8-1-1999

Personal Privacy in the Information Age: Comparison of Internet Data Protection Regulations in the United Stats and European Union

Domingo R. Tan

PERSONAL PRIVACY IN THE INFORMATION AGE: COMPARISON OF INTERNET DATA PROTECTION REGULATIONS IN THE UNITED STATES AND THE EUROPEAN UNION

I. INTRODUCTION

"The right to be let alone - the most comprehensive of rights, and the right most valued by civilized men."[1]

Unless you refuse to get a driver's license,[2] make all of your calls from pay phones,[3] and deal only with cash,[4] your personal information, habits, and preferences are essentially fair game for anyone who wants to know about them. Likewise, the use of the Internet[5] leaves an individual susceptible to invasions of privacy.

---

1. Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

2. In an effort to build a national database of photos to assist retailers in preventing fraud, a New Hampshire company, Image Data LLC, purchased more than 22 million driver's license photographs from motor vehicle officials in South Carolina, Florida, and Colorado. *See* Robert O'Harrow, Jr. & Liz Leyden, *U.S. Helped Fund License Photo Database*, WASHINGTON POST, Feb. 18, 1999, at A01; *see also* Robert O'Harrow, Jr., *Drivers Angered Over Firm's Purchase of Photos*, WASHINGTON POST, Jan. 28, 1999, at E01; Karen Gullo, *Databank Raises Privacy Fears*, DETROIT NEWS, Feb. 19, 1999, at A5; Robert O'Harrow, Jr., *ACLU Cites Photo Flap, Seeks New Privacy Laws*, WASHINGTON POST, Feb. 19, 1999, at E01.

3. "Your telephone bills, both mobile and land-line, provide permanent, un-erasable details of every person you have ever called - name, address, telephone number, date and duration." Stuart Goldsmith, *Telephone Privacy* (visited Mar. 1, 1999) <http://www.stuartgoldsmith.com/tp .html>.

4. Even people who pay cash for groceries, in exchange for saving a few cents on a tube of toothpaste or six-pack of soda, sign up for and use "discount cards" that grocery stores use to track their buying and spending habits. *See* Schlumberger Limited & Studio Z, Commentary by Zelda Gordon – Aired 8/10/98 on KUNM Radio, *Frequent Shopper Cards - KUNM Commentary* (visited Mar. 1, 1999) <http://www.amadorbooks.com/nocards8.htm>; *Smart Cards Allow Supermarkets Loyalty Scheme To Target Individual Shoppers* (last modified June 16, 1998) <http://www.slb.com/ir/news/sct-edah0698.html>. In one instance, a man injured his knee after falling in a San Diego grocery store. When the man filed a lawsuit against the grocery store, the attorneys for the store investigated the store's records and discovered that the man had a "discount card" and was a frequent purchaser of alcohol. The attorneys used this information to shift responsibility for the accident to the man. *See* Ashley Craddock, *Panel Debates On-line Privacy Issues* (visited Mar. 4, 1999) <http://www.wired.com/news/news/politics/story/13223 .html>.

5. "The 'Internet' is the catch-all word used to describe the massive world-wide

This Comment compares Internet data protection regulations in the United States and the European Union. Part II introduces the issue of privacy. It provides the definition of privacy and explores various topics involving privacy on the Internet.

Part III examines Internet data protection regulations in the United States. It focuses on the constitutional protection of privacy rights and the passage of several privacy acts in the United States. This section also analyzes the current U.S. Internet policy of industry self-regulation and the reasons for the policy's inadequacy.

Part IV discusses Internet data protection regulations in the European Union. Specifically, it concentrates on the European Data Protection Directive that became effective on October 25, 1998.

Part V examines the effect of the European Union Directive on the United States. It focuses on the controversy arising from their different approaches to data privacy protection, with the European Union requiring the creation of comprehensive data protection legislation and the United States allowing the Internet industry to develop a self-regulatory regime.

Part VI ultimately concludes that the United States should follow the European Union's example and create comprehensive data protection legislation to protect personal privacy on the Internet.

