LAW OF ELECTRONIC COMMERCE

FOURTH EDITION

2

JANE K. WINN
BENJAMIN WRIGHT

ASPEN
LAW & BUSINESS

CHAPTER 14

PRIVACY AND COLLECTIONS OF DATA

§ 14.01 OVERVIEW

Advances in database-management technologies and the falling prices of communications and information-processing technologies are contributing to an explosion in business applications for data. If the data describes individuals, then privacy law may limit some of the uses a business may make of that data. American privacy law is a complex patchwork of statutes and common-law doctrines which in aggregate have a surprisingly narrow scope when applied to the business use of personal information. This is in marked contrast with the privacy law of the European Union, which grants very general, very strong privacy rights to individuals in the EU.

With regard to databases composed of factual information that does not describe individuals, U.S. law is also very unclear. While the EU has created a new intellectual property right for databases of factual information, each time similar legislation is introduced in the U.S., it has been blocked by civil liberties organizations, research scientists, and librarians. In the absence of such a new "sui generic" intellectual property right, owners of commercial databases of information that do not qualify for copyright protection must look to a patchwork of doctrines such as trespass to chattels, misappropriation, and trade secret law for some form of protection.

The U.S. approach to protecting the privacy of personal information has relied heavily on a combination of relatively lax "self-regulation" for most businesses and relatively strict regulation for certain industry sectors. Financial services companies have been hard hit by new state and federal regulations trying to combat the problem of identity theft. Many health care providers have had to

overhaul their systems for handling patient health records in order to comply with new federal medical record privacy regulations. What has made these regulations particularly onerous is that they include computer security standards to insure that sensitive information actually remains confidential. Web businesses that target children are now required to observe some of the strictest information practices of any businesses in the U.S.

Outside of these regulated industries, most U.S. businesses are permitted to establish their own privacy policies and are held liable for unfair trade practices only if they fail to follow their own published policy. California was the first state to pass a law requiring businesses that collect personal information from California residents to post a privacy policy, so in principle any U.S. business outside California that fails actively to exclude California residents is now required to post a privacy policy. In order to give this self-regulatory system some credibility, third party services such as TRUSTe WebTrust and BBBOnline establish minimum standards of privacy protection and permit merchants who agree to abide by those minimum standards to display a "seal" from the online privacy seal service. These third party services lack resources actually to investigate whether their members are in compliance and may be reluctant to criticize their primary revenue source—their members. The Federal Trade Commission has taken enforcement actions against more than a dozen Web businesses in recent years, securing settlements ranging from a few thousand dollars to nearly half a million dollars for alleged failures to follow posted privacy policies.

By contrast, the EU has recently enacted several directives establishing broad protections for the privacy of personal information. Given the glaring disparity between the strong privacy protection regime in the EU and the weak regime in the U.S., in the mid-1990s, European governments threatened to block flows of personal information from Europe to the U.S. Such an outcome would have been unacceptable for U.S. businesses such as multinational corporations, airlines, and financial services companies that regularly move personal information between the U.S. and EU. The U.S. and EU reached a compromise, known as the "Safe Harbor," that permits individual U.S. companies to certify that their handling of the personal information of EU citizens conforms to the standards of EU law. U.S. companies that participate in the Safe Harbor may transfer personal information from the EU to the U.S.; any violations of the terms of the Safe Harbor are subject to Federal Trade Commission enforcement, not separate enforcement actions by every national data protection office in Europe. In the years since the Safe Harbor was announced to great acclaim, it has substantially failed to meet expectations on either side of the Atlantic. Instead of tens of thousands of companies joining, only a few hundred U.S. companies have joined. The EU Commission tried to determine actual compliance rates among U.S. companies participating in the Safe Harbor and found that based simply on posted privacy policies and without any examination of actual internal practices, many companies were not in compliance with Safe Harbor requirements. While the EU

has not tried to revoke its agreement to the Safe Harbor or renegotiate its terms, it has vigorously disputed U.S. treatment of airline passenger name records after changes in procedures were implemented as counterterrorism measures. Given the huge gap between U.S. and EU approaches to the privacy of personal information, such conflicts are bound to recur on a regular basis.

