscript{59} The retail financial institution may not be able to detect the difference between its own consumer...


\textsuperscript{58} Mindy Charski, E-Finance: convenience over security, U.S. News & World Rep., May 1, 2000, at 69.

accessing his or her personal financial information, and the aggregator accessing that information on behalf of the consumer.\(^6\) As a result, the financial institution may fail to comply with applicable law governing privacy and security of personal financial records when it unknowingly releases that information to a third party. Consumers may not be aware of these restrictions, however, and may resent any obstacles a financial institution may place in the way of their choice to use an account aggregation service. Possible claims against an account aggregator might include copyright infringement if any original work of authorship is reflected in the data, violation of the Computer Fraud and Abuse Act,\(^6\) unfair competition, theft of trade secrets, or misappropriation. In addition, the action by the aggregator may result in the regulated financial intermediary breaching its own obligations under the Electronic Funds Transfer Act,\(^6\) Regulation E,\(^6\) or other consumer protection law requiring statements, disclosures, or error resolution services to be provided to a consumer in connection with an electronic financial service.

First Union’s complaint against the account aggregator shows the vulnerability of database assets in the insecure environment of the Internet and the problems created by the lack of a secure, widely used system for authentication of identities in Internet commerce.\(^6\)

**BIDDER’S EDGE**

eBay maintains an Internet auction site that permits registered users of the service to offer items for sale or to make bids on items offered by others. Users of the eBay site must register and agree to the terms of the eBay User Agreement, which prohibits the use of “any robot, spider, other automatic device, or manual process to monitor or copy our web pages . . . without our prior expressed written permission.”\(^6\) Bidder’s Edge, AuctionWatch, and other auction-listing aggregator sites use comparison shopping bots to collect information about listings on other Internet auction sites such as eBay and then provide their own users with direct access to those listings on the eBay site.\(^6\) eBay has license agreements with some

\(^6\) Charski, supra note 58.
\(^6\) Banks Look Forward To Becoming Aggregators, RETAIL DELIVERY NEWS, Apr. 26, 2000.
\(^6\) eBay, Inc. v. Bidder’s Edge, Inc., 100 F. Supp. 2d 1058 (N.D. Cal. 2000) (order granting preliminary injunction). “Programs that recursively query other computers over the Internet in order to obtain a significant amount of information are referred to . . . by various names, including software robots ['bots'], . . . spiders and web crawlers.” Id. at 1060 n.2. These programs “perform searching, copying, and retrieving functions” on the web sites of others. Id. at 1060.
aggregators, granting them permission to re-list eBay’s auction goods. Other aggregators have been unwilling to enter into such license agreements, and eBay has taken steps to block their access to its servers in an attempt to stop searches of its databases by bots and “deep linking” into its site.67

eBay filed suit against Bidder’s Edge in December 1999 alleging that after Bidder’s Edge had failed to reach agreement with eBay in negotiations for a license to search the eBay site, Bidder’s Edge had continued to access the eBay site approximately 100,000 times a day.68 This constituted approximately one percent of all traffic on the eBay site.69 eBay requested that Bidder’s Edge stop listing eBay auction items on its site, but Bidder’s Edge refused to do so. eBay then tried to prevent Bidder’s Edge from accessing its site by blocking the IP addresses Bidder’s Edge was using, but Bidder’s Edge managed to evade these controls by accessing the site from proxy servers.70 eBay sought a preliminary injunction to prevent Bidder’s Edge from accessing its site and cited eight legal theories: (i) trespass to chattels, (ii) false advertising under the Lanham Act,71 (iii) federal and state trademark dilution, (iv) violation of the Computer Fraud and Abuse Act,72 (v) unfair competition, (vi) misappropriation, (vii) interference with prospective economic advantage, and (viii) unjust enrichment.73 On May 24, 2000, the district court granted the preliminary injunction based on the trespass to chattels theory, barring Bidder’s Edge from further accessing the eBay site pending disposition of the litigation.74

The eBay case against Bidder’s Edge shows how difficult it may be for an Internet business to preserve the value of its franchise when part of its business model involves displaying sensitive information on a public, insecure network. It also shows the limitations of clickwrap agreements as a form of defense against unauthorized access and use of that information.

**BOO.COM AND TOYSMART.COM**

The effects of bankruptcy on the dot-com world are just beginning to be measured. How liquidators will value dot-com assets, and how this valuation will affect the rights of creditors, joint venturers, licensors, and licensees is at present a relative unknown. The failures in mid-2000 of Boo.com and Toysmart.com, however, illustrate some of the issues that will arise as more dot-coms seek bankruptcy protection.

67. Id. at 23.
68. eBay, 100 F. Supp. 2d at 1063.
69. Id.
70. Id.
73. eBay, 100 F. Supp. 2d at 1063.
74. Id. at 1073.
In 1999, Boo.com was launched as a state-of-the-art fashion web site. Its highly-sophisticated three-dimensional clothing display, which cost more than £70 million to develop, attracted more than five hundred thousand visitors per month.\(^{75}\) A "Club Boo" membership club and newsletter service were employed to generate a substantial database of actual and potential customers. The company, however, could not generate sufficient revenues to cover its expenditures and filed for bankruptcy just six months after its launch.\(^ {76}\)

By May 2000, Boo.com had liquidated most of its assets. Its "front-end" assets, including its brand, web site, and associated intellectual property, were sold to another web fashion company, Fashionmall.com, based in New York City.\(^ {77}\) Most significantly, Fashionmall.com acquired data on 350,000 Boo.com customers,\(^ {78}\) with no indication of compliance with Boo.com's privacy policies or EU requirements relating to customer data.\(^ {79}\)

Toysmart.com launched its web site in early 1999, offering a broad selection of discount toys through e-commerce consumer sales. In September 1999, Toysmart became a licensee of TRUSTe, a group that reviews and certifies on-line privacy policies. Toysmart posted the following privacy statements on its web site: "Personal information voluntarily submitted by visitors to our site, such as name, address, billing information and shopping preferences, is never shared with a third party," and "[w]hen you register with toysmart.com, you can rest assured that your information will never be shared with a third party."\(^ {80}\)

On June 9, 2000, creditors of Toysmart.com forced the struggling company into involuntary bankruptcy.\(^ {81}\) Prior to the involuntary petition, Toysmart.com had retained the services of The Recovery Group, a Boston management consultant, in an effort to find buyers for its assets. A Wall Street Journal advertisement for Toysmart.com's asset sale listed, among other things: "Intangibles, i.e., URL name, databases, customer lists, marketing plans, web site content, [and] software intellectual property."\(^ {82}\)

76. Id. While Boo.com's insolvency proceeding was governed by non-U.S. law, the issues presented are very similar to those that will arise for U.S. Internet companies faced with insolvency.
77. Id.
79. See infra notes 284-308 and accompanying text.
Shortly after the *Wall Street Journal* advertisement appeared, consumers, privacy activists, and others protested the sale. On July 10, 2000, the FTC filed a complaint in the bankruptcy case, seeking a permanent injunction against the sale of Toysmart.com’s customer lists and a declaration that any such sale would constitute a violation of the FTC Act, in light of the privacy statements previously published by Toysmart.com. Shortly thereafter, Toysmart.com entered into a settlement agreement with the FTC, allowing Toysmart.com to sell its customer list to a buyer “in a related market.”

Boo.com and Toysmart.com illustrate the potential conflict of privacy interests and creditors’ rights in the context of insolvency. The cases also show the significance of the divergent approaches to privacy in the United States and the EU. While the FTC complaint in Toysmart.com was based solely on the company’s own privacy policy, EU directives could allow such an action by EU data protection authorities even in the absence of a company privacy policy. Finally, these cases raise the question whether creditors should seek security interests in data where customer databases are key assets of electronic commerce companies.

**BUSINESS-TO-BUSINESS E-HUBS**

In the last year, many businesses and organizations have announced their intention to play a role in facilitating business-to-business commerce by establishing new Internet marketplaces. These marketplaces may be “vertical” if they serve a single industry; examples of this type of marketplace include Enron Online, Commerx PlasticsNet, and Chemdex. They may be “horizontal” if they provide the same functions or automate the same business processes across different industries; examples of this type of marketplace include MRO.com, Ariba, and Employease. One

---

84. *See FTC News Release, supra note 81.*
85. *FTC Approves Pact Allowing Toysmart’s Customer-List Sale, WALL ST. J., July 24, 2000, at A28. The restrictions agreed to, however, were subsequently overturned by U.S. Bankruptcy Judge Carol Kenner, who ruled that restricting the sale to a particular type of buyer was premature and counterproductive. Jerry Guidera & Frank Byr, *Judge Refuses to Set Conditions on Toysmart Sale, WALL ST. J., Aug. 18, 2000, at B6.*
The major business benefit of participation in these "e-hubs"\textsuperscript{93} is the returns to scale they offer: a seller can contact dozens or hundreds of buyers with a single message into the network; a buyer can compare a wide range of offers from sellers with a single search. Because of this economic advantage, these e-hubs are expected to become an important feature of the business-to-business electronic commerce landscape within the near future, although in 2000, many of these projects had not yet progressed beyond the design phase.\textsuperscript{94}

It is likely that different e-hubs will pursue different business models. Some will maintain a neutral position between buyers and sellers while some will be organized for the benefit of either a group of buyers or a group of sellers. Some will be organized as proprietary ventures while some will be organized as industry associations. One of the many issues that each e-hub will have to resolve among its different groups of stakeholders will be what types of data will be collected and by whom; under what conditions third parties may be granted access to these data collections; and what uses may be made of these data collections.\textsuperscript{95} For example, the rules of the marketplace could be expected to have provisions governing the conditions under which buyers may analyze information about the behavior of sellers, or sellers may analyze information about the behavior of buyers. Given that many of the participants in the marketplace may have interests adverse to one another, it will be important to make clear the scope of permitted collection, analysis, and transfer of data generated by the operation of the marketplace.

The example of e-hubs shows the importance of: (i) identifying the flows of data within a cooperative framework; (ii) identifying possible adverse interests among participants; (iii) technological opportunities for the collection of data as well as blocking the collection of data; (iv) security to prevent access to sensitive data by those not admitted to the e-hub; and (v) drafting of agreements to cover the rights and responsibilities of the participants in the e-hub. Major e-hubs present the scenarios of a market structure similar in scale and complexity to airline CRS systems discussed above, but without government regulation. With the addition of new and powerful data technologies discussed below, organization and management of these relationships presents major legal challenges.


\textsuperscript{94} See generally id. (explaining the importance of the B2B landscape).

BUSINESS AND TECHNOLOGY DRIVERS AFFECTING THE GROWING USE OF DATABASES

The anecdotal evidence presented by these case studies indicates that the number of disputes and potential disputes over ownership of data is increasing rapidly. If this is the case, it may reflect major recent changes in the technological framework for electronic commerce that have not yet been adequately assimilated into commercial law doctrines. Important technological changes that have made it easier to develop databases include the migration of electronic commerce from closed, secure networks to open, insecure networks that make it much easier to harvest a wide array of data without the knowledge or consent of interested parties. Advances in data mining and customer profiling technologies permit the conversion of what would once have been an indigestible mass of random information into valuable marketing data. In addition, merchants must now compete in marketplaces offering access to millions of potential customers, but within which customers have become more fickle and impatient, thus requiring merchants to be ever more sophisticated and prompt in anticipating and meeting the needs of customers and prospective customers.

New technology also can create threats to electronic commerce companies. For example, recent developments in distributed information sharing may make it impossible to prevent worldwide distribution of data once it becomes public, or to enforce intellectual property rights to that data. Effective data security technology and processes therefore are critical to companies that rely on consumer databases, and increasingly important to avoiding legal liabilities.

EXPANDING COMPUTER COMMUNICATION NETWORKS AND DATA CAPTURE OPPORTUNITIES

The open architecture of the Internet has created an environment for electronic commerce in which there are many more opportunities for, and many fewer institutional constraints on, collecting data than were formerly possible. In the 1970s, databases were stored on mainframe computers, and those computers were often kept isolated in rooms with special climate controls.96 When data was shared among computers, it might be transported on punch cards or rolls of magnetic tape. Concepts that appear in some data privacy laws such as "data controller"97 originated at the time because there was normally a unique person or group of persons who controlled access to information on a computer. When computer networks were first built, they were connected by dedicated communications lines such as

96. Computers were located in cold rooms to preserve magnetic tape media.
owned or leased lines, or relied on the services of “value-added networks” that guaranteed a high level of security and integrity in communications.