II. PRIVACY

Privacy is a fundamental human right recognized, either explicitly or implicitly, around the world in nearly every country's constitution.[6] Increasingly, however, these privacy rights are being eroded by new technologies.[7] These technologies include

---

network of computers. The word 'Internet' literally means 'network of networks.'" Kevin Hughes, *Entering the World-Wide Web: A Guide to Cyberspace* (last modified Oct. 9, 1993) <http:www.hcc.hawaii.edu/guide /www.guide.html>. *See generally* Virtual Internet Guide (last modified Feb. 12, 1999) <http://www.dreamscape.com/frankvad/internet.html> (discussing the structure and uses of the Internet).

6. *See* David Banisar & Simon Davies, *Privacy and Human Rights: An International Survey of Privacy Laws and Practice* (visited Mar. 1, 1999) <http://www.gilc.org/privacy/survey/ intro.html>.

7. *See id.*

biometrics,[8] identity cards,[9] wiretaps,[10] video surveillance cameras,[11] and, as this Comment illustrates, the Internet. In response to this privacy erosion, there is a growing trend around the world towards the enactment of comprehensive privacy and data protection acts.[12]

A. What is Privacy?

Privacy is not a straightforward concept and, therefore, is difficult to define.[13] It is not a single interest, but rather has several different dimensions. Privacy can be divided into four

---

8. *See* Howard Millman, *The One and Only You* (visited Mar. 4, 1999) <http://www.infoworld.com/cgi-bin/displayArchive.pl?/98/26/e06-26.87.htm> (describing biometrics as "a science and business, [that] identifies people by their physical characteristics such as fingerprints and voice patterns . . ."); *see also* Banisar & Davies, *supra* note 6 (discussing the implementation of biometrics schemes across the world, such as a national fingerprint system for unemployment benefit and health care entitlement in Spain, a thumbprint database for elections in Jamaica, and DNA databases in the United Kingdom and the United States for use in police investigations). *See generally Internet Privacy Means More Than Passwords* (visited Jan. 14, 1999) <http://www.techserver. . /111898/info22_23466_noframes.html.> (describing the growth of the biometrics industry).

9. *See* Banisar & Davies, *supra* note 6 (stating that most countries of the world including Germany, France, Belgium, Greece, Luxembourg, Portugal, and Spain, use some type of identity card).

10. *See id.* (describing the wiretapping abuse of telephone, fax, and telex communications occurring in most countries).

11. *See id.* (discussing the increased use of video surveillance cameras by countries to monitor public areas, housing estates, car parks, and public facilities, and by employers to monitor employees in the workplace); *see also Smile - You're on Surveillance Camera* (visited Jan. 14, 1999) <http://www.nyposton-line.com/121598/editorial/8439.htm.> (describing the growing use of surveillance cameras in New York).

12. *See generally Privacy International* (last modified Feb. 10, 1999) <http://www.privacy.org/pi> (describing the adoption of privacy legislation in various countries). *See also* Banisar & Davies, *supra* note 6 (discussing the three major reasons for the movement towards comprehensive privacy and data protection laws in many countries, which are: 1) to remedy past privacy violations that occurred under previous authoritarian regimes; 2) to promote electronic commerce; and 3) to ensure that trade with the European Union will not be affected by the requirements of the European Union Data Protection Directive).

13. There are numerous viewpoints on the issue of privacy. Author, Edward Bloustein describes privacy as "an interest of the human personality that protects the inviolate personality, the individual's independence, dignity, and integrity." Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962, 971 (1964). According to author, Ruth Gavison, privacy is "a state which can be lost, whether through the choice of the person in that state or through the action of another person." Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 428 (1980).

general facets: 1) information privacy, which concerns the control and handling of personal data; 2) bodily privacy, which involves the integrity of an individual's body against invasive procedures; 3) privacy of communications, which covers individuals' interests in communicating among themselves using various forms of communications; and 4) territorial privacy, which involves setting limits or boundaries on intrusion into a specific space or area.[14] This Comment will focus on the area of information privacy as it pertains to the individuals who use the Internet.