Even though enforcement actions are relatively few, many companies that fail to follow fair information practices have found themselves defendants in class action lawsuits brought on behalf of their customers. Although a large number of high profile class action lawsuits based on various theories of information privacy rights were filed between 1999 and 2002, few were successful. Nevertheless, the threat of either a class action lawsuit or a deceptive trade practices enforcement action brought by the FTC or one of the state attorneys general has encouraged many U.S. businesses to focus more attention on how they handle personal information. A substantial investment of resources will be required of any business that intends to post an accurate privacy policy and follow it consistently, including segregating personal information based on the privacy policy that was in effect when it was collected and notifying customers whenever their policy changes.

§ 14.02 RIGHTS IN DATA AND TECHNOLOGICAL CHANGE[1]

The open architecture of the Internet has created an environment for electronic commerce in which there are simultaneously 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, machines which were often kept isolated in rooms with special climate controls.[2] 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"[3] originated at this time because there was normally a unique person or group of people who controlled access to information on a computer. When computer networks were first built, they were connected by dedicated communications lines, such as owned or leased lines, or relied on the services of "value-added networks" that guaranteed a high level of security and integrity in communications over the network.

The Internet is an open, public, and cooperative facility accessible to an almost unlimited number of people worldwide. 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

---

[1] This section is based on Jane Kaufman Winn & James R. Wrathall, *Who Owns the Customer? The Emerging Law of Commercial Transactions in Electronic Customer Data*, Bus. Law. (forthcoming, Nov. 2000).

[2] Computers were located in cold rooms because they would otherwise overheat.

[3] *See, e.g.*, EU Data Protection Directive art. xx

of the operating systems or the network systems connecting 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 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.[4]

Once information is stored on a server connected to the Internet, that information may be accessed by anyone with access to the Internet unless some access controls are established. Given the open architecture of the Internet, effective access controls may be difficult to design or maintain.[5] When an individual is using the Internet, his or her behavior may be observable to a large number of other individuals. A record of that behavior may also be collected and saved without the individual being made aware that is taking place. 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.[6] 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.[7] In addition, ActiveX, Java, or JavaScript applets[8] 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.[9] This is the type of undisclosed end-user monitoring RealNetworks used for marketing purposes and which eventually resulted in the filing of several class-action lawsuits.[10]

Unless some additional steps are taken, however, it may be difficult to determine just which person is associated with a particular online behavior being observed and recorded. Any computer that is part of the Internet needs to have an Internet Protocol (IP) address[11] in order to be recognized by the network, but there

---

[4] *See generally* Trust in Cyberspace (Fred B. Schneider ed. 1999).

[5] 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.

[6] Jesus Mena, Data Mining Your Website 193 (1999).

[7] Web Traffic Analysis, ZDNetUK Online Briefing, available at ≪www.zdnet.co.uk/itweek/brief/1999/44/internet/02.html≫.

[8] An *applet* is a small program sent to an end user's computer together with a requested Web page. The applet may be sent without the end user's knowledge, and the scope of the applet's functions may not be clear to the end user.

[9] For an explanation of the history file in Netscape products, *see* ≪http://help.netscape.com/kb/consumer/19960627-14.html≫.

[10] *See* RealNetworks case study.

[11] In the most widely installed level of the Internet Protocol today, an IP address is a 32-bit number identifying each sender or receiver of information sent in packets across the Internet. When

is not yet any 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 sites without having to reenter identifying information each time.[12] 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 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 identifying information, for instance through a registration form.

Many "free" offers available to individual users are not free at all, but instead involve loading software onto the individual's computer able to transmit a wide range of information about the online activity of the individual, or at least his or her computer. For example, free Internet access providers such as *netzero.com* collect clickstream data in order to monitor individual behavior online.[13] 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 and organizations to determine 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, failure to implement policies and procedures to guarantee compliance, or failure to implement adequate technological safeguards.