The Internet is an open, public, cooperative facility accessible to an almost unlimited number of people worldwide. While there are standard-setting organizations such as the Internet Engineering Task Force and the World Wide Web Consortium that help develop standards for the Internet, no central organization has authority or responsibility for it. The networking standards that permit data to be exchanged over the Internet were designed to maximize flexibility, resilience, and openness rather than to achieve a high degree of security for communications flowing over the network.98 There are no authoritative security standards for computer systems connected to the Internet, and the degree of information system security in place at different sites varies widely. The security of the operating systems or the network systems that connect individual computers to the Internet has not kept up with the security challenges created by the openness of the Internet. Because the difficulty of maintaining the security of computer systems connected to the Internet has increased dramatically, many system administrators can no longer maintain the same level of security that was once possible. As a result, security problems are now endemic to the Internet and there is unlikely to be any improvement in the near future.99

Once information is stored on a server that is connected to the Internet, that information may be accessed by anyone with access to the Internet unless some access control is established. Given the open architecture of the Internet, effective access controls may be difficult to design or maintain.100 When an individual is using the Internet, his or her behavior may

---

98. The Internet is a “packet-switched” network, unlike the telephone network, which is a “circuit-switching” network.

Packet-switched describes the type of network in which relatively small units of data called packet are routed through a network based on the destination address contained within each packet. Breaking communication down into packets allows the same data path to be shared among many users in the network. This type of communication between sender and receiver is known as connectionless (rather than dedicated). Most traffic over the Internet uses packet switching and the Internet is basically a connectionless network.

Whatis.com, packet-switched [last modified Dec. 1, 2000], available at <http://www.whatis.com/WhatIs_Definition_Page/0,4152,212737,00.html>. The packet-switched format was chosen during the Cold War for the Internet to make it more resilient in the event an attack destroyed part of the network.

99. See generally NATIONAL RESEARCH COUNCIL, TRUST IN CYBERSPACE (Fred B. Schneider ed., 1999).

100. For this reason, it is common to place information accessible from the Internet on a proxy server outside the firewall of an enterprise rather than permit direct access through the firewall into the enterprise. See Whatis.com, proxy server [last modified Apr. 14, 2000], available at <http://www.whatis.com/WhatIs_Definition_Page/0,4152,212840,00.html>.

be observable to a large number of other individuals, and a record of that behavior may also be collected and saved without the individual’s awareness. A record of everything that happens while an individual is visiting a site may be captured by the site owner in server log files and later analyzed.101 Web traffic analysis measures the number of pages delivered to visitors, how long it took to load a completed page, and how much data was transmitted.102 In addition, ActiveX, Java, or JavaScript applets103 may be sent to the visitor’s personal computer by the server to create animations, perform calculations, or send back to the server copies of information from the visitor’s computer. For example, an applet could send back to the server a copy of the browser’s “history file” which keeps a record of all web pages the end user has visited recently.104 This is the type of undisclosed end user monitoring RealNetworks used for marketing purposes that resulted in the filing of several class action lawsuits.105

Unless some additional steps are taken, however, it may be difficult to determine which person is associated with a particular online behavior that has been observed and recorded. Any computer that is part of the Internet needs to have an IP address106 in order to be recognized by the network, but there is not yet a universally accepted system for tying the identity of a specific person to an IP address or any other form of online identifier. The technology for placing text files known as “cookies” on the hard drive of individual users of Internet browsers was first developed with Netscape version 1.1 to permit individual users to access web

103. An applet is a small program that can be sent to an end user’s computer together with a requested web page. WhatisPcom, applet (last modified Aug. 3, 2000), available at <http://www.whatis.com/WhatIs_Definition_Page/0,4152,211580,00.html>. The applet may be sent without the end user’s knowledge; the scope of the applet’s functions may not be clear to the end user.
105. See RealNetworks case study, supra notes 36-47 and accompanying text.
106. In the most widely installed level of the Internet Protocol [IP] . . . today, an IP address is a 32-binary digit number that identifies each sender or receiver of information that is sent in packet across the Internet. When you request an HTML page or send e-mail, the Internet Protocol part of TCP/IP includes your IP address in the message (actually, in each of the packets if more than one is required) and sends it to the IP address that is obtained by looking up the domain name in the [URL] you requested or in the e-mail address you’re sending a note to. At the other end, the recipient can see the IP address of the web page requestor or the e-mail sender and can respond by sending another message using the IP address it received.

sites without having to reenter identifying information each time. The use of cookies to identify users and track their movements need not be limited to movements on a single web site, however, as cookies are now used by Internet advertisers to track individual users' movements from site to site. While the cookie file on a user's hard drive need not contain any personally identifying information about an individual user, it may nevertheless permit the party collecting clickstream data to associate Internet browsing with a real world identity if the user has provided personally identifying information through a registration form.

Many free offers available to individual users are not free at all, but involve loading software onto the individual's computer that transmits a wide range of information about the online activity of the individual. For example, free Internet access providers such as Netzero, AltaVista, and Freeinternet.com collect clickstream data in order to monitor individual behavior online. The acquisition of that data, which clearly has some market value even if the provider of the "free" service undertakes not to sell that data to third parties, is what subsidizes the services provided to users without charge.

In this environment, it may be very difficult for individuals or organizations to be sure what information is being collected, to what uses that information is being put after it has been collected, or with whom the information is being shared. Privacy policy statements or other contractual undertakings may provide a starting point for finding answers to these questions, but formal undertakings with regard to data practices and actual data practices may diverge due to conscious disregard, due to failure to implement policies and procedures to guarantee compliance, or due to failure to implement adequate technological safeguards. For example, RealNetworks appears to have either made a management decision to collect personal information outside the scope of its posted privacy policy in order to obtain a marketing advantage, or to have failed to implement policies and procedures that would have led employees to realize that such a major departure from its posted privacy policy would not be condoned by top managers. Other organizations appear to have posted privacy policies without taking the necessary steps to make sure those policies are adhered to consistently. For example, in January 2000 Drkoop.com's privacy policy stated:


The only information drkoop.com obtains about visitors to its Web site is information supplied voluntarily by visitors.\textsuperscript{110}

Yet, this statement was contradicted by Drkoop.com's practice of placing cookies on its visitor's computers and profiling their online activities, which was made clear from the terms of service posted on the site:

The cookie itself does not contain Locator Information although it will enable drkoop.com to relate your use of the site to information that you have specifically and knowingly provided to the site.\textsuperscript{111}

Faulty web design and communications security may also create situations where an organization unintentionally releases data to third parties in violation of its stated privacy policy or other contractual undertaking. For example, in January 2000 a study of the privacy policies and practices of health care web sites uncovered several web sites that accidentally sent their user's email address, customer ID number, or other personally identifiable information to banner ad network companies when the user clicked on a banner ad, due to faulty HTML coding in the health care web site itself.\textsuperscript{112}

\textbf{EXPANDING DATA ANALYSIS TOOLS}

A database is a collection of data that is organized so that its contents can easily be accessed, managed, and updated.\textsuperscript{113} The most prevalent type of database is the relational database, in which data is defined so that it can be reorganized and accessed in a number of different ways without having to reorganize the database. A user can make interactive queries for information from a relational database or can gather data for reports. Databases may support transaction-processing operations or marketing and management decisions within an organization. Until recently, databases created and maintained to support operations within an organization were standard elements of business IT systems, but the use of separate databases designed specifically to support marketing and management decision making was not common. Advances in database technologies and falling costs for data storage and analysis are making the creation of separate databases designed specifically to support marketing and management decision making much more common.

The term "data warehouse" is often used to describe separate databases that have been designed to support marketing and strategic decision-

\textsuperscript{111.} \textit{Id.}
\textsuperscript{112.} \textit{Id.} at 36.
\textsuperscript{113.} \textit{WEBSTER'S NEW WORLD DICTIONARY} 352 (3d ed. 1988).
A data warehouse is a central repository for all or significant parts of the data that an enterprise's multiple business systems collect. Data is first gathered from various sources, such as online transaction processing applications, then selectively extracted and organized within the data warehouse database for use by analytical applications and user queries. One of the major challenges facing businesses with online operations today is the integration of clickstream data collected from visits to a web site with data collected from operations processed by legacy systems. Once the logistical problems associated with creating "webhouses" that combine data from web and legacy systems have been resolved, businesses will have very powerful support systems to aid in marketing and strategic decision making.

"Data mining is the analysis of data for relationships that have not previously been discovered. For example, the sales records for a particular brand of tennis racket might, if sufficiently analyzed and related to other market data, reveal a seasonal correlation with the purchase by the same parties of golf equipment," pay-per-view television programs, or over-the-counter health products. Data mining can (i) establish associations between facts that were not known to have any correlation; (ii) determine chronological sequences of events; (iii) facilitate classification of data according to newly recognized patterns such as customer profiles; (iv) allow clustering of data into groups not previously known; and (v) support forecasting based on newly discovered patterns that aid prediction. The data warehouse concept is gaining acceptance in part because of the possibility of fruitful data mining.

COMPETITIVE ADVANTAGES FROM EFFECTIVE EXPLOITATION OF DATABASES

The combination of larger, more robust customer databases and sophisticated data warehousing and mining technology can offer substantial competitive advantages to electronic commerce businesses. Companies can develop the ability to better identify likely customers and to recognize and anticipate individual preferences, resulting in increased sales and higher margins. In addition, once it is assembled, a customer database
may be shared with other companies, offering an additional revenue stream at a low incremental cost.

These benefits may be offset by the potential transaction costs of transacting in consumer data and the greater uncertainty created in today's changing legal environment. Business models that operate within the letter of the law may nevertheless be challenged by regulatory agencies and litigants that seek to expand on existing privacy theories.120

**THREATS TO INTELLECTUAL PROPERTY RIGHTS POSED BY DISTRIBUTED INFORMATION-SHARING TECHNOLOGY**

New technology not only creates opportunity, but also presents significant threats to electronic commerce companies. Recent advances in information-sharing technology have markedly increased the importance of data security in maintaining and sharing database assets.

An important attribute of computer networks is the ability to share and send data files. Given the increased capabilities for file sharing on the Internet, legal constraints such as copyright and licensing requirements become even more important to the owners of databases and similar intellectual property. While the Internet creates greater potential for abuse of data rights than traditional media, enforcement still is possible by tracking data transfers to specific servers and seeking an injunction prohibiting the owner of the server from any further distribution in violation of such legal rights.

However, a new type of software has been developed that allows individuals to search directly within each others' hard drives and download any files contained in special user-designated folders. This new software is known as "peer-to-peer information-sharing technology," or P2P for short.

These information-sharing programs, such as Napster, Gnutella, and Freenet, enable users to freely distribute information to one another, regardless of copyright or other legal constraints. For example, the Napster web site contains the program which must first be downloaded. Thereafter, the web site need only be accessed to assist the user in matching his or her music file request with another Napster user whose hard drive contains the requested file. The files themselves are not stored at the Napster site. Napster does, however, depend on a central server to resolve data requests and verify identities of participants, so that there is a potential legal remedy for copyright abuse—shutting down Napster's business. This is precisely

120. *See supra* notes 37-56 and accompanying text.
the remedy sought by the Recording Industry Association of America in a lawsuit filed against Napster in June 2000. 124

By contrast, later generation programs such as Gnutella and Freenet allow uncontrolled file sharing by participants, without any central server or other point of control. Once a user has downloaded the operating program, the user can access open files maintained by any other program participant through a "broadcast search" that seeks out the file on the systems of all of the individuals participating. 125

Gnutella poses an even greater potential threat to holders of trade secrets. For example, Napster users may only use the program to download MP3 music files. 126 In contrast, Gnutella users can transfer any type of computer file, including databases and MSWord documents. 127 Furthermore, it is possible for ISPs to block access to the Napster site, 128 whereas the only way to prevent files from being transferred via Gnutella would be to disable every machine of every Gnutella user. 129

Gnutella does not rely on a central repository of information. 130 There is no one "target" for aggrieved parties to single out for legal action. Gnutella is a technology, not an entity. Freenet is similar, but goes a step further, adding a built-in system to ensure the anonymity of senders, recipients, and storers. 131 The system is designed to "transparently" move, replicate, and delete files as necessary. 132


125. Its designers see Freenet as a technology that will "liberate" information, operating under the principle that "information, by nature, seeks to be free." Ian Clarke, et al., Freenet: A Distributed Anonymous Information Storage and Retrieval System (July 1, 2000), available at <http://www.freenetproject.org/index.php?page = theoppr>.