B. Privacy and the Internet

With an estimated ninety-seven million Internet users worldwide in 1998, a number which is projected to more than triple to about 320 million by the year 2002,[15] the protection of electronic data is one of the most important issues today. According to a number of surveys, Internet users report that privacy protection is one of their greatest concerns. According to a Boston Consulting Group (BCG) Consumer survey, over 75% of users expressed concern over websites[16] monitoring their browsing on the Internet.[17] Similarly, 40% of Internet users have provided

---

14. *See* Banisar & Davies, *supra* note 6.

15. *See* Reuters Limited, *A Call for E-Commerce Research* (visited Mar. 2, 1999) <http://www.news.com:80/News/Item/0,4,26852,00.html?st.ne.ni.rel>. "According to some predictions, nearly one billion people will be on-line in the next 10 years." *Information Industry: Promise of Superhighway Will Not be Realized Without Privacy Protections*, BUS. WIRE, INC., Mar. 4, 1998, *available in* LEXIS, News Library, Curnws File [hereinafter *Information Industry*] (quoting Joseph L. Dionne, Chairman and CEO of the McGraw-Hill Companies). One study estimates that 23 million people in the United States log on to the Internet. *See* Lizette Alvarez, *Internet is New Pet Issue in Congress*, N.Y. TIMES, June 28, 1998, §1, at 16. A report for Mediamark Research Inc. approximates that 53.5 million adults in the United States, 27% of the adult population, use the Internet and that some 72 million American adults have access to the Internet. *See US Net Users Grow by 23%* (last modified Nov. 5, 1998) <http://cyberatlas.Internet.com/highlights/numbers.html>. The number of U.S. women who use the Internet is estimated to have escalated to 40% in 1997, from its previous mark of only 5% in 1994. *See Informative Statistics on Web Findings*, COMPUTIMES (Malaysia), Apr. 30, 1998, *available in* LEXIS, News Library, Curnws File.

16. A website is "an Internet destination where you can look at and retrieve data. All the websites in the world, linked together, make up the World-Wide Web." *Site Seeing On the Internet* (visited Jan. 13, 1999) <http://www.ftc.gov/bcp/online/pubs/online/sitesee/index.html>.

17. *See Are You Losing Business by Not Addressing Privacy Concerns?* (visited Oct. 5, 1998) <http://www.truste.org/webpublishers/privacypays/policy.html> [hereinafter *Losing Business*].

false information at least once when registering at a website, and over 70% worry about making on-line[18] purchases.[19] Another survey indicated that 78% of Internet users would go on-line more often if they felt that the privacy of their personal information was better protected.[20] Statistics clearly indicate that on-line users highly value privacy and are concerned about the dissemination of their personal information. Concerns about the vulnerability of the Internet to invasions of privacy are not unjustified.

1. Personal Information on the Internet

The Internet is an exciting tool that places vast information at your fingertips. With a click of a mouse, you can buy an airline ticket,[21] book a hotel,[22] send flowers to a friend,[23] or purchase your favorite stock.[24] While the Internet serves as a tremendous resource for information, products, and services, this same technology also provides companies with the ability to collect information about you and potentially distribute that information to others.

---

18. The term "to be on-line," as used herein, means "to be connected to the Internet."

19. *See Losing Business*, *supra* note 17.

20. *See Information Industry*, *supra* note 15.

21. *See generally* Cheap Tickets, Inc., *Welcome to Cheap Tickets Online* (visited Mar. 1, 1999) <http://www.cheaptickets.com>; Yahoo, Inc., *Yahoo! Travel* (visited Mar. 1, 1999) <http://travel.yahoo.com>; Airline International Travel, *Search for Discount Airfares* (visited Mar. 1, 1999) <http://members.aol.com/lowerair/index.html>.

22. *See generally* Express Hotel Reservations, *New York City Hotel Reservations, Discounts, Savings, Deals* (last modified Mar. 1, 1999) <http://www.express-res.com>; Hotel Reservations Network, *Hotel Reservations: Online Discounts for Hotels, Resorts, & Inns* (visited Mar. 1, 1999) <http://www.180096hotel.com>; Webscope, *Hotels and Travel on the Net* (visited Mar. 1, 1999) <http://www.hotelstravel.com>.