A *database* is a collection of data organized so that its contents can easily be accessed, managed, and updated. The most prevalent type of database is the *relational database*, in which data is defined so that it can be reorganized and

---

the user requests an HTML page or sends e-mail, the Internet Protocol part of TCP/IP includes the user's 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 requested or in the e-mail address sent a message. At the other end, the recipient can see the IP address of the Webpage requestor or the e-mail sender and may respond by sending another message using the IP address it received. Definition of *IP address*, available at <<www.whatis.com>>.

[12] Definition of "cookies," available at <<www.cookiecentral.com/cookie3.htm>>.

[13] Josh Smith, *The Real Cost of Free Software*, Ziff Davis Smart Business for the New Economy, Aug. 1, 2000 (available in Lexis News); Hugh Son, *Beware: The Free Internet's Downside Can Really Add Up*, N.Y. Daily News, May 21, 2000 (available in Lexis News).

accessed in a number of different ways without having to reorganize the database.[14] The term "data warehouse" is often used to describe separate databases that have been designed to support marketing and strategic decision-making.[15] A *data warehouse* is a central repository for all or significant parts of the data that an enterprise's various 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.[16] 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.[17] 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 decisionmaking.

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 establish associations between facts that were not known to have any correlation: chronological sequences of events; classification of data according to newly recognized patterns such as customer profiles; clustering of data into groups not previously known; and 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.[18]

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 assembled a customer database may be shared with other companies, offering an additional revenue stream at a low incremental cost.

The combination of easy access to sensitive personal information and poor security for personal computers, Internet communications, and even many business information systems has produced an explosion of identity theft problems

---

[14] Definition of "database," available at ≪www.whatis.com≫.

[15] *See generally* Vitek R. Gupta, An Introduction to Data Warehousing, available at ≪http://systems-services.com/dwintro.asp≫.

[16] Definition of "data warehouse," available at ≪www.whatis.com≫.

[17] Beth Stackpole, *Targeting One Buyer—or a Million,* Datamation, March 2000, available at ≪http://itmanagement.earthweb.com/datbus/article.php/621301≫.

[18] Definition of "database," available at ≪www.whatis.com≫.

in the U.S. While recent legislation makes it easier for individuals to access their credit reports in order to learn whether they are victims of identity theft and increases the punishment for perpetrators,[19] it is difficult to imagine that such superficial changes in the manner in which sensitive personal information is generally handled in the U.S. will make much of a dent in the problem. Even as efforts increase to crack down on well-known forms of financial fraud such as identity theft, new forms of fraud create new problems. *Phishing* attacks use spoofed e-mails that appear to come from well-known businesses to direct recipients to fraudulent Web sites that appear to be major commercial sites in order "to fool recipients into divulging personal financial data such as credit card numbers, account usernames and passwords, [or] social security numbers."[20] According to the Anti-Phishing Working Group, an industry coalition formed in 2003 to combat the skyrocketing rate of phishing attacks, as many as 5% of recipients to respond to these spoofed e-mails.[21] Phishing is a relatively low-technology attack that exploits the poor security characteristic of most Internet communications and relies on "social engineering" to succeed.

§ 14.03 PRIVACY RIGHTS

The idea of a right to privacy first gained attention in the United States with the 1890 publication of a law review article by Samuel Warren and Louis Brandeis.[22] Privacy law has developed in fits and starts in the intervening years, creating a complex patchwork of statutes and common-law doctrines.[23] As a result of the *ad hoc* manner in which U.S. privacy law has developed, some types of privacy are highly protected while others, such as medical records, are almost completely without any form of legal protection. This approach to privacy law is in marked contrast with the European Union's approach, which proceeds from a comprehensive, coherent statement of privacy law principles in the 1995 Data Protection Directive.[24]

Due to both the uneven and, in some cases, nonexistent protection provided privacy under U.S. law and the recent explosion in business uses for personal information, a flood of privacy legislation has appeared in the United States in recent

---

[19] For discussion of identity theft law reforms, *see infra* §§ 14.03[C], 14.03[L].