126. An extension, however, of the Napster protocol called OpenNap, <http://opennap.sourceforge.net>, permits sharing of any media type. Doug Bedell, Filing through file-sharing software, DALLAS MORNING NEWS, June 22, 2000, at 8F.


129. Or to pull Gnutella out of circulation, as occurred shortly after Gnutella was created by Nullsoft, a subsidiary of AOL. AOL reportedly paid 21-year old Gnutella developer Justin Frankel $100 million for it, then promptly removed it from the Internet at the behest of Time-Warner, which (i) is in the process of being acquired by AOL, and (ii) is suing Napster, alleging copyright infringement. See Julia Angwin, AOL Takes Step To Let Customers Download Music, ASIAN WALL ST. J., June 29, 2000, at 13, 2000 WL-WSJA 2942265; Diary: Tamed Rebel, MARKETING WK., June 29, 2000, at 62, 2000 WL 10579026. In spite of this, Gnutella is still widely available, and other similar programs have been, and are now being, produced.


131. See Clarke et al., supra note 125.

132. Id.
The advent of these peer-to-peer information-sharing technologies has important implications for licensors and other compilers of customer data. Companies that own data assets should not assume that they will be able to enforce copyright or contract protections for databases should they become public. Accordingly, effective data security and encryption will become increasingly vital to protect the value of data and other intangible assets and to ensure compliance with privacy laws.133

CURRENT U.S. LEGAL FRAMEWORK FOR PROTECTION OF DATABASE ASSETS

The U.S. law that applies to transactions in data assets is drawn from a number of sources, including federal statutes enacted pursuant to the Intellectual Property Clause of the U.S. Constitution; common law theories; contract law; and the Uniform Commercial Code and proposed Uniform Computer Information Transactions Act. These are summarized below in turn, followed by a discussion of individuals' privacy rights and legislative attempts to create new database rights in the United States.

COPYRIGHT PROTECTION OF DATABASES AS COMPILATIONS

Article I, section 8 of the U.S. Constitution grants Congress the power "[t]o promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries."134 In enacting intellectual property legislation, Congress has balanced the need to incentivize and protect the rights of authors and inventors135 with the public's rights to access, particularly to facts and factual materials.

The 1976 Copyright Act expressly covers nine categories of works, including "compilations."136 "A 'compilation' results from a process of se-
lecting, bringing together, organizing, and arranging previously existing material of all kinds, regardless of whether the individual items in the material have been or ever could have been subject to copyright.” The protection accorded to a compilation, however, “extends only to the material contributed by the author of such work, as distinguished from the preexisting material employed in the work, and does not imply any exclusive right in the preexisting material.”

Historically, Congress and the Supreme Court based legal protection for compilations and databases on two distinct theories. The first, known as the “sweat of the brow” theory, provided protection where compilations resulted from substantial effort and investment of the creator. The second rationale based copyright protection on the “selection and arrangement” of the underlying data, requiring elements of originality or creativity, regardless of the extent of the effort employed.

In *Feist Publications, Inc. v. Rural Telephone Service Co.*, however, the U.S. Supreme Court expressly rejected the “sweat of the brow” theory. *Feist* considered whether a White Pages phone book—a quintessential database, listing names, addresses, and phone numbers of persons living in a defined geographic area in alphabetical order—was entitled to copyright protection.

*Feist* Publications, Inc. (*Feist*) sought to compile a White Pages telephone book for the state of Kansas. *Feist* offered to pay for rights to use data collected by local telephone publishing companies. All of the local publishers agreed, with the exception of Rural Telephone (*Rural*). *Feist* went forward with its comprehensive directory, including publication of 1,309 of *Rural*'s listings without *Rural*'s permission. *Rural* sued, alleging breach of copyright in its White Pages listings. The case ultimately reached the U.S. Supreme Court.

In rejecting the “sweat of the brow” theory previously relied on to protect compilations, the Court found that the purpose of copyright was to motivate authors to create works and not to reward them based solely on “industrious efforts.” The 1976 revisions to the Copyright Act leave no doubt that originality, not “sweat of the brow,” is the touchstone of copyright protection in directories and other fact-based works. The Court noted

139. See Jeweler's Circular Publ'g Co. v. Keystone Publ'g Co., 281 F. 83, 88 (2d Cir. 1922).
142. Id. at 344.
143. Id. at 349 (“The primary objective of copyright is not to reward the labor of authors, but '[:]'to promote the Progress of Science and useful Arts.'” (quoting U.S. Const. art. I., § 8, cl. 8)).
that the threshold requirement for establishing originality was low, and that factual compilations may meet the requirement where the author's selection and arrangement of the facts is original.\textsuperscript{144} Because Rural expended insufficient creativity to make the White Pages directory original, it was not protected under copyright.\textsuperscript{145} A number of later cases have applied the \textit{Feist} originality analysis in denying copyright protection for databases.\textsuperscript{146}

\textit{Feist}'s holding is sound as a matter of copyright law. Its practical import, however, is problematic for database companies. Many commercially valuable databases consist of vast quantities of data that are aggregated at great expense for a variety of later uses but in basic form are not "selected" or "arranged" in any particular way. These data often are processed using software that allows the end user to sort and use them most productively. Thus, a competitor who can access the underlying data need only modify the software interface, or the underlying arrangement and/or selection, and will avoid copyright violation under \textit{Feist}. This was the holding in \textit{Matthew Bender & Co. v. West Publishing Co.},\textsuperscript{147} where the defendant extracted substantial components of West's case law database, including West's "star pagination" system, and was found not to have violated the Copyright Act.\textsuperscript{148}

\textbf{COMMON LAW THEORIES OF DATABASE PROTECTION}

\textbf{"Hot News" and Common Law Misappropriation}

Facts themselves are not eligible for protection under copyright law.\textsuperscript{149} In certain cases, however, courts have found common law rights associated

\begin{itemize}
\item\textsuperscript{144} Id. at 348 ("[C]hoices as to selection and arrangement, so long as they are made independently by the compiler and entail a minimal degree of creativity, are sufficiently original that Congress may protect such compilations through the copyright laws." (citing \textsc{Melville B. Nimmer & David Nimmer, Nimmer On Copyright §§2.11[D], 3.03 (1990)). The Court found the originality requirement in the language of the Copyright Act governing "original works of authorship," 17 U.S.C. § 102(a), as well as an implicit requirement under the Intellectual Property clause of the Constitution. \textit{Id.} at 355.
\item\textsuperscript{145} Id. at 362-64.
\item\textsuperscript{147} 158 F.3d 693 (2d Cir. 1998).
\item\textsuperscript{148} \textit{Id.} at 708; \textit{see also} \textit{Warren Publ'g, Inc. v. Microdos Data Corp.}, 115 F.3d 1509 (11th Cir. 1997) (directory of U.S. cable television systems lacked creativity required to obtain copyright protection after \textit{Feist}; refusing to enjoin third party distribution of electronic copy of Warren's Television & Cable Factbook).
\item\textsuperscript{149} \textit{Feist}, 499 U.S. at 351.
\end{itemize}
with the use or publication of commercially valuable facts, typically under the tort doctrine of misappropriation.

The landmark Supreme Court case of International News Service (INS) v. Associated Press (AP)\(^{150}\) held that commercially valuable "hot news" would be protected for limited time periods against wrongful misappropriation by competing businesses. During World War I, INS transmitted AP news reports to INS newspapers, which were used to prepare stories issued by newspapers in direct competition with AP papers. AP sued, seeking to enjoin this practice. The Court held that although news reports were not protectable by AP as against the public, INS's practice of exploiting them for commercial gain constituted misappropriation, a form of unfair competition.\(^{151}\) Specifically, the Court held that where a defendant unfairly procures factual material acquired by a competitor, and the defendant uses such material in competition with the defendant, relief would be appropriate under the tort doctrine of misappropriation.\(^{152}\)

The "hot news" theory established by INS offered an alternative to copyright law in protecting data assets against commercial exploitation. By focusing on the commercial interests posed in conflicts over data use, the courts could avoid the lack of copyright originality in many compilations. This potential protection, however, has been largely eliminated by application of preemption principles resulting from the comprehensive federal statutory framework governing copyright.\(^{153}\)

The Copyright Act includes an express provision defining the scope of preemption of state statutes and common law.\(^{154}\) State laws that create copyright-like rights are preempted if: (i) the material protected comes within the subject matter of copyright (i.e., is a type of work generally protected by copyright); and (ii) the state laws establish rights equivalent to any of the exclusive rights within the general scope of the copyright statute (i.e., the right asserted is equivalent to a right protected by copyright.)\(^{155}\) Accordingly, courts addressing misappropriation claims following

\(^{150}\) 248 U.S. 215 (1918).

\(^{151}\) Id. at 235-36.

\(^{152}\) Id. at 241-42.

\(^{153}\) As a result of this potential conflict with preemption principles, \(\text{INS}\) has been limited in subsequent opinions. See, e.g., Cheney Bros. v. Doris Silk Corp., 35 F.2d 279, 280 (2d Cir. 1929).


\(^{155}\) [All legal or equitable rights that are equivalent to any of the exclusive rights within the general scope of copyright as specified by section 106 in works of authorship that are fixed in a tangible medium of expression and come within the subject matter of copyright as specified by sections 102 and 103 . . . are governed exclusively by this title. Thereafter, no person is entitled to any such right or equivalent right in any such work under the common law or statutes of any State.

\(\text{Id.}\)
INS have held that state law must require proof of some "extra element" of protection by a plaintiff to avoid federal preemption.\textsuperscript{156}

A number of cases have applied "hot news" analysis and found an "extra element" of protection under common law principles.\textsuperscript{157} Any potential expansion, however, of the "hot news" doctrine appears to have been cut short as a result of the Second Circuit’s recent opinion in \textit{National Basketball Association v. Motorola, Inc.}\textsuperscript{158} (NBA) and subsequent cases.

\textit{NBA} arose out of a business launched by Motorola, Inc. to market a pager product for the dissemination of real-time information about NBA games. Motorola did not enter into an agreement with the NBA establishing rights to distribute this information. Motorola contracted with Sports Team Analysis and Tracking Systems, Inc. (STATS) to perform the information gathering from radio and television broadcasts, followed by transmission of the data via satellite to radio stations and then to Motorola pagers and a public web site. At the time the case was filed, the NBA had recently established its own information service, "Gamestats," to provide similar real-time information such as updates on game scores, although the service was not "live" at the time of trial.

The NBA and NBA Properties, Inc. filed suit seeking an injunction prohibiting the Motorola paging business, alleging copyright infringement, false advertising under the Lanham Act,\textsuperscript{159} and misappropriation, among other counts. The district court dismissed the copyright claim, but held that Motorola improperly misappropriated valuable NBA-generated information.\textsuperscript{160} The court applied the doctrine of "partial preemption," finding that although broadcasts of NBA games would be entitled to copyright protection, the games themselves were not,\textsuperscript{161} and therefore that the "subject matter" test for preemption had not been met.\textsuperscript{162} The court held in favor of the NBA on the claim of misappropriation, finding that Motorola and STATS "do not contribute in any manner ... to th[e] value upon which their product relies."\textsuperscript{163} Their service, in effect, deprived the NBA of its right to reap its own just reward.