23. *See generally* USA Flowers, *Welcome to USA-Flowers* (visited Mar. 1, 1999) <http://www.usa-flowers.com>; Flowerlink, *Your Flowerlink to Friends and Loved Ones* (visited Mar. 1, 1999) <http://ygguaranteed.flowerlink.com>. The Internet also provides opportunities to send flowers electronically via e-mail. *See generally* E-Flower, *Send an Electronic Bouquet* (visited Mar. 1, 1999) <http://vweb.net/eflower/sendflower.html>; The Florist 800 Network, *Welcome to the E-Bouquet*™ (visited Mar. 1, 1999) <http://www.800send.com/eflower/ sendflower.html>.

24. *See generally E*Trade* (visited Mar. 1, 1999) <http://www.etrade.com/cgi-bin/gx.c. . .ic+Home?gxml=hpb_discover_c_t.html>; *Chicago Mercantile Exchange* (visited Mar. 1, 1999) <http://www.cme.com>.

a. Data Collection

A survey released by the Electronic Privacy Information Center found that nearly half of the 100 most popular websites collected information from users.[25] Personal information about Internet users is becoming easy to collect, or some may even say steal, due to software implementations known as "cookies."[26] "Cookies represent a coming effort by organizations to monitor people's interest in their products and services through the covert gathering of personal data without their knowledge and consent."[27] Generally, cookies allow websites to "tag" their visitors with unique identifiers so that they can be identified each time they visit the site.[28] The information obtained by the cookies identifies users' e-mail addresses, the names of their browsers, the types of computers they use, the universal resource locators (URL) or Internet addresses, the duration of the users' contact with websites, the specific pages of the websites that are visited, and what electronic transactions are made.[29]

b. Personalization

Many companies are turning to the Internet in search of ways to get closer to their customers. In order to achieve this goal, these companies are engaging in a process known as personalization. Personalization technology generates personalized web pages for

---

25. *See* Electronic Privacy Information Center, *Surfer Beware: Personal Privacy and the Internet* (last modified June 1997) <http://www.epic.org/reports/surfer-beware.html>.

26. A "cookie" is "a general mechanism which server side connections can use to both store and retrieve information on the client side of the connection." *Persistent Client State - HTTP Cookies*, (visited Mar. 1, 1999) <http://www.netscape.com/newsref/std/cookie_spec.html>. *See generally* Martin R. Kalfatovic, *Cookies: Stating the Not So Obvious on the Web* (last modified July 15, 1997) <http://www.lita.org/newslett/v18n4/edgeweb.html> (discussing the origin of the name "cookie"); *What are Cookies?* (visited Mar. 6, 1999) <http://www.rbaworld.com/Security/Computers/Cookies/cookies.html> (describing four different types of cookies: visitor cookies, preference cookies, shopping basket cookies, and tracking cookies); Simson Garfinkel, *The Persistence of Cookies* (visited Mar. 1, 1999) <http://www.hotwired.com/packet/garfinkel/96/50/ index2a.html> (stating that cookies can actually be used to improve the Internet).

27. *Commercialization of the World Wide Web: The Role of Cookies* (visited Mar. 1, 1999) <http://www2000.ogsm.vanderbilt.edu. . .65a/group5/paper.group5.paper2.htm> (quoting *Privacy Times* Editor, Evan Hendricks).

28. *See id.*

29. *See* Jim Erickson, *Are Those Who Go On-line to Send Junk Mail Out of Line?*, STAR TRIB., June 30, 1996, at 3D.

customers based on the demographic data obtained from these individuals.[30] In addition to the information that the individuals voluntarily provide, companies also acquire demographic data by monitoring browsing and buying patterns of the individuals who visit the companies' websites.[31]

The use of personalization technology is becoming common for many companies. For example, American Airlines and its cross-marketing partners, Hertz and Hilton, use personalization to improve their businesses by appealing to the needs and interests of each specific customer.[32] After accumulating information about a particular individual, a new, personalized Web page is created for that individual each time the individual enters the American Airlines website.[33] For example, "a person who requests a price quote for a[n American Airlines] flight to Boston will also receive extra information on the same web page as the ticket price, such as for a Hertz car and a Hilton hotel room during that same period."[34] Brokerage firms also plan to use personalization technology. These firms can monitor clients' viewing preferences on the brokerage's website, such as their assessment of specific stock quotes, thereby allowing brokers to recommend investments related to specific stocks.[35]

c. Anonymity

The issue of anonymity[36] on the Internet raises heated debates between supporters of free expression and those who believe that anonymity is only a shield for people who engage in abusive, hurtful, or illegal activity.[37]