[20] Anti-Phishing Working Group, *What Is Phishing?*, ≪http://www.antiphishing.org/≫ (accessed September 1, 2004).

[21] *Id.*

[22] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890).

[23] *See generally*, Paul M. Schwartz & Joel R. Reidenberg, Data Privacy Law (1996); Marc Rotenberg, The Privacy Law Sourcebook 1999: United States Law, International Law and Recent Developments (1999). Rotenberg's collection of statutes is published by the Electronic Privacy Information Center (EPIC) and updated on a regular basis. The most recent issue may be obtained from the EPIC Web site at ≪www.epic.org/bookstore≫.

[24] Data Protection Directive (DPD), Council Directive 95/46/EC, 1995 O.J. (L 281) 31; *see infra* § 14.05.

years. The number of new privacy laws or regulations issued is unprecedented, and this trend will likely not abate in the near future. Rather, this sudden increase in the volume of privacy legislation may be a harbinger of a trend which will persist for some time, possibly until the protection of privacy rights under U.S. law approaches something equivalent to the current level of privacy protection enjoyed by individuals in Europe. In the United States, however, powerful business interests like the Direct Marketing Association, whose current business models are premised on the lack of comprehensive privacy laws, will lobby long and hard to block major privacy legislation. Privacy laws enacted in the United States therefore may take the form of the recent Gramm-Leach-Bliley privacy provisions:[25] long, complex, opaque and, in the final analysis, providing little substantive protection.

Although information privacy rights guaranteed by law in the United States are quite limited, the concept of fair information practices has been recognized for some time. The first statement of fair information principles came in 1973, in a study of computers and privacy rights issued by the U.S. Department of Health, Education and Welfare.[26] The fair information principles set out in that study included:

1. Maintain no secret information systems. (A "secret" system is one whose existence and purpose is known only to a select few.)
2. Collect only that information necessary to the lawful purpose of a record system and, when feasible, collect personal information directly from the data subject.
3. Be sure that the information is relevant, accurate, timely, and complete.
4. Provide the data subject with access to information about himself and a procedure by which to challenge and correct that information.
5. Use data only for the particular purpose for which it was initially collected except as permitted by the specific, informed consent of the data subject. (This is generally referred to as the "secondary use" limitation.)
6. Protect data against unauthorized disclosure, alteration, or loss. (The "security" principle).[27]

U.S. privacy laws vary widely in the degree to which they mandate fair information practices, or the scope of information to which fair information practices are applied.

---

[25] *See infra* § 14.03[N].

[26] U.S. Dep't of Health, Education, & Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens *viii* (1973).

[27] George Trubow, *The European Harmonization of Data Protection Laws Threatens U.S. Participation in Trans-Border Data Flow*, 13 J. Int'l L. Bus. 159, 162 (1992).

[A] United States Constitution

The Constitution is a source of privacy rights under U.S. law.[28] The Supreme Court has discovered a right of privacy implicit in the Bill of Rights that protects individuals from government interference in certain contexts. In *Griswold v. Connecticut*,[29] the Court found that a state law prohibiting the use of contraceptives by married couples violated a privacy right implicit in the First Amendment right of freedom of association. In *Loving v. Virginia*,[30] the Court found that a state anti-miscegenation statute prohibiting "white" persons from marrying "colored" persons violated a privacy right implicit in the equal protection and due process clauses of the Fourteenth Amendment. In *Roe v. Wade*,[31] the Court found that women have a privacy right under the Fourteenth Amendment to terminate a pregnancy. In *Paul v. Davis*,[32] however, the Court found that an individual had no constitutional right to privacy to prevent local law-enforcement officers from distributing a photograph of an individual in a police flyer labeled "active shoplifters." The Court did affirm that, although there is no explicit right of privacy in the Constitution, implicit "zones of privacy" may be created by other constitutional guarantees that impose limits upon governmental power. Those privacy rights do not apply to any tort that a government official may commit against a citizen, but apply to matters relating to marriage, procreation, contraception, family relationships, and child rearing and education.[33] It is clear that privacy rights implicit in the Constitution protect individuals against governmental action in a limited number of circumstances, all of which are unlikely to arise in the context of electronic commerce.