On appeal, the Second Circuit reversed, holding that the NBA-generated data sold by Motorola and STATS met the "subject matter"

\textsuperscript{158} 105 F.3d 841 (2d Cir. 1997).
\textsuperscript{161} \textit{NBA}, 939 F. Supp. at 1093, 1097.
\textsuperscript{162} Id. at 1098 n.24.
\textsuperscript{163} Id. at 1105.
standard for preemption. “Although game broadcasts are copyrightable while the underlying games are not, the Copyright Act should not be read to distinguish between the two when analyzing the preemption of a misappropriation claim based on copying or taking from the copyrightable work.”\textsuperscript{164} Such a distinction would significantly expand states’ power to enact copyright-like protections for non-copyrightable works, and “render the preemption intended by Congress unworkable.”\textsuperscript{165} Considering the broadcasts and the underlying games together, the court concluded that the facts taken from the NBA games by STATS and Motorola were within the subject matter of copyright, thereby preempting application of the common law.\textsuperscript{166}

The court went further, stating that: “[O]nly a narrow ‘hot-news’ misappropriation claim survives preemption for actions concerning material”\textsuperscript{167} that satisfies the subject matter prong of the preemption test, where the plaintiff can prove: (i) the time-sensitive nature of the factual information, (ii) free riding by the defendant, (iii) a threat to the very existence of the product or service offered by the plaintiff, (iv) the plaintiff generates or collects the information at some cost or expense, and (v) the defendant’s use of the information is in direct competition with the product or service offered by the plaintiff.\textsuperscript{168} The information gathered and transmitted by Motorola and STATS was of course time sensitive, but was gathered and transmitted at their expense, and did not constitute “free-riding” or pose a threat to the NBA’s “Gamestats” products.\textsuperscript{169} Because the claim did not meet the narrow “hot news” test, it was preempted under the Copyright Act.\textsuperscript{170}

**Trade Secrets**

The common law trade secret doctrine can provide an alternative source of protection for databases. The doctrine generally protects valuable, confidential business information from misappropriation where the holder takes reasonable measures to maintain its secrecy. “Because of the intan-

\textsuperscript{164} See National Basketball Ass’n, Inc. v. Motorola, Inc., 105 F.3d at 848-49; see also 17 U.S.C. § 101 (1994 & Supp. IV 1998) (protecting a “fixed” broadcast if it is simultaneously recorded).

\textsuperscript{165} National Basketball Ass’n, Inc. v. Motorola, Inc., 105 F.3d at 849.

\textsuperscript{166} See id. at 848-50.

\textsuperscript{167} Id. at 852.

\textsuperscript{168} Id.

\textsuperscript{169} See id. at 854. The court found three distinct NBA-generated informational products: (i) generating information by hosting professional basketball games; (ii) “transmitting live, full descriptions of those games” (e.g. broadcasting the games); and (iii) “collecting and retransmitting strictly factual information about the games.” See id. at 853. It found no “competitive effect whatsoever” in relation to the first two products, and that the market would reward the “superior” product in relations to the third, rather than prevent the NBA from entering that market at all. See id. at 853-54.

\textsuperscript{170} See id.
The Business Lawyer; Vol. 56, November 2000

gible nature of a trade secret, the extent of the property right therein is defined by the extent to which the owner of the secret protects his interest from disclosure to others.\footnote{171}

The Uniform Trade Secrets Act,\footnote{172} enacted in forty-one states and the District of Columbia, defines "Trade Secret" as:

information, including a formula, pattern, compilation, program, device, method, technique, or process, that:

(i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and

(ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.\footnote{173}

The trade secret doctrine has been used in a number of cases to protect customer lists and other databases from misappropriation.\footnote{174} Because of the secrecy requirement, however, the trade secret doctrine is of limited use to database companies that disseminate their products widely. To prevail in an action for trade secret violation, the database owner must prove that the database contains information that is kept secret and provides a valuable business advantage.\footnote{175} Courts have provided trade secret protection for customer lists that include addresses and phone numbers used by a company in a private, proprietary manner.\footnote{176} By contrast, mass-marketing of a database would indicate that the contents are not something that the company intends to keep secret. An unpublished district court decision bolsters this conclusion by finding that mass-market distribution of a product would likely forfeit any available trade secret protection.\footnote{177} Because secrecy is the linchpin of trade secret protection, this cause of action may not provide protection to a widely disseminated database.

\footnote{171}{Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1002 (1983) (citations omitted).}
\footnote{173}{Unif. Trade Secrets Act § 1(4), \textit{14} U.L.A. 438.}
\footnote{174}{See \textit{MAI Sys. Corp. v. Peak Computer, Inc.}, 991 F.2d 511 (9th Cir. 1993) (affirming summary judgment finding trade secrets in plaintiff's customer database); Surgidev Corp. v. Eye Tech., Inc., 828 F.2d 452, 455 (8th Cir. 1987) (concluding that ophthalmologist customer list generally known to others in the industry is entitled to trade secret status); American Paper & Packaging Prods., Inc. v. Kirgan, 183 Cal. App. 3d 1318, 1324 (Cal. Ct. App. 1986) (citing 28 A.L.R.3d § 7) (rejecting an argument that customer list is not protected as trade secret); Fred's Stores of Miss., Inc. v. M & H Drugs, Inc., 725 So. 2d 902, 911 (Miss. 1998) (concluding that a pharmacy master customer list is a trade secret where maintained confidentially).}
\footnote{176}{See, e.g., Forest Lab., Inc. v. Formulations, Inc., 299 F. Supp. 202 (E.D. Wis. 1969), aff'd in part rev'd in part, Forest Lab., Inc. v. Pillsbury Co., 452 F.2d 621 (7th Cir. 1971).}
\footnote{177}{See Stac Elec. v. Microsoft Corp., 38 F.3d 1222, No. 94-1349, 1994 WL 467221, at *1 (Fed. Cir. (Cal.) July 5, 1994).}
CONTRACT RIGHTS IN DATA AND DATABASES

In the absence of strong copyright and trade secret protections, database owners have turned to contract provisions to protect their interests. These have included mass-market licenses, i.e., "shrinkwrap" and "clickwrap" contracts as part of the data product, which purport to bind the ultimate users of database products.

Historically, courts limited the protection available to databases under contract theories, on the grounds that: (i) copyright law preempted enforcement of common law contract rights restricting access to factual information; and (ii) mass market and other "form" licenses were unenforceable as against public policy or lacked assent under contract law.178 Recent cases have reversed this trend, finding mass market licenses to be enforceable, and the proposed UCITA includes provisions that would enforce such licenses under appropriate circumstances.

ProCD v. Zeidenberg: Using "Shrinkwrap" License Provisions to Protect Databases

ProCD, Inc. created a CD-ROM mega-phonebook compilation of more than 3000 telephone directories at a cost of approximately $10 million over a two-year period.179 The packaging of each CD-ROM product included written notice that a license was enclosed in the database application, limiting its use to non-commercial purposes.180 The license restrictions also appeared on the computer screen each time the enduser executed the software, and were set out in the software user’s manual.181

A Wisconsin computer science student, Matthew Zeidenberg, purchased the ProCD database application and developed his own software to access the database. Zeidenberg then placed the resulting database on an Internet server and charged a fee for third parties to access it.

ProCD filed suit against Zeidenberg, alleging that he breached the terms of the shrinkwrap license when he placed the database on the server and provided access across the Internet.182 The Seventh Circuit held that ProCD’s shrinkwrap license was enforceable and prohibited Zeidenberg’s use of the database.183 The Seventh Circuit relied upon contract law and the Uniform Commercial Code in finding that “[a] vendor, as master of

178. Step-Saver Data Sys., Inc. v. Wyse Tech., 939 F.2d 91, 105-06 (3d Cir. 1991) (concluding that “box-top license agreement” printed on package containing computer software were not part of the parties’ agreement and therefore unenforceable); Vault Corp. v. Quaid Software Ltd., 847 F.2d 255, 270 (5th Cir. 1988) (holding that license agreement provisions prohibiting decompilation or disassembly were unenforceable).
179. ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1449 (7th Cir. 1996).
180. Id. at 1450.
181. Id.
182. Id.
183. Id. at 1449.
the offer, may invite acceptance by conduct, and may propose limitations on the kind of conduct that constitutes acceptance.”

In response to Zeidenberg’s argument that copyright law preempted the use of such a shrinkwrap license, the Seventh Circuit observed: “courts usually read preemption clauses to leave private contracts unaffected. . . . [j]ust as [the copyright preemption clause] does not itself interfere with private transactions in intellectual property, so it does not prevent states from respecting those transactions.” Moreover, “whether a particular license is generous or restrictive, a simple two-party contract is not ‘equivalent to any of the exclusive rights within the general scope of copyright’ and therefore may be enforced.”

ProCD has been widely regarded as an important and positive development in providing legal protection for databases. Under prior theories of copyright preemption and contract law, database companies had no viable means to establish protection of database assets. Under ProCD and a number of subsequent decisions, database companies should carefully draft and review contract provisions to maximize this protection. Companies, however, also should note that the terms of a proposed click-wrap agreement may be modified. Even where a party has included click-wrap terms, the provisions of a specific, negotiated license generally will be held to prevail.

184. Id. at 1452. The court, relying on several sections of the U.C.C. as adopted by Wisconsin, stated:

“A contract for sale of goods may be made in any manner sufficient to show agreement, including conduct by both parties which recognizes the existence of such a contract.” . . . A buyer accepts goods under § 2-606(1)(b) when, after an opportunity to inspect, he fails to make an effective rejection under § 2-602(1). ProGD extended an opportunity to reject if a buyer should find the license terms unsatisfactory; Zeidenberg inspected the package, tried out the software, learned of the license, and did not reject the goods.

185. Id. at 1454-55. The copyright preemption clause (§ 301(a)), in pertinent part, provides that “all legal or equitable rights that are equivalent to any of the exclusive rights within the general scope of copyright . . . are governed exclusively by this title.” 17 U.S.C. § 301(a) (1994).

186. ProCD, 86 F.3d at 1455.


188. See Morgan Labs, Inc. v. Micro Data Base Sys., Inc., 41 U.S.P.Q.2d (BNA) 1850 (N.D. Cal. 1997) (refusing to apply shrink wrap exclusive choice of forum clause where an independent license agreement had been negotiated by the parties). Authority is split as to whether terms received with a product become part of the parties’ agreement. At least one jurisdiction has already declined to follow the reasoning in Hill and ProCD, pointing out that a computer vendor generally is not, as the ProCD court found, master of his “offer,” because in the typical consumer transaction, it is the buyer who is the offeror. See Klocek v. Gateway, Inc., 104 F.
The Uniform Computer Information Transactions Act

The Uniform Computer Information Transactions Act (UCITA) is a model contract law statute proposed for enactment at the state level. UCITA applies to “computer information transactions,” including commercial agreements “to create, modify, transfer, or license computer information or informational rights in computer information.” While primarily intended to govern licensing of computer information already generated, this broad definition logically could be extended to sales and other non-licensing transactions. UCITA’s purpose is to clarify and harmonize the law governing computer information transactions to support commerce in cyberspace.

“Computer information” is “information in electronic form which is obtained from or through the use of a computer or which is in a form capable of being processed by a computer.” “Informational rights” are “all rights in information created under laws governing patents, copyrights, mask works, trade secrets, trademarks, publicity rights, or any other law that gives a person, independently of contract, a right to control or preclude another person’s use of or access to the information on the basis of the rights holder’s interest in the information.” UCITA’s concept of “informational rights” goes beyond traditional “intellectual property rights” and will offer potentially greater protection to database creators.

UCITA’s new rules of authentication and assent allow for easier on-line contract formation. UCITA expressly validates electronic contracts, including contracts between humans and electronic agents, and authorizes reliance on records that are kept solely in electronic form. Finally, consistent with ProCD and other similar cases, UCITA validates mass-market licenses for information products. The transactions do not need to be negotiated, so long as the end user has the opportunity to review the full terms of the license and affirmatively manifests assent.

Supp. 2d 1332, 1340-41 (D. Kan. 2000). Using only basic U.C.C. principles, the court reasoned that the offeree, Gateway, accepted the offer when it completed the transaction or, at the latest, when it shipped the goods. Thus, under U.C.C. § 2-207 (“battle of the forms”), the accompanying license is a mere proposal to add terms. Because the contract is not between merchants, such terms do not become part of the contract unless the offeror explicitly agrees to them. The failure to reject the goods is not an acceptance of the proposed terms, but rather a mere acknowledgment that the seller had delivered conforming goods. See id. at 1337-41.