---

30. *See* Gregory Dalton, *Personalizing On-line Data Raises Privacy Concerns -- As the Technology Matures, Companies Mull User Reactions Savvy: Open Sesame's Technology Monitors User Behavior*, INFORMATION WEEK, (last modified June 15, 1998) <http://www.techweb.com/se/ directlink.cgi?IWK19980615S0032>.

31. *See id.*

32. *See* Gregory Dalton, *Pressure For Better Privacy -- Business Moves to Fend Off Regulation of Internet Data*, INFORMATION WEEK, (last modified June 22, 1998) <http://www.techweb.com/ se/directlink.cgi?IWK19980622S0040>.

33. *See id.*

34. *Id.*

35. *See* Dalton, *supra* note 30.

36. Anonymity is "the quality of state of being unknown or unacknowledged." Karina Rigby, *Anonymity on the Internet Must be Protected* (visited Nov. 4, 1998) <http://swissnet.ai. mit.edu/6095/st. . .fall95-papers/rigby-anonymity.html>.

37. *See id.*

There are numerous reasons for people to hide their true identities when using the Internet.[38] For example, "you may want to protect yourself from an oppressive government, send something 'off the record' to a journalist, communicate with a self-help organization, . . . or just want to post all those politically incorrect thoughts from your work account at the Christian Coalition."[39] Because of the extremely conservative society in which we live, certain opinions, statements, and lifestyle choices can expose an individual to danger.[40] Anonymity is particularly significant for people who wish to express their views on-line about sensitive or controversial issues, such as sexual abuse, affirmative action, and harassment, without fear of retribution or embarrassment.[41] The lack of anonymity on the Internet can lead to "public ridicule or censure, physical injury, loss of employment or status, and in some cases, even legal action."[42]

III. INTERNET DATA PROTECTION REGULATIONS IN THE UNITED STATES

Individual privacy in the United States is protected through a combination of constitutional guarantees, federal and state statutes, regulations, and voluntary industry codes of conduct that apply to the public and private sectors in different ways.

A. Constitutional Protections

The United States Constitution does not specifically mention a right to privacy. As such, U.S. Citizens do not have an explicit federal constitutional right to privacy. The U.S. Supreme Court has, however, interpreted the Bill of Rights as creating, through its penumbras, "a right of personal privacy, or a guarantee [that] certain areas or zones of privacy [do] exist under the Constitution."[43] In addition, a number of state constitutions

---

38. *See Anonymity on the Internet* (last modified Feb. 13, 1999) <http://www.dis.org/erehwon/anonymity.html>.

39. *Id.*

40. *See* Rigby, *supra* note 36.

41. *See id.*

42. *Id.*

43. Roe v. Wade, 410 U.S. 113, 153 (1973) (holding that the right to privacy is broad enough to encompass a woman's decision whether or not to terminate her pregnancy); *see also* Griswold v. Connecticut, 381 U.S. 479, 485 (1965) (holding a statute prohibiting the

specifically enumerate the right to be protected from privacy invasions.[44] Notwithstanding the judicially recognized right to privacy in the U.S. Constitution and various state constitutions, the U.S. Supreme Court has yet to extend this right to personal information. Some informational privacy protections can, however, be found in the First and Fourth Amendments of the U.S. Constitution.[45]

1. First Amendment Protections

The First Amendment, which is most commonly associated with protecting speech and religion from government interference, also protects informational privacy. The First Amendment to the U.S. Constitution provides:

> Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press, or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.[46]

The First Amendment provides some level of informational privacy regarding defamatory speech.[47] In *New York Times Co. v. Sullivan*,[48] the U.S. Supreme Court held that for a public official[49] to prevail in a defamation suit, the public figure must show that the defamatory statement is false and that the statement was made with actual malice. The Court did not extend this heightened burden of proof to private individuals. While this holding can be viewed as limiting the applicability of common law right-of-privacy

---

giving of contraceptive information unconstitutional, thereby recognizing a right to "marital" privacy); Paul v. Davis, 424 U.S. 643, 713 (1976) (holding that the Constitution protects a right of privacy from governmental intrusions regarding intimate personal decisions concerning matters relating to marriage, procreation, contraception, family relationships, and child rearing and education).