The Fourth Amendment protects individuals from unreasonable searches and seizures by government officials. In *O'Connor v. Ortega*,[34] the Court held that if a public employee has a reasonable expectation of privacy in his or her office and files, then the Fourth Amendment may prohibit a public employer from searching the office and files. Even if an employee has a reasonable expectation of privacy, however, that interest must be weighed against the government's need to supervise and control employees in a government office in order to perform the office's operations. In order to balance the employer's interest in efficiency in the workplace and control over employee behavior with the employee's privacy rights, the reasonableness of the belief that the search would turn up evidence of

[28] In addition, state constitutions may create privacy rights for the residents of that state.
[29] 381 U.S. 479 (1965).
[30] 388 U.S. 1 (1967).
[31] 410 U.S. 113 (1973).
[32] 424 U.S. 693 (1976).
[33] 424 U.S. at 712.
[34] 480 U.S. 709 (1987).

what the employer was investigating and the scope of the search relative to the reason for the search should be taken into account.[35]

Individuals have a right of anonymity against the government in certain limited circumstances, such as when the NAACP's refusal to provide its membership list to the state of Alabama was upheld by the Supreme Court as protected by the First Amendment.[36] In *McIntyre v. Ohio Elections Commission*,[37] the Supreme Court stuck down an Ohio statute requiring anyone circulating written materials endorsing or opposing a candidate or referendum to include the author's name and address. It is unlikely that the First Amendment gives individuals a right to anonymity online, as this right is quite limited.[38]

In *Bartnicki v. Vopper*,[39] the Supreme Court held that the First Amendment protected a radio station from civil liability under state and federal wiretap statutes[40] after it broadcast a recording of a cell phone conversation that had been unlawfully intercepted and recorded. In a conversation made using cell phones, union leader and a negotiator engaged in collective bargaining on behalf of a teachers union discussed the possibility of damaging the property of local school board members as a tactic to gain leverage in the negotiations. An unknown person intercepted the call, recorded it, and provided the tape recording to a local group opposed to the activities of the teachers' union. That group then turned over the recording to a local radio station, which broadcast it on a public affairs talk show. The individuals whose cell phone conversation had been intercepted sued the radio station, the talk show host, and the president of the local group for damages under the Pennsylvania and federal wiretap statutes. The Supreme Court held that the application of wiretap statutes in this case would violate the First Amendment because the public interest in the content of the speech outweighed the privacy rights conferred by statute.

In *Quigley v. Rosenthal*, the Tenth Circuit held that the Anti-Defamation League (ADL) was not protected by the First Amendment when it released the contents of an illegally intercepted wireless phone conversation.[41] In October 1994, after the Quigleys had become embroiled in a series of squabbles with their neighbors, the Aaronsons, the Aaronsons began using a scanner to intercept the Quigley's telephone calls. The Aaronsons contacted the local prosecutor and the

---

[35] 480 U.S. at 726.

[36] NAACP v. Alabama, 357 U.S. 449 (1958).

[37] 514 U.S. 334 (1995).

[38] *See, e.g.*, California Bankers Ass'n v. Schultz, 416 U.S. 21 (1976) (banks may keep microfilm records of all checks from contributors deposited by civil rights groups).

[39] 532 U.S. 514, 121 S. Ct. 1753 (2001)

[40] Pennsylvania Wiretapping Act, 18 Pa.C.S. §§ 5703, 5725, 5725(a); 18 U.S.C. §§ 2511, 2520, 2520(c)(2). *See* § 14.03[H] and § 21.04[B] for further discussion of the federal Electronic Communications Privacy Act.

[41] Quigley v. Rosenthal, 327 F.3d 1044 (10th Cir. 2003).