191. Id. § 102(a)(10).
192. Id. § 102(a)(38).
193. Id. § 107.
194. Id. § 211.
195. UCITA substantially expands the concept of manifested assent, allowing contract formation without “a signature, specific language or any specific conduct.” Pamela Samuelson & Kurt Opsahl, How Tensions Between Intellectual Property Policy and UCITA Are Likely to be Resolved, 570 PLI/Pat 741, 752-53 (1999) (quoting in part Reporter’s Note to UCITA § 112).
To the extent that UCITA makes contractual relationships governing data transactions more certain to be enforceable, then in any jurisdiction which has enacted UCITA, parties to transactions in data would be well advised to specify as precisely as possible the rights and responsibilities of the parties in their agreements. Because the primary focus of UCITA is on transfers of information governed by license agreements, however, UCITA may provide few answers to questions about the right to control the same information that is collected by more than one party at the same time.

The primary focus of UCITA is on contractual relationships, but in the insecure environment of the Internet, not all parties collecting clickstream data may be in contractual relationships with each other. For example, netzero.com may be monitoring one of its subscriber’s Internet activity at the same time that activity is being monitored by a portal site such as Yahoo! that the subscriber has visited, by an advertiser displaying a banner ad to the subscriber, and by the business that paid for the banner ad to which the subscriber clicked through after seeing the ad. While netzero.com’s primary interest may be in profiling its subscriber’s behavior and selling information about that behavior in the aggregate to businesses to target its subscribers, netzero.com may be able to draw some interesting inferences about the business models of the portal, the business that paid for the banner ad on the portal site, and the advertising agency that booked the banner ad for that business. Netzero.com is not in a contractual relationship with any of those parties, however, just as netzero.com’s subscriber is not in a contractual relationship with the banner ad company. Should any of the parties collecting information about the subscriber implement a technological fix to block the data collection practices of the others, and a dispute arises as to the right to implement that fix, there may be no contractual relationship in place to resolve the dispute.196

Another open question that the provisions of UCITA do not clearly resolve is the enforceability of site licenses. Many web sites post privacy policies that govern their practices with regard to personal information they collect. It is unclear whether the act of posting these privacy policies creates a contractual relationship between the individual visiting the site and the party posting the privacy policy. UCITA includes a “two click” rule to indicate when it should be beyond question that a contract has been formed online,197 but sites that post privacy policies do not require

196. In some instances, advertisers and ad servers may themselves dispute ownership of customer data. See Bob Tedeschi, IBM May Get Stingy With Click Data from Ads, CHI. TRIB., Nov. 15, 1999, at 8; Kathryn Kranhold & Michael Moss, Keep Away From My Cookies, More Marketers Say, WALL ST. J., Mar. 20, 2000, at B1.

197. The February 2000 draft of UCITA § 112(d) provides:

Conduct or operations manifesting assent may be proved in any manner, including a showing that a person or an electronic agent obtained or used the information or in-
visitors to click once, let alone twice, to acknowledge awareness of the provisions of the policy. The FTC has pursued web site operators who failed to comply with the terms of their posted privacy policies based on unfair and deceptive trade practices theories, not breach of contract theories.\textsuperscript{198} Claiming that a privacy policy creates a contractual relationship between the individual whose information has been collected subject to it and the web site operator may seem to be a good way to strengthen individual privacy rights on the web, but would then subject individuals to liability under the now ubiquitous "site license."\textsuperscript{199}

\textbf{SUI GENERIS RIGHTS IN DATABASES}

In recent years the U.S. Congress has considered legislation that would create independent, sui generis rights in database assets, comparable to those established by the EU Database Directive.\textsuperscript{200} These efforts have been supported by two basic policy arguments.

First, there is a basic sense of unfairness in the holding of \textit{Feist} and its progeny. Many argue that it is inequitable that third parties may copy and use freely databases which require substantial resources to create.\textsuperscript{201} Moreover, the incentives to create such databases are reduced if there is no significant competitive advantage available to the creator.

Second, in the absence of comparable database protection in the United States, databases owned by U.S. companies will not be protected under European law. Accordingly, many U.S. companies have strongly urged Congress to pass database protection legislation.

Several bills have been considered in Congress since 1996. The Collections of Information Antipiracy Act, H.R. 354, was introduced on January 19, 1999.\textsuperscript{202} H.R. 354 would, in essence, enact the "sweat of the brow" theory of copyright protection rejected in \textit{Feist},\textsuperscript{203} to protect electronic formational rights and that a procedure existed by which a person or an electronic agent must have engaged in the conduct or operations in order to do so. Proof of compliance with subsection (a)(2) is sufficient if there is conduct that assents and subsequent conduct that reaffirms assent by electronic means.


\textsuperscript{199} See generally, Ticketmaster Corp. v. Tickets.com, Inc., 54 U.S.P.Q.2d (BNA) 1344 (C.D. Cal. 2000) (granting summary judgement to the defendant Tickets.com on Ticketmaster's breach of contract claim based on a site license with leave to amend pleadings if Ticketmaster could show Tickets.com's knowledge of the terms of the site license plus facts showing implied agreement to them).

\textsuperscript{200} See EU Database Protection Directive, infra, note 97.

\textsuperscript{201} Warren Publ'g, Inc. v. Microdos Data Corp., 115 F.3d 1509 (11th Cir. 1997).


databases that were created with substantial investment, and focus on preventing commercial harm and misuse by third party competitors. Analogous to the EU Database Protection Directive, this comprehensive approach includes provisions to protect the user community, including fair and transformative use provisions and exemptions for librarians and educators. In addition, the bill includes specific protections for Internet Service Providers. A number of interests, including the U.S. Department of Justice, have questioned the constitutionality of this approach, to the extent that it provides protection for factual materials. An alternative, less sweeping approach has been proposed that would essentially enact common law theories of misappropriation. It is unclear whether Congress will act and, if so, which approach it would take in considering database protection legislation. It is likely, however, that the issue will become more visible in future legislative sessions.

**PRIVACY RIGHTS OF INDIVIDUALS**

*Overview.* Under U.S. law, privacy rights in general and information privacy rights in particular are a patchwork of different statutes and common law doctrines that provide some protection for individuals in some contexts. The Restatement (Second) of Torts includes four invasion of privacy torts: intrusion upon a person’s seclusion or solitude; public disclosure of embarrassing private facts about someone; publicity which places someone in a false light in the public eye; and appropriation, for the use or benefit of the wrongdoer, of someone’s name or likeness. Not all these rights are recognized in all jurisdictions however. The U.S. Supreme Court recognized the right of privacy as a constitutional right in Griswold v. Connecticut, but that right only protected the citizen against intrusions by the government, not by other private parties.

*Historical Development.* Beginning in the 1970s, as the use of computers grew, awareness grew of the potential social impact computers and databases might have, and a number of privacy laws were enacted in the United States. If individuals have rights to prevent personal information from being accessed, collected, analyzed, or transferred under one of these privacy laws, then businesses that violate those rights in their data collection practices may face civil or criminal liability.

204. See EU Database Protection Directive, infra, note 97.
208. Restatement (Second) of Torts § 652A(2) (1977).
209. 381 U.S. 479 (1965).
For example, in 1970, Congress passed the Fair Credit Reporting Act,\textsuperscript{210} regulating the collection and use of personal information by consumer credit reporting agencies. In 1974, Congress passed the Privacy Act,\textsuperscript{211} which regulated the collection and use of personal information by the government. The Family Educational Rights and Privacy Act of 1974\textsuperscript{212} permits a student or the student’s parents to access educational records, and prohibits educational institutions receiving federal funding from using or disclosing the contents of a student’s educational records without the student’s consent, or for minor students, a parent’s consent. Congress passed the Right to Financial Privacy Act of 1978\textsuperscript{213} following a Supreme Court decision that held that the Fourth Amendment did not apply to government efforts to obtain individual financial records,\textsuperscript{214} and it established notice and access procedures for access to personal financial information by government agencies. The Counterfeit Access Device and Computer Fraud and Abuse Act of 1984\textsuperscript{215} made it a crime to access a “federal interest computer” and obtain information, financial institution and consumer credit reporting agency files, without authorization. The scope of this law has repeatedly expanded as the law has been updated since 1984, most recently when Congress passed the National Information Infrastructure Protection Act of 1996.\textsuperscript{216} The Cable Communications Policy Act\textsuperscript{217} prohibits a cable television company from collecting or disclosing information about its subscribers without their consent. The Video Privacy Protection Act\textsuperscript{218} prohibits video rental stores from disclosing their customers’ names and addresses, and the titles of the videos they have rented. The Identity Theft and Assumption Deterrence Act of 1998\textsuperscript{219} made it a crime to transfer or use a means of identifying another person with the intent to engage in unlawful activity.

Electronic Communications. The Electronic Communications Privacy Act of 1986 (ECPA)\textsuperscript{220} protects all forms of electronic communications from unlawful interception and disclosure, and unlawful access to stored communications. “It is not always obvious which ECPA provisions cover communications, such as electronic mail, that are both transmitted and stored.”\textsuperscript{221} The prohibition from intentionally accessing a stored electronic

\textsuperscript{211} 5 U.S.C. § 552a.
\textsuperscript{212} 20 U.S.C. § 1232g.
\textsuperscript{213} 12 U.S.C. §§ 3401-3422.
\textsuperscript{215} 18 U.S.C. § 1030.
\textsuperscript{216} 18 U.S.C. § 1030 (Supp. IV 1998).
\textsuperscript{218} 18 U.S.C. § 2710.
\textsuperscript{221} Michael Hatcher, Jay McDannell & Stacy Ostfeld, Computer Crimes, 36 AM. CRIM. L. REV. 397, 415 (1999). See also id. at 414 n.131 (citing United States v. Reyes, 922 F.
communication without authorization does not apply to an employer who monitors employee communications using an employer-provided system in the ordinary course of business, however. In addition, stored messages may be accessed and reviewed by the operator of an electronic communication service, although they may not disclose such stored messages.

**Financial Information.** On November 12, 1999, the Gramm-Leach-Bliley Act became law. Title V of the Act ("Disclosure of Nonpublic Personal Information") protects the financial privacy of consumers by (i) limiting the instances in which a financial institution may disclose nonpublic personal information about a consumer to nonaffiliated third parties; and (ii) requiring a financial institution to disclose to all of its customers the institution's privacy policies and practices.

Financial Information. On November 12, 1999, the Gramm-Leach-Bliley Act became law. Title V of the Act ("Disclosure of Nonpublic Personal Information") protects the financial privacy of consumers by (i) limiting the instances in which a financial institution may disclose nonpublic personal information about a consumer to nonaffiliated third parties; and (ii) requiring a financial institution to disclose to all of its customers the institution's privacy policies and practices.

On February 24, 2000, the FTC released draft regulations under the Gramm-Leach-Bliley Act that would require financial institutions to provide notice of their privacy practices to customers and would restrict the ability of these institutions to disclose personal information about consumers to nonaffiliated third parties. Because "financial institutions" are defined extremely broadly under the proposed regulations, many categories of businesses—particularly those that are engaged in the extension of credit—may be surprised to find themselves covered by these notice, opt-out, and disclosure requirements.

Covered financial institutions are required under the proposed rules to provide "clear and conspicuous" notice of their privacy practices to (i) any "consumer" whose nonpublic information the institution wants to disclose to a nonaffiliated third party; and (ii) anyone who will become a "customer" (prior to the time they actually become a customer). Notices can be provided in electronic form (as opposed to hard copy form) only if the consumer or customer agrees.

Supp. 818, 836-37 (S.D.N.Y. 1996) (concluding that pressing a button on a pager to discover callers' identities was not an interception of a transmission but an access of stored communications); Steve Jackson Games, Inc. v. U. S. Secret Service, 36 F.3d 457, 458 (5th Cir. 1994) (holding that seizing a computer to recover stored email messages was not interception of a transmission but an access of stored communications). Compare United States v. Smith, 155 F.3d 1051, 1063 (9th Cir. 1998) (concluding that a voicemail message accessed without authorization from a corporate voicemail system, recorded onto an audiotape and turned over to law enforcement was an interception of a transmission not an access of a stored communications).