44. *See, e.g.*, CAL. CONST., art. I, § 1; ARIZ. CONST., art. II, § 8; ILL. CONST., art. I, § 6.

45. *See generally* U.S. CONST. amend. I; U.S. CONST. amend. IV.

46. U.S. CONST. amend. I.

47. Defamatory speech, or defamation, includes false written statements of fact (libel) and false spoken statements of fact (slander). *See* BARRON'S LAW DICTIONARY 131–32 (4th ed. 1996).

48. 376 U.S. 254 (1964).

49. Public officials include "any elected or appointed person holding a public office and having duties relating to the sovereign powers of government." BARRON'S LAW DICTIONARY, *supra* note 47, at 404.

torts, it can also be seen as recognizing of the need for a high level of protection regarding the accuracy and truthfulness of statements made against private individuals. Although the First Amendment may facially appear to be concerned solely with the free flow of information through its protections of free speech and free press, it also clearly protects some level of informational privacy.

2. Fourth Amendment Considerations

As with the First Amendment, the Fourth Amendment to the U.S. Constitution also protects informational privacy. The Fourth Amendment states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[50]

An individual's right to privacy is protected under the Fourth Amendment's prohibition against unreasonable searches and seizures.[51] In *Olmstead v. United States,*[52] the U.S. Supreme Court ruled that no warrant was necessary for federal agents to tap telephone wires.[53] The Court held that the Fourth Amendment only protects against "physical invasions" by law enforcement officers.[54] *Olmstead*, however, was overruled in 1967 by the Court's subsequent decision in *Katz v. United States.*[55] In *Katz*, the U.S. Supreme Court held that the interception of a telephone conversation in a public telephone booth constitutes a search and seizure for Fourth Amendment purposes.[56] The Court stated:

> the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection . . . . But what he seeks to preserve as private, even in an area

50. U.S. CONST. amend. IV.
51. *See id.*
52. 277 U.S. 438, 466 (1928).
53. *See id.* at 464.
54. *See id.*
55. 389 U.S. 347, 353 (1967).
56. *See id.* at 353.

accessible to the public, may be constitutionally protected.[57]

As opposed to *Olmstead's* "physical invasion" requirement, the Court in *Katz* held that the threshold question for determining the existence of Fourth Amendment protection is whether the individual has a "reasonable expectation of privacy."[58]

B. Information Privacy Statutes

Presently, there is no comprehensive law in the United States guaranteeing privacy rights in personal information. There are, however, various privacy and security statutes that address specific privacy needs. Although existing federal statutes provide some level of informational privacy protection, there are gaps in this protection that can only be rectified by the enactment of a comprehensive federal statute.

1. Electronic Communications Privacy Act

Although vastly inadequate, the Electronic Communications Privacy Act[59] (ECPA) is currently the most comprehensive data protection legislation that protects personal information on the Internet. The ECPA covers all forms of digital communication, including transmissions of text and digitized images, in addition to voice communication.[60] The law prohibits unauthorized eavesdropping not only by the government, but by all persons and businesses.[61] The ECPA also prohibits unauthorized access to messages stored on computer systems, and unauthorized interception of messages in transmission.[62]

The ECPA contains numerous exceptions. The ECPA does not assure on-line system users' privacy rights from system operators for stored messages.[63] Since a system can be configured to store all messages that pass through it, the operator effectively has the ability to review all messages that pass through the system. Under the ECPA, it is illegal for a system operator to reveal stored

57. *Id.* at 351–52.
58. *Id.* at 353.
59. *See* 18 U.S.C. §§ 2510–2521, 2701–2711 (1998).
60. *See id.* §§ 2510–2521.
61. *See id.* § 2510.
62. *See id.* § 2511.
63. *See id.* § 2702(b).

private messages or users to anyone else.[64] It is legal, however, to reveal messages falling under certain specific exceptions noted in the ECPA.[65] For instance, a message sent to the operator himself can be disclosed, if he so chooses, since the operator is treated like any other recipient of a letter.