Anti-Defamation League to complain about the Quigley's threatening behavior and anti-Semitic comments and, with the encouragement of the ADL, continued monitoring the Quigleys' phone conversations. When the Aaronsons filed a civil suit, Saul Rosenthal, director of the Denver ADL office, held a press conference denouncing the Quigleys, and the local prosecutor charged them with ethnic intimidation. But after the Quigleys counterclaimed for invasion of privacy by intrusion, false light invasion of privacy, defamation, and violation of the federal Wiretap Act, the local district attorney dropped the prosecution and issued an apology. The Quigleys were awarded $10 million in damages, which was upheld on appeal. The Tenth Circuit rejected the ADL claim that Rosenthal's public comments should be privileged and distinguished this case from *Bartnicki* on three grounds: the content of the conversation was of private, not public, interest; the ADL had not accurately reported on the contents of the conversation; and the ADL had actively participated in making the illegal tapes.

In 2003, the Supreme Court ruled that the disclosure of a sex offender registry by means of a public Web site does not violate the due process rights of a convicted sex offender whose name appeared in the registry.[42] A convicted sex offender, who was required by Connecticut's Megan's Law[43] to register with the local Department of Public Safety, filed a 42 U.S.C. § 1983 action claiming that the law violates the Fourteenth Amendment's Due Process Clause. The offender argued that he had not been provided with an opportunity to contest the issue of his current dangerousness; however, the site stated that listings were based on previous conviction and that state officials had not determined that any registrant was currently dangerous. The Supreme Court held that due process considerations had to be met for the conviction upon which listing in the registry was based, but not for the subsequent public disclosure of the fact of the conviction. The public disclosure of the conviction did not violate any procedural due process rights, and the offender had not challenged the statute on substantive due process grounds.

In *United States v. Thorn*,[44] the Eighth Circuit held warrantless searches by agency personnel in connection with an investigation of employee misuse of computer resources did not violate the Fourth Amendment, because a state employee who had signed an agency computer-use policy that included prohibitions against pornographic materials had no reasonable expectation in the contents of his computer.[45] Evidence that the employee had accessed pornographic materials in violation of that policy was found while the employee's

---

[42] Connecticut Dep't of Pub. Safety v. Doe, 538 U.S. 1 (2003), *overruling* Doe v. Dep't of Pub. Safety ex rel. Lee, 271 F.3d 38 (2d Cir. 2001).

[43] Conn. Gen. Stat. § 54-257 (2004).

[44] 375 F.3d 679 (8th Cir. 2004). For further discussion of employee consent to employer IT policies, *see infra* § 21.02.

[45] 375 F.3d at 683 (citing O'Connor v. Ortega, 480 U.S. 709 (1987)).

computer was being searched as part of an investigation of work-related misconduct. Additional pornographic materials were found on his desk after the defendant authorized his supervisor to search the papers on his desk to look for a tax document. The Eighth Circuit also refused to suppress evidence obtained by local law enforcement after warrants were issued based on affidavits from the agency personnel who had conducted the warrantless searches.

[B] Tort Law

The Restatement (Second) of Torts recognizes four separate causes of action for invasion of privacy,[45.1] based on the work of Dean William L. Prosser:[46] intrusion upon another's seclusion; misappropriation of another's name and likeness; public disclosure of private facts; and false-light publicity. Intrusion upon another's seclusion requires that someone intrude upon their physical seclusion or into their private affairs, and that this intrusion be highly offensive to a reasonable person.[47] This tort may protect privacy rights in personal information, but the invasive behavior must be quite outrageous in order for liability to be imposed.[48] If someone appropriates another person's name or likeness in order to gain some economic benefit, then the person whose identity was misap-propriated may have an invasion of privacy cause of action.[49] Public disclosure of private facts requires that the disclosure be highly offensive to a reasonable person and involve facts that are not of legitimate concern to the public.[50] False-light publicity involves publicizing information with knowledge of or with reckless disregard for its falsity in a manner that would be highly offensive to a reasonable person.[51] As with any Restatement, these privacy rights are effective only to the extent that a particular jurisdiction incorporates them into the law of that jurisdiction. The degree to which states have recognized these privacy rights varies widely.