226. *Id.* at 11,176.
227. *Id.* at 11,175-76.
228. *Id.* at 11,180.
The Emerging Law of Commercial Transactions in Electronic Customer Data 253

Notices to be required by the proposed rules are to include, among other things:

- the categories of nonpublic information about consumers that are collected;
- the categories of nonpublic personal information about current and former consumers that are disclosed;
- the categories of affiliates and nonaffiliated third parties to whom nonpublic personal information about consumers is disclosed;
- explanation of the consumer’s right to opt out of disclosure, including the methods by which the consumer may exercise that right; and;
- the company’s policies and practices with respect to protecting the confidentiality, security, and integrity of nonpublic personal information.229

FTC’s proposed rules do not preempt state law unless the state law is “inconsistent” with the rules.230 If a state enacts a statute or regulation that affords consumers greater protection than the proposed rules, it will not be considered inconsistent with the rules and will not be preempted.231

Health Information. Federal law currently does not govern the use of private health records. About half the states have comprehensive medical records confidentiality laws. The Health Insurance Portability and Accountability Act of 1996 included a provision requiring Congress to enact a national medical information confidentiality law by August 21, 1999.232 In mid-2000, the Department of Health and Human Services was finalizing new regulations that would create the first comprehensive medical record privacy rights under U.S. law after Congress failed to enact legislation on medical record privacy under its own self imposed deadline contained in the Health Insurance Portability and Accountability Act of 1996.233 Industry groups have attacked these medical record privacy regulations as being too restrictive, but privacy advocates have also criticized the regulations as inadequate.234

Children’s Information. The Children’s Online Privacy Protection Act of 1998 (COPPA),235 governs online collection and use of personal information from children under age thirteen. The FTC issued regulations

229. Id. at 11,181-82.
231. Id.
implementing COPPA in April 2000. Although COPPA is aimed primarily at web sites designed for children, any web site that contains a children’s “area” is subject to the full force of the rules. Web site operators that knowingly collect any personal information from a child in any context must comply with COPPA with respect to that information. As a practical matter, all companies that collect registration information that includes date of birth may be required to meet COPPA’s requirements, because they will be unable to prevent users from inputting birth dates indicating ages below thirteen.

State Privacy Law Initiatives. During the last few years, states have enacted legislation in a variety of contexts that create privacy rights or impose conditions on the use of personal information. For example, states have passed laws protecting personal information related to: cable television viewing habits, computer access, personal information in the hands of merchants, consumer lists, library records, videotape rental records, and tax information. At the time this article went to press there were more than 300 on-line privacy bills, aimed at the use of personal data, pending in state legislatures.

To date, states have not undertaken widespread enforcement of these requirements; however, in a few highly publicized recent actions state At-

---

237. COPPA has five principal compliance requirements. It requires the posting of: (i) A specific children’s privacy policy, with a “prominent” link from the site’s home page; (ii) The name, address, telephone number, and e-mail address of the employee or office responsible for privacy issues at the web site’s operator’s office; (iii) An identification of the type of information collected (e.g., e-mail address, home address, etc.); (iv) A description of all uses of the information, whether and why the site stores children’s personal information, and the security measures used to protect such information; and (v) If there is (or will be) disclosure of children’s personally identifiable information to third parties, including affiliates. If so, the policy must: identify such third parties by type (e.g., retailers); describe the use third parties will make of the information (e.g., marketing, targeted advertising, etc.); identify any assurances of confidentiality obtained from such third parties (or lack thereof); notify parents that they may refuse to permit such third party disclosure without losing any opportunities for their child to interact with the site; and confirm that children’s participation in any game or activity will not be conditioned on the provision of more personal information than is necessary to participate. Id. at § 312.4(b).
238. FLA. STAT. ANN. § 364.24 (West 1998).
239. OHIO REV. CODE ANN. §§ 2913.01-.04 (Anderson 1996).
244. N.C. GEN. STAT. § 75-28 (1999).
245. Marcia Stepanek, None of Your Business, BUS. Wk., June 26, 2000, at 78. A February, 2000 estimate places the number of pending state and federal bills related to privacy, both on- and off-line, at 500, and further estimated that the total would reach approximately 2,000 by the end of the year. Kelly Hearn, Wild Web hears hoofbeats of lawmakers, CHRISTIAN SCI. MONITOR, Feb. 14, 2000, at 20.
The Emerging Law of Commercial Transactions in Electronic Customer Data 255
torneys General have filed suit against major financial institutions and Internet advertising companies based on alleged unlawful uses of consumer data.246

While the number of enforcement actions remains low, states have recently indicated that pursuing privacy violations will soon be a top priority. In March, the National Association of Attorneys General (NAAG) voted to make computer crime and consumer privacy issues top priorities.247 Going a step further, NAAG’s 2000 summer meeting was the first in its history to devote all public sessions to privacy issues.248

Self Regulation and FTC Enforcement. Internet and other data-intensive companies have attempted to avoid regulation through adoption of self-regulatory privacy policies, consistent with and monitored by third party organizations such as TrustE. Some have viewed self regulation as insufficient and designed more for public relations purposes than protecting consumer data.249

The FTC has taken action in some cases to add teeth to self-regulatory efforts. For example, in late 1998 FTC filed an action against GeoCities, alleging violations of GeoCities’ stated privacy policies in its use and distribution of customer data.250 The case was resolved by a consent decree pursuant to which GeoCities was required to implement various corrective measures and otherwise ensure compliance with its original stated policies.251 In June 2000, FTC filed a similar action against Toysmart.com, seeking to prohibit a bankruptcy sale of Toysmart’s customer data that would have violated Toysmart’s posted privacy policy.252


247. Id.

248. Id.


251. Id.

It is also reasonable to expect that consumer lawsuits challenging data practices will, in relevant cases, be based on alleged violations of corporate policies. While self regulation may not have a direct enforcement mechanism, the prospect of FTC actions or class action litigation should lead companies to carefully comply with their published policies.

**Online Privacy Legislation.** On May 22, 2000, the FTC issued a report (Report) describing its comprehensive search of online privacy disclosures and practices.\(^{253}\) By a 3-2 vote of the Commissioners, the FTC concluded in the Report that industry efforts at self-regulation have been insufficient.\(^{254}\) Accordingly, the Report recommended legislation that would establish required privacy measures including notice, choice, access, and security, and also would give an implementing agency authority to promulgate and enforce rules to enforce more detailed standards.\(^{255}\) In mid-2000, Congress was considering a broad online privacy bill similar to that recommended by the FTC.\(^{256}\) As of this writing, however, no such legislation has been enacted.

**DATABASE LICENSING RIGHTS IN BANKRUPTCY**

As illustrated by the case studies of Boo.com and Toysmart.com, bankruptcy scenarios can create significant problems and opportunities for parties to database licenses, their creditors, and third parties. Unfortunately, the Bankruptcy Code provisions that govern rights in data and intellectual property create significant ambiguities. The Bankruptcy Code historically focused on real property, physical assets, and contractual business relationships. New economy licensed assets such as software code, databases, content, and other intellectual property and intangibles, often are not clearly addressed under the Bankruptcy Code.

The filing of a bankruptcy petition has a number of important effects. For the debtor, bankruptcy filing can allow immediate suspension of ongoing contractual obligations and require the sale of assets to satisfy outstanding obligations to creditors. For companies that do business with the debtor, filing of a bankruptcy petition can result in termination or assignment of licensed assets to third parties, discontinuation of fee payments, and the potential for material breaches of license terms such as confidentiality and data security. Creditors will want to maximize the proceeds from the sale of the debtor’s assets, and third parties may use bankruptcy as an opportunity to acquire assets, or the entire company, at a substantial discount.


\(^{254}\) Id. at ii.

\(^{255}\) Id. at 36-38.

\(^{256}\) Consumer Privacy Protection Act, S. 2606, 106th Cong. (2000).
Effects of Bankruptcy on Licensees. After the filing of a petition for bankruptcy, section 365 of the Bankruptcy Code authorizes the Trustee to stop performance to third parties immediately if that would benefit the estate. This can have important adverse effects on parties that had ongoing licensing arrangements with companies going into bankruptcy. In Lubrizol Enterprises, Inc. v. Richmond Metal Finishers, Inc.,257 for example, Richmond Metal Finishers had granted Lubrizol a non-exclusive license to use a proprietary metal coating process. Richmond filed a Chapter 11 petition, and its trustee sought to reject the license in order to increase the value that would be obtained by selling or licensing the technology to a third party in the bankruptcy proceeding. The court upheld the Trustee’s action, holding that the effects on the licensee were not relevant to the decision.258

The Lubrizol holding created alarming risks for the increasing number of businesses that relied on licensed technology and intellectual property. Every license, no matter how vital to the licensee’s business, would be subject to potential termination merely upon the filing of a bankruptcy petition by the licensor. To address this problem, Congress passed the Intellectual Property Licenses in Bankruptcy Act (section 365(n)).259

Section 365(n) is intended to balance the rights of debtors, licensees, and third parties. It provides that when a debtor-licensor rejects a license in intellectual property, the licensee may elect either to (i) treat the license as terminated, if the rejection would have constituted a breach under non-bankruptcy laws;260 or (ii) retain the licensee’s rights under the license as they existed as of the time of filing of the bankruptcy petition, provided that the licensee continue to make payments due under the license.261 If the rights are retained, the licensee also may renew the license at its option either under the terms of the contract or otherwise under applicable non-bankruptcy law.262

The definition of “intellectual property” under the Bankruptcy Code is narrower than in nonbankruptcy law. It includes trade secrets, patents, and copyrighted materials, but does not extend to trademarks.263 Application of this definition to new economy assets results in uncertainties. For example, the courts are split on whether Internet domain names are personal

258. Lubrizol, 756 F.2d at 1048.
259. 11 U.S.C. § 365(n) (1994). For analysis of whether the kinds of “clickstream data” and other customer profiles developed by on-line retailers will qualify as intellectual property, see supra notes 134-77 and accompanying text. Note that at this point the issue is far from settled. For purposes of this part, it will be assumed that such data will be afforded applicable protection in bankruptcy.
260. Id. § 365(n)(1)(A).
261. Id. § 365(n)(1)(B).
262. Id. § 365(n)(1)(B)(i), (ii).
263. Id. § 101(35A).
property, trademark rights, or other intellectual property. Database assets will need to be analyzed under principles of trade secret and copyright law to determine whether they constitute "intellectual property" for purposes of section 365(n). Other assets that may or may not constitute intellectual property under the Code include content licenses, web linking licenses, strategic alliance and co-branding agreements, and web hosting licenses.

Effects of Bankruptcy on Licensors. Parties that license databases or access to customer data through alliance agreements also may be affected where the licensee files for bankruptcy. In those cases, the licensor may have a strong interest in prohibiting sale or transfer of the database to a third party for the benefit of the estate.

Section 365(c) of the Bankruptcy Code provides that a trustee may assume or assign certain executory contracts of the debtor. As a practical matter, it may be necessary for the trustee to assume key contracts to continue operations, such as, for example, an Internet businesses web hosting agreement. Alternatively, a trustee might seek to assign valuable contracts to third parties in exchange for cash payments into the estate.

Section 365(c)(1)(A) of the Bankruptcy Code, however, restricts the ability of a trustee to assign executory contracts where such assignment would be prohibited under non-bankruptcy law. As a general matter, common law principles prohibit assignment of personal services contracts. Because intellectual property rights historically have been viewed as being in the nature of personal property, the section 365(c) restriction on assignment may extend to a number of different types of intangible assets. For example, in *Everex Systems, Inc. v. Cadtrak Corp. (In re CFLC, Inc.)*, the Ninth Circuit prohibited a debtor from assigning its rights under a non-exclusive patent license. This principle may be important to licensors who seek to prevent transfer of intellectual property to third parties who may be competitors or potential customers in their own right.


266. 11 U.S.C. § 101(35A) defines "intellectual property" as to include "trade secret" "to the extent protected by applicable nonbankruptcy law." *Id.*

267. *See id.*, § 365(c) (setting out certain instances where a trustee may not assume or assign executory contracts of the debtor).


269. 89 E3d 673 (9th Cir. 1996).