Another exception involves divulging information to government authorities. A message that is accidentally obtained by a system operator can be disclosed to legal authorities if the operator believes that illegal activity is taking place over the system.[66] Authorities then have the right to review these messages to the extent they deem necessary to confirm the system operator's apprehensions.[67] If, however, the authorities want to intercept or review messages at their leisure, they must first obtain an appropriate warrant from a judge or magistrate.[68]

In order to read a message that is stored for less than 180 days on an on-line system, a government agent must obtain a warrant.[69] On the other hand, if a desired message has been stored for over 180 days, the agent need only obtain an administrative subpoena.[70] System operators who cooperate with government agents that have proper warrants and court orders are not held subject to legal action by users whose messages are seized by the government.[71]

If the system operator happens to violate a user's privacy rights under the ECPA, such as posting private e-mail to the public, the ECPA gives the user the right to sue the system operator.[72] The system operator must then remove the public posting and can be held responsible for any monetary damages incurred as a result of the privacy violation.[73] The ECPA also allows for recovery of attorney fees.[74] This is especially important

64. *See id.*
65. *See id.*
66. *See id.* § 2702(b)(6).
67. *See id.* § 2703.
68. *See id.* §§ 2516–2518, 2703.
69. *See id.* § 2703.
70. *See id.*
71. *See id.*
72. *See id.* §§ 2520, 2707.
73. *See id.*
74. *See id.* §§ 2520(b)(3), 2707(b)(3).

in cases where proving operator misconduct or determining the dollar amount of damage is so difficult that users would otherwise refrain from bringing the case to court in the face of high legal costs. There are also criminal penalties for violating the ECPA.[75]

2. Other Informational Privacy Acts

In addition to the Electronic Communications Privacy Act, Congress has enacted several other acts protecting informational privacy. These acts include:

1) The Tax Reform Act, which protects the confidentiality of tax returns and return-related information and limits the dissemination of individual tax data among several federal agencies.[76]

2) Freedom of Information Act, which regulates third party access to government records, including records containing personal information.[77]

3) Right to Financial Privacy Act, which limits government access to bank records.[78]

4) Fair Credit Reporting Act, which regulates the use of credit information by credit reporting agencies.[79]

5) Cable Communications Policy Act, which requires the government to possess a court order to access cable records.[80]

6) Telecommunications Act, which safeguards customer information held by telecommunications carriers.[81]

7) Telephone Consumer Protection Act, which regulates

---

75. *See id.* § 2701(b).
76. *See* 26 U.S.C. § 6103 (1998).
77. *See* 5 U.S.C. § 552 (1998).
78. *See* 12 U.S.C. §§ 3401–34 (1998).
79. *See* 15 U.S.C. § 1681 (1998).
80. *See* 47 U.S.C. § 551 (1998).
81. *See* 47 U.S.C. § 153 (1998).

telemarketing practices.[82]

8) Federal Records Act, which regulates the disposal of federal records.[83]

C. Self-Regulation

In regard to on-line privacy protection, the United States currently follows a policy of industry self-regulation. Despite numerous on-line businesses establishing their own privacy guidelines,[84] the government, Internet users, and many on-line businesses agree that current industry efforts fall "far short of what is needed to protect [Internet users]."[85]

In June 1998, the Federal Trade Commission (FTC) released a "Report to Congress on Privacy On-line" that was highly critical of the effectiveness of self-regulation as a means of protecting privacy on the Internet.[86] Of the 1,400 websites examined by the FTC, only 14% informed visitors of their information collection

---

82. *See* 47 U.S.C. § 227 (1998).

83. *See* 44 U.S.C. §§ 2101–2118 (1998).