In 2004, an Illinois court of appeals upheld a summary judgment ruling that turning over cell phone customer information to researchers constituted neither the tort of intrusion upon seclusion[52] nor a breach of a service agreement.[53] Cell phone service providers retrieved customer record information including names, addresses, and social security numbers and provided that information to researchers who compared it with public death records and specific causes of

[45.1] Restatement (Second) of Torts, § 652A.

[46] William L. Prosser, *Privacy*, 48 Cal. L. Rev. 383 (1960).

[47] Restatement (Second) of Torts, § 652B.

[48] *See, e.g.*, Nader v. General Motors, 255 N.E.2d 765 (N.Y. 1970).

[49] Restatement (Second) of Torts, § 652C.

[50] *Id.* § 652D.

[51] *Id.* § 652E.

[52] Restatement (Second) of Torts § 652B.

[53] Busse v. Motorola, Inc., 2004 Ill. App. LEXIS 738 (Ill. App. Ct. 2004).

death. In addition, the researchers used the information to mail out questionnaires to cell phone users. The results of both studies were published, but individual cell phone users were not identified in either report. Some of the cell phone customers brought suit against the cell phone companies that participated in the studies, claiming invasion of privacy by intrusion upon seclusion and breach of contract. The plaintiffs failed to establish that the information provided to the researchers were private facts or that it was revealing, compromising or embarrassing, so the invasion of privacy claim was rejected. The breach of contract claim was rejected because the actions of the phone company were authorized by the Telecommunications Act of 1996.[54]

In 1999, Liam Youens murdered Amy Boyer as she left work and then killed himself, after having obtained the information he needed to track her down from Docusearch, an information broker. Youens had met Boyer when the two attended high school together and had created a Web site describing his obsession with her and stalking her. Docusearch first sold him Boyer's social security number for $45. It then hired a subcontractor to place a "pretext" call to Boyer at work, pretending the call was from Boyer's insurance company, in order to convince Boyer to reveal her work address, charging Youens $109 for this information. Helen Remsburg, Amy's mother, sued Docusearch for wrongful death in federal district court. Because of the novelty of the issues raised, the federal court certified five questions of law to the New Hampshire Supreme Court.[55] In *Remsburg v. Docusearch*,[56] the New Hampshire Supreme Court resolved the questions as follows:

- Does a broker who sells information to a client pertaining to a third party have a cognizable legal duty to that third party with respect to the sale of the information? Held: Yes, the threats posed by stalking and identity theft lead to the conclusion that the risk of criminal misconduct is sufficiently foreseeable so that an investigator has a duty to exercise reasonable care in disclosing a third person's personal information to a client.[57]
- If a broker obtains a person's social security number from a credit reporting agency as a part of a credit header without the person's knowledge or permission and sells the social security number to a client, does the individual whose social security number was sold have a cause of action for intrusion upon her seclusion? Held: Yes, if it can be shown

[54] 47 U.S.C. § 222(c)(3), (d)(2) (2004) (allowing carriers to provide customer data in aggregate and to disclose customer data to protect the carrier's own rights). In addition, 47 C.F.R. § 64.2005(c)(2) (2004) permits wireless service providers to disclose customer data for research on the health effects of wireless phone use.

[55] Remsburg v. Docusearch, Inc., 2002 U.S. Dist. LEXIS 7952 (D.N.H. 2002).

[56] 149 N.H. 148 (N.H. 2003).

[57] *Id.* at 155.

that the intrusion was such that it would have been offensive to a person of ordinary sensibilities.[58]

- When a broker obtains a person's work address by means of a pretextual telephone call and sells the work address to a client, does the individual whose work address was deceitfully obtained have a cause of action for intrusion upon her seclusion? Held: No, because where a person's work address is readily observable by members of the public, the address cannot be private information.[59]

- If a broker obtains a social security number from a credit reporting agency as a part of a credit header, or a work address by means of a pretextual telephone call, and then sells the information, does the individual whose social security number or work address was sold have a cause of action for commercial appropriation against the broker? Held: No, because the broker who sells personal information does so for the value of the information itself, not to take advantage of the person's reputation or prestige.[60]