Some courts have gone further, reading section 365(c)(1)(A) also to prohibit the assumption of an executory contract where the assignment of that contract would be prohibited under the common law. In re Catapult Entertainment, Inc.,271 for example, held that a debtor could not assume rights to continue use of a non-exclusive patent where the licensor objected.272 These cases have very important implications for new economy companies that rely on licensed intellectual property. If that intellectual property may not be assumed, the threat of bankruptcy may alter the relative leverage of the debtor, creditor, and licensors.

DATA AND DATABASES IN THE EUROPEAN UNION

Within the European Union in recent years, there has been strong legislation passed both to protect individual privacy rights in data and to protect proprietary interests in databases. The EU made an effort at the 1996 diplomatic conference convened by the World Intellectual Property Organization (WIPO)273 to have a multilateral treaty drafted that would have propagated the EU model of database protection around the world. Although this effort was unsuccessful in 1996, it is likely that WIPO will return to the issue in the future.274

FAIR INFORMATION PRACTICE PRINCIPLES AND THE OECD PRIVACY GUIDELINES

In the United States, the idea of fair information practice principles was first systematically articulated by the Department of Health, Education and Welfare in a 1973 report entitled Records, Computers and the Rights of Citizens (HEW Report).275 The “fair information practice principles” first evolved in the context of the rights of individuals as against the government, and have become widely adopted among U.S. governmental agencies since they were developed. In addition to the HEW Report, the major U.S. government reports setting forth the core fair information practice principles are: The Privacy Protection Study Commission, Personal

271. 165 F.3d 747 (9th Cir. 1999).
272. Id. at 754-55. See also City of Jamestown v. James Cable Partners (In re James Cable Partners), 27 F.3d 534 (11th Cir. 1994); In re West Elec. Inc., 852 F.2d 79 (3d Cir 1988); Breeden v. Catron (In re Catron), 158 B.R. 629 (E.D. Va. 1993), aff'd, 25 F.3d 1038 (4th Cir. 1994).
273. The World Intellectual Property Organization is a specialized agency of the United Nations charged with oversight of multilateral intellectual property law treaties.
Privacy in an Information Society; In 1978, Organization for Economic Cooperation and Development (OECD) convened a group of experts to study developments in different countries and to produce guidelines that might form a consensus position on privacy issues, facilitating harmonization of national laws in this area. In 1980, the OECD published its Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD Guidelines). The OECD Guidelines included principles providing that individuals should be notified when personal data is being collected; that the amount of personal data collected and the uses to which it may be put should be limited; that data collected for one purpose should not later used for another; that personal data should be disclosed without the consent of the subject; that it should be kept secure; that individuals should have a means of learning who is collecting data about them; that individuals should be allowed to access data that has been collected about them and to have corrections made if the data is not accurate; and that there should be some means of holding those who collect personal data accountable for compliance with these principles.

The OECD Guidelines may be difficult to interpret and apply to more contemporary data collection practices for several reasons. They refer to a “data controller,” but organizations that collect from a variety of sources in open network environments may not have any single person or even a single group of people who are in control of data collection practices. There is no de minimis threshold on what constitutes a data record, which creates administrative problems of staggering proportions in trying to meet notice, consent and access requirements with regard to data subjects. Given the volume of information now being collected about individ-

281. See id. arts. 7-14.
282. See id. art. 1(a)
uals and the distributed manner in which it may be stored, the security problems associated with granting individuals the right to access data and make corrections to it are also very significant, especially given that there is no generally agreed upon system for checking the identity of the party requesting access to a data record.

Some more recent statements of fair information practice principles add the idea of “chain of trust” which requires that whenever information is used or transferred, it should always enjoy the same level of protection. If the chain of trust notion were added to fair information practices, a party in control of personal information would be under an obligation not to permit its onward transfer without confirming that the data after transfer would be subject to the same controls and limitations as it was before the transfer. The chain of trust idea helps to clarify the rights and obligations of a party wishing to make an onward transfer of data, but does not necessarily address the rights and obligations of a party receiving an onward transfer of data. If the notion of chain of trust becomes generally recognized as a fair information principle, however, it could create a “due diligence” obligation on the part of a party receiving an onward transfer of data to ensure that it had been informed of all relevant limitations that would apply to its own use of the data.

THE EU DATA PROTECTION DIRECTIVE

Overview. Countries in the European Union (EU) have taken a fundamentally different approach to consumer data rights than the United States, imposing regulatory requirements and prohibitions on many aspects of use, collection, and distribution of customer data. EU data protection laws are consistent with the fair information practice principles developed in the United States with regard to government collections of data, and with the OECD Guidelines. Because of differences among the EU member states themselves, the EU decided in the early 1990s to “harmonize” national data protection laws and to prevent transfer of customer data to countries lacking “adequate” levels of data protection.

This effort resulted in the EU Data Protection Directive (Directive), adopted in 1995. The Directive was to be implemented by the member states no later than October 1998, but as of January 2000, only half of the member states had enacted the Directive into national law. Nevertheless, all are on the way to adopting new laws, and their courts and data pro-


284. EU Database Protection Directive, supra note 97.
tection authorities are already interpreting existing laws in light of the Directive.

Processing Requirements and Prohibitions. The Directive covers the “processing” (defined to include anything that can be done with data, from collection to deletion285) of “personal data” (any information identified or identifiable to a natural person286), by automated or manual means, subject to a few narrow exclusions. Processing for purely personal or household purposes is excluded, as are government activities (such as the police and the military) that are outside the scope of the EU Treaty itself. In effect, virtually all processing of personal data for commercial purposes is to be covered by national laws implementing the Directive.

Under Article 6 of the Directive, “data controllers,” defined as persons or entities that determine the purposes and means of processing, alone or jointly with others,287 are responsible for meeting substantive “data quality” requirements and otherwise protecting covered data. Processing is only permitted where the individual “data subject” has given “unambiguous” consent, or where the processing is necessary for (i) the performance of a contract with the data subject; (ii) in order to enter into a contract with the data subject; or (iii) to comply with a legal obligation.288 Processing may also be allowed under a general balancing test, where the individual’s privacy interests do not override the “legitimate interests” of the controller,289 but this is a basis that has not been clearly defined to date. Processing of “special categories” of sensitive data (race, religion, political opinion, trade union membership, health, or sex life) generally requires specific consent.290 The Directive requires that data subjects have rights of access to the covered data291 and to object to direct marketing.292

Data Exporting. EU member states are obliged to provide that data is exported only to third countries that ensure “an adequate level of protection,” as determined by the Commission under specified procedures. Most non-EU countries, including the United States, have failed to demonstrate protections deemed to be “adequate” by the EU. Accordingly, the United States and EU have developed “safe harbor” provisions that allow the transfer of data to qualifying entities in the United States.293

Contract Protections. A number of EU member states permit data flows from individual companies (or among business networks such as travel

285. See id. art. 2(b).
286. Id. art. 2(a).
287. Id. art. 2(d).
288. Id. art. 7(b), (c).
289. Id. art. 7(f).
290. See EU Database Protection Directive, supra note 97, art. 8.
291. See id. art. 12.
292. See id. art. 14(b).
reservation systems) based on contractual guarantees, which in some countries must be approved in advance by the data protection authority between the data “exporting” party in Europe and the data “importing” party in the United States or some other third country. If the importing party fails to comply with its obligations under the agreement, the data protection authority may take action against the exporting party in Europe to suspend transfers. A number of “model” contracts have been developed to govern transborder data flows that would be effective under article 26 of the Directive, although none have formally been approved by the Commission to date.

Enforcement. The Directive stipulates that member states must give independent data protection authorities investigative powers and the authority to order the blocking of data processing or data transfers. The member states also must provide for judicial remedies, including injunctive relief, compensatory damages, and “suitable” sanctions to ensure compliance. The Directive establishes EU-level procedures, including procedures for adopting additional measures that are binding on all member states as a treaty obligation.

The Directive has major implications for U.S. companies doing business through the Internet or using customer data that has or may have originated in the EU. EU member states may assert jurisdiction to prohibit certain uses of exported data, and it also is conceivable that EU data subjects could seek relief in U.S. courts for violations of data protection agreements or safe harbor provisions by U.S. companies.

**THE EU DATABASE DIRECTIVE**

On January 1, 1998, the EU Directive on the Legal Protection of Databases (Database Directive) became effective. The Database Directive is intended primarily to stimulate investment in databases in EU member states and to increase the European share of the database market. The Database Directive defines a database as “a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means.” The Database Directive provides protection, equivalent to copyright in the United States, based on “substantial investment” by the creator in obtaining, verifying or presenting the database’s contents, but only where selection or arrangement of the database’s contents constitute “the author’s own intellectual creation.”

294. EU Database Protection Directive, supra note 97, art. 28.
295. Id. arts. 22, 24.
297. See id. recitals 11 & 12.
298. Id. art. 1(2).
299. See id. recital 15 & art. 3(1).
The rights conferred by the Database Directive may be transferred, assigned, or granted by the holder under contractual license. The Directive states, however, that the new rights may not prejudice other rights in the contents of the database. In particular, rights under the Database Directive are made subordinate to the rights conferred by the Data Protection Directive.

Qualifying databases are protected from the time of completion for a period of 15 years from the first of January following the date of completion, with additional 15-year periods when the creator makes any "substantial change" or accumulates a series of successive changes that constitute a "substantial new investment" in the database.

The Database Directive allows the generator “to prevent extraction and/or re-utilization of the whole or of a substantial part” of the database contents and to prevent repeated and systematic extraction or re-utilization which unreasonably prejudices the maker’s “legitimate interests.” It also creates exceptions for extraction or re-utilization that constitutes “public lending” or extracting and/or re-utilizing insubstantial parts of the contents of the database. The lawful user is authorized to use the database for any purpose that does not conflict with normal exploitation of the database or unreasonably prejudices the legitimate interest of the maker.

The Database Directive applies to persons in the EU. The Directive also provides protection for persons located in countries outside of the EU that have enacted “comparable” database protections. As noted above, the U.S. Congress has considered legislation that would enact sui generis data-

300. Id. art. 7(3).
301. See id. art. 7(4).
302. The Database Directive provides:

Whereas the objective of this Directive, which is to afford an appropriate and uniform level of protection of databases as a means to secure the remuneration of the maker of the database, is different from the aim of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, which is to guarantee free circulation of personal data on the basis of harmonized rules designed to protect fundamental rights, notably the right to privacy which is recognized in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms; whereas the provisions of this Directive are without prejudice to data protection legislation.

Database Directive, supra note 296, recital 48 (citation omitted).
303. See id. art. 10(1).
304. See id. art. 10(3).
305. See id. art. 7(1).
306. See id. art. 7(5).
307. See id. art. 8(1).
308. See id. art. 8(2).
base protection rights comparable to those under the EU Database Directive, but to date that legislation has not become law.

COMMERCIAL LAW AND COMMERCIAL TRANSACTIONS IN DATA

MANAGING OPEN NETWORK DATA COLLECTION PRACTICES BY CONTRACT

In open network environments, a party that wishes to limit the rights of other parties to collect data that can be accessed over the network has several choices: (i) make it impossible as a practical matter to access the data, which might require removing it from the Internet; (ii) enter into a formal contractual relationship with other parties who have a motive for collecting the data and the ability to do so, although not all such parties may be willing to enter into a contractual relationship; or (iii) put up a "terms of access" notice and argue that a contract that includes the terms of access notice has been formed by anyone who does in fact access the data. The enforceability of "legal notices" on web sites that try to impose license terms on anyone accessing the web site is unclear. Intellectual property law may not protect data that is accessible over a public network such as the Internet. A "terms of access" notice that is modeled after such "legal notices" site licenses is not so clearly a license, because the underlying right of the party posting the notice to exclude third parties is unclear. A contract term limiting a party's right to collect data that it is technologically feasible for it to collect may not have much practical effect unless it is supported by the design of the information systems of the parties, or if effective mechanisms exist for detecting and sanctioning non-compliance. If a party by contract waives the right to collect data to which it has ready access, and with regard to which it has an economic interest, the party receiving the waiver may want to consider auditing or having a third party audit the information system of the other party to be certain the other party does not in fact plan to collect the data. Finding a technological mechanism to monitor and possibly block access to data might be preferable to relying on the undertaking of a party to implement

309. See, e.g., Ticketmaster Corp. v. Tickets.com, Inc., 54 U.S.P.Q.2d (BNA) 1344 (C.D. Cal. 2000) (granting summary judgment to the defendant Tickets.com on Ticketmaster's breach of contract claim based on a site license with leave to amend pleadings if Ticketmaster could show Tickets.com's knowledge of the terms of the site license plus facts showing implied agreement to them).

policies and procedures to ensure that the behavior of all persons within its organization conforms with its contractual obligations. The open architecture of the Internet, however, may make it difficult or impossible to devise technologies to backstop such contractual undertakings.

The right to access certain types of data in the future may be governed by a contractual provision, but that may not adequately protect the interests of the party counting on a future flow of data. A similar problem would arise for a party counting on receiving a future flow of data if the party promising to transfer it files for bankruptcy.311

If a contract term grants a party access to data, and the accessing party develops profiling algorithms based on the assumption that it will have access to that data in the future, then the party is at risk of losing the value of that profiling algorithm if it loses access to that data in the future. Dot-com companies may be particularly vulnerable in this regard if their only interaction with their customers is through their web site. If their ability to convert visitors into customers and to continue to appeal to customers is a result of using an interface that has been improved through the use of profiling technologies, then an erosion in the quality of their profiling may translate into a less engaging interface and lower revenues.

RIGHTS OF TRANSFEREES OF DATA VERSUS RIGHTS OF DATA SUBJECTS

Two important foundations of modern commercial law are the doctrine of good faith purchase312 and the alienability of property.313 As databases become an increasingly important form of commercial property, it will be necessary to determine whether these basic commercial principles apply to databases. If they do not, acquiring title to database assets will be more problematic and markets for database assets may be less liquid. In light of the dignitary values associated with personal information, that may be the unavoidable outcome of harmonizing the concerns animating data protection laws and those animating commercial law.

If the doctrine of good faith purchase applies to databases, then a transferee of a database who receives the asset in exchange for value, in good faith and without any notice that the transferor may be subject to claims or defenses, such as a breach of the privacy rights of the individuals whose

311. See supra text accompanying notes 295-296.
313. See, for example, pre-revision U.C.C. § 9-311 on alienability of debtor’s rights, which provides that notwithstanding any agreement to the contrary between the debtor and the secured party, the debtor’s rights in the collateral may nevertheless be transferred to a third party. Such a transfer would put the debtor in breach of the security agreement, but could not prevent the third party from acquiring an interest in the collateral.
data is contained in the database, would take the asset free of those claims or defenses. The doctrine of good faith purchase could only be applied to database transactions as a matter of common law, however, as there is no statutory basis for such a rule today. If copyright law applies rather than commercial law to database transactions, there is nothing really equivalent to the concept of good faith transferee and any subsequent transferee would be liable for infringement, even if unintentional. Any judicial development of law applicable to transfers of data that breach privacy rights that reasons by analogy from copyright law would not create a doctrine of good faith purchase. UCITA shows its origins in software licensing law, which developed in large part as a type of copyright licensing law, and grants the licensor a near-absolute right to forbid subsequent transfers. If a court reasons by analogy from UCITA, it would similarly not create a good faith purchase doctrine.

If the “chain of trust” concept proposed in draft HHS medical records under the Health Insurance Portability and Accountability Act were incorporated into other U.S. privacy laws, then the transferee would not be able to avoid claims or defenses based on a claim of good faith purchase. The concept of “chain of trust” might be interpreted as implying that the transferor and transferee are under an obligation of due diligence to determine the conditions under which data is held prior to transfer and to ensure that the same conditions prevail after the transfer. In countries with strong data protection laws, the outcome is likely to be the same as under the “chain of trust” concept if the data subject has rights against any party who is in control of personal information without consent and notice. If a data subject is covered by strong data protection laws, it may still be possible to make novel uses of the data or to transfer the data onward to third parties if the data subject has executed a broad waiver of his or her rights, and such a waiver is enforceable.

**IMPACT OF BANKRUPTCY ON COMMERCIAL TRANSACTIONS IN DATA**

Bankruptcy proceedings may affect the way data is held and used in a variety of ways. An individual whose data is contained in a database and who has consented to that collection and use may face unexpected problems if the party in control of that data files for bankruptcy and the bankruptcy court does not recognize the original limits placed on the use of the data. A business that expects to receive certain types of data in the

314. See UCITA § 503. UCITA as a whole is subordinate to article 9. Id. § 103(c). A grant of an article 9 security interest in information would be valid under article 9 even though it would constitute a breach of the agreement transferring the information that purports to prevent any subsequent transfer of the information, including in the form of a security interest. U.C.C. § 9-406 (1999).

future may find that its access to that data is terminated if the transferor files for bankruptcy. A business that has entered into contracts limiting the uses to which certain forms of data may be put as part of a strategic alliance with another business may find that those contractual terms become unenforceable if the alliance partner files for bankruptcy.

A business organization that is a legal but not a natural person has no rights under data protection laws, and must rely on the enforcement of contract terms for its rights against third parties. Such a party who has consented to the collection and use of data by another party may face unexpected difficulties if the party holding the data files for bankruptcy and the consenting party’s rights are protected by a simple contract and not ownership of an intellectual property right or security interest. The consenting party’s rights under the agreement may be terminated without any effective recourse if the trustee in bankruptcy has no reason to reaffirm the contract or if claim cannot be classified as secured. If the bankruptcy trustee considers the database to be an asset and tries to find buyers for that asset, the consenting party may not be the only person bidding on the asset.

The consenting party will need to find a way to ensure that the bankruptcy trustee is not permitted to sell the data to the highest bidder if that is the consenting party’s competitor. One strategy may be to establish in the governing license agreements that the database asset is licensed with a copyright license that is non-assignable under common law.316 Another approach would be to include in the license agreement provisions governing related ongoing services of the database licensee that are personal in nature. If a third party cannot perform those services adequately, the license may not be assignable under section 365(c). At a minimum, the license should include non-compete clauses that specify direct competitors of the licensor, who should not be permitted to acquire the data under any circumstances.

PRACTICAL STRATEGIES FOR MANAGING DATA RIGHTS AND RISKS IN A CHANGING LEGAL ENVIRONMENT

The failure of the law to keep pace with the rapid evolution of technology and business models is creating increasing risk for companies that depend on database assets. These risks include:

- Regulatory enforcement actions by the FTC, SEC, state agencies and officials, and EU authorities;
- Litigation by consumers and privacy organizations;
- Loss of access to critical databases maintained by third parties;

• Uncontrolled third party distribution of proprietary databases as a result of security lapses or lack of contractual protections;
• Loss of control over use and distribution of licensed data that are transferred in the course of a licensee’s bankruptcy proceeding;
• Loss of key database assets that are licensed from third parties facing bankruptcy; and
• Failure to take maximum advantage of business opportunities that require sophisticated data risk management.

Given the uncertainties and increasing importance of data assets, affected companies and their counsel should consider a proactive approach towards identifying and reducing these risks, possibly including the following four general action items:

Designate a data risk manager and conduct a company-wide data audit to identify compliance requirements, liability exposures, key third-party relationships, and data security needs. Minimizing data risks is as much a management challenge as a legal problem. Successful management of these risks requires commitment at the highest levels of the corporation, attention by qualified and capable managers with a clear mandate, effective communication within the company, and dedication of appropriate resources.

Unfortunately, most corporations today are not well structured to accomplish these goals. Data and databases are used and maintained by a variety of corporate departments, typically including Information Technology, Marketing, and Human Resources. Managers in these groups have primary responsibilities (i.e., generating revenues and keeping computer systems working) that are full time responsibilities and often are not consistent with effective data risk management. On the other hand, the General Counsel’s office and legal staff will be involved in discrete licensing projects and transactions, but typically do not have a full understanding of the data flows and technologies. They are charged principally with getting the deal done, not slowing it down by adding new considerations. Moreover, the technology industry has grown so steadily and at such a rapid pace that relatively little attention has been paid to the downside risks and legal implications of worst-case scenarios. With the slowing economy in the early 2000s, greater conservatism and proactive risk management in licensing transactions may be appropriate.

For companies that rely on customer databases or third-party data relationships, especially companies in the financial services and health care sectors, designation of a V.P.-level manager with responsibility for data risks will be an important step towards effective management of data risks. This “Data Officer” should have a basic understanding of the company’s technology and data operations; reporting and line authority over Information Technology personnel; a clear mandate from senior management; and sufficient resources to achieve the company’s data risk objectives and to most effectively take advantage of market opportunities.
The Data Officer should supervise an initial and annual company-wide audit or review of data collection, storage, uses, and transfers. The scope of this review will depend on the nature of the company’s operations and the extent of the data risks presented. It could range from file review and meetings with appropriate personnel over a few week period, to a comprehensive audit, undertaken and reported by third-party consultants. The results of the data review should be used to formulate privacy policies and other corporate procedures to address data risks.

Conduct thorough legal and liability exposure analyses in designing and implementing new initiatives. Technological advances and new business models that leverage customer data increasingly bring the risk of violations of law and perceived abuses of privacy interests. Federal and state officials, and the plaintiffs’ bar, will be expected to aggressively pursue litigation based on alleged privacy violations. The case studies reviewed above may only be a preview of the coming waive of litigation over privacy rights. As demonstrated in other areas, where the basic legal framework is unformed or uncertain, there is a greater tendency towards litigation and judicial resolution of competing rights.

Review of new corporate initiatives involving customer data should include the Data Officer, and where appropriate, in-house and outside counsel to consider regulatory and commercial risks in light of existing laws and anticipated future laws. Even at the pace of “Internet time,” proposed transactions should be evaluated for risk minimization and long-term sustainability. Aggressive action may be the hallmark of the new economy, but the cost of extricating the company from a risky or failed data venture may be greater than the opportunity cost of not going forward.

Evaluate third party contracts, including partnerships, alliances, marketing agreements, and participation in B2B hubs, that may create material data rights and exposures. The value derived from databases increasingly is created through partnerships involving multiple parties in the data chain. In these circumstances, intellectual property protection is at its lowest, privacy and security risks are high, and therefore clear and enforceable contract rights are critically important. Effective multi-party data sharing and database access frameworks can be established by contract. Harmonization across jurisdictions remains, however, an issue that may not be resolvable by contract. In addition, as the market fluctuates, third parties may become insolvent, so that the potential for bankruptcy should be considered and addressed through appropriate licensing strategies.

In negotiating and implementing corporate transactions, conduct thorough due diligence with respect to data assets and include specific representations, warranties, and indemnification provisions to address data rights and risks. Data rights and responsibilities should be carefully considered before a transaction is consummated. The acquirer should conduct full due diligence of data assets to evaluate any potential regulatory and litigation exposure of the target and to ensure that the transaction goals will be met consistent with the terms of existing contract frameworks.
CONCLUSION

Commercial uses of information are expanding more rapidly than the law governing commercial transactions in information. As a result, parties to data transactions should pay close attention to contract provisions governing rights in data as a first line of defense in protecting those rights. Contractual obligations may not be fully enforceable, however, given the current unsettled state of the law in this area. Privacy law or trade practices law doctrines may apply in specific contexts to render contract provisions unenforceable, or to create enforcement and liability risks associated with data that may not have been foreseen by the parties.

Because of technological advances and changing business models, database assets will only become more valuable and numerous in the future. As more cases involving rights in data are litigated, interest in legislative action will increase. The conflicting interests of the various parties claiming rights in data will not be easy to resolve, however, and it is unclear that any legislation in this area is likely to garner the widespread support that would be necessary for rapid enactment.

The state of uncertainty is unlikely to abate any time soon, even if Congress enacts legislation granting intellectual property rights in databases or clearer privacy rights for individuals. In the face of uncertain legal rights in data, parties holding valuable database assets would be well advised to focus on practical strategies and technologies that can be used to safeguard physical control over those assets. When the applicable law is uncertain, possession may be a functional substitute for clear legal rights in many instances. Critical evaluation, risk analyses, and careful planning with regard to data assets will become increasingly important as the law and technology in this area continue to evolve.