84. *See generally AT&T Expands On-line Privacy Policy; Emphasizes Protection of Children and Strengthens Customer Choice*, BUS. WIRE, INC., Sept. 9, 1998, *available in* LEXIS, News Library, Curnws File (announcing AT&T's expansion of its on-line privacy policy); *Internet Coalition to Promote On-line Privacy Trustmark*, POST-NEWSWEEK BUS. INFO., INC., Mar. 31, 1998, *available in* LEXIS, News Library, Curnws File (discussing companies that conduct business on the Internet, such as Adobe, BPI Communications, CBS, CNET, Collier Newfield, ConEx, Digimarc, MSNBC, Playboy Enterprises New Media Group, Sony On-line Ventures, IBM, AT&T, and the New York Times, using their own version of a seal of approval to promote consumer confidence in on-line transactions); *CyberMedia Enhances Its Internet Privacy Software*, PR NEWSWIRE ASS'N, INC., Sept. 3, 1998, *available in* LEXIS, News Library, Curnws File (describing Cybermedia's enhancement of its Internet privacy software to provide better protection of personal information); *HP Calls for Self-Regulation to Address On-line Privacy*, BUS. WIRE, INC., June 23, 1998, *available in* LEXIS, News Library, Curnws File (outlining Hewlett-Packard's new on-line privacy program).

85. *FTC Blasts On-line Privacy Efforts*, POST-NEWSWEEK BUS. INFO., INC., June 4, 1998, *available in* LEXIS, News Library, Curnws File. *See generally American Express Comments on FTC Report on Consumers' On-line Privacy*, M2 COMM. LTD., June 5, 1998, *available in* LEXIS, News Library, Curnws File (discussing American Express' support of the Federal Trade Commission's effort to help ensure more businesses develop and follow clear policies to protect consumer privacy); R. Scott McDuffie, *Self-Regulation Won't Happen* (visited Jan. 20, 1999) <http://www4.zdnet.com. . .rdesk/talkback/talkback_21781.html> (describing an Internet user's lack of confidence in the industry's ability to regulate itself).

86. *See* Federal Trade Commission, *Privacy Online: A Report to Congress* (last modified June 1998) <http://www.ftc.gov/reports/privacy3/toc.htm>.

practices.[87] Despite this lack of notice, 85% percent of these sites collect personal information.[88] Furthermore, only 2% of the websites examined posted a comprehensive privacy policy.[89] The results regarding children's sites are even more unsettling. Of the 212 children's sites surveyed, 89% collected personal information from youngsters, and only about half provided some disclosure of their practices.[90] Additionally, only 23% of the sites advised children to obtain permission before releasing their personal information; a meager 8% promised to notify parents of data collection practices; and less than 10% gave parents control over the harnessing and use of their children's data.[91] These statistics indicate that the FTC's conclusion, that the on-line industry's privacy efforts fallen "short" of what is needed, is a vast understatement.

On June 23, 1998, Commerce Secretary, William M. Daley, warned the on-line industry that "if the private sector won't ensure consumers their privacy is protected on-line, then the federal government will step in and try."[92] Likewise, Robert Pitofsky, Chairman of the Federal Trade Commission, stated that "unless industry can demonstrate that it has developed and implemented broad-based and effective self-regulatory programs by the end of this year, additional governmental authority in this area would be appropriate and necessary."[93] In a bid to preempt federal privacy legislation, numerous on-line industry groups are attempting to develop more effective privacy policies.[94]

---

87. *See id.*
88. *See id.*
89. *See id.*
90. *See id.*
91. *See id.*
92. *Protect Privacy or Feds Will - Daley*, POST-NEWSWEEK BUS. INFO., INC., June 23, 1998, *available in* LEXIS, News Library, Curnws File.
93. Mark Suzman, *FTC Chief Warns of Internet Privacy Action*, FIN. TIMES LIMITED (London), July 22, 1998, at 3.
94. *See generally* Courtney Macavinta, *Net Industry Reacts to FTC Threat* (visited Nov. 4, 1998) <http://www.news.com/News/Item/0,4,22762,00.html> (discussing the submission of a nine-point privacy protection plan to President Clinton by twelve high-tech trade groups representing more than 11,000 companies); *Industry Presses For On-line Privacy Self-Regulation*, POST-NEWSWEEK BUS. INFO