- If a broker obtains a person's work address by means of a pretextual telephone call, and then sells the information, is the broker liable under the New Hampshire Consumer Protection Act to the person it deceived? Held: Yes, because the pretextual telephone call is unlawful deceit and the statute protects anyone harmed by unlawful business methods, not just those in privity with the merchant.[61]

In 2004, Boyer's mother settled her claims against Docusearch for $85,000 so the holdings were never applied by the federal district court to the facts of the Boyer case.[62] In 2003, the New Hampshire Supreme Court ruled in a declaratory judgment action brought by Docusearch's insurer that the insurance company had no duty to defend or indemnify its insured with regard to the negligence claim, but reversed and remanded the invasion of privacy and consumer protection claims.[63]

In *Gates v. Discovery Communications, Inc.*,[63.1] the California Supreme Court ruled that it was not an invasion of privacy for a television documentary

---

[58] *Id.* at 157.

[59] *Id.*

[60] *Id.* at 158.

[61] *Id.* at 160.

[62] Rosemary Barnes, *Snooping Online Is Big Business*, San Antonio Express-News, Aug. 28, 2004, at 7H (available in Lexis News).

[63] Preferred Nat'l Ins. Co. v. Docusearch, Inc., 149 N.H. 759 (N.H. 2003).

[63.1] 34 Cal. 4th 679; 101 P.3d 552; 21 Cal. Rptr. 3d 663 (Cal. 2004).

to reveal that an individual had previously served a prison term for a felony, even though that individual had since lived an obscure, lawful life and become a respected member of the community. The trial court had overruled the defendant's demurrer with regard to the invasion of privacy claim, and rejected the defendant's anti-SLAPP motion to strike the claim.[63.2] The Court of Appeals and the Supreme Court rejected the trial court's reasoning, holding that the First Amendment protected the documentary producers and presenters who had published information gathered from public official court records.

An AOL subscriber was unsuccessful in claiming that the deliberate release of an AOL screen name violated his privacy rights under either state or federal law.[63.3] The subscriber alleged that an unknown AOL employee had released his anonymous screen name to an unknown third party, which published intimate details about him on a listserv. The court held that the parties were bound by the terms of the subscriber agreement, which was governed by Virginia law, and that because only a fictitious name had been released, not the plaintiff's actual name or likeness, there was no cause of action under Virginia's law prohibiting the unauthorized release of the name or picture of a person.[63.4] The court also rejected the customer's claim under the Electronic Communications Privacy Act (ECPA)[63.5] because the complaint alleged that a third party, not the provider, had intercepted, used, or disclosed the customer's communications, and the ECPA does not provide for secondary liability.

[C] Fair Credit Reporting Act

The Fair Credit Reporting Act of 1970 (FCRA)[64] was the first major piece of federal legislation protecting individual information-privacy rights enacted in response to the widespread use of computers in business operations. FCRA regulates the circumstances under which credit reporting agencies may disclose consumer credit reports, and provides consumers with ways to dispute negative entries on their credit reports. A *credit reporting agency* is a party regularly engaged in the practice of assembling or evaluating consumer credit information for the purpose of furnishing consumer reports to third parties.[65] A *credit report* constitutes a communication of information by a consumer reporting agency bearing on a consumer's creditworthiness, and which is used in order to determine

---

[63.2] Cal. Code Civ. Proc. § 425.16 (2006) (SLAPP stands for "strategic lawsuit against public participation"); *see supra* § 2.02[B] for further discussion of anti-SLAPP legislation.

[63.3] Motise v. America Online, Inc., 2005 U.S. Dist. LEXIS 36991 (D. Va. 2005).

[63.4] Va. Code Ann. § 8.01-40 (2006).

[63.5] 18 U.S.C. § 2511 (2006); *see infra* § 18A.03[A] for further discussion of the ECPA.

[64] 15 U.S.C. §§ 1681-1681t.

[65] *Id.* § 1681a(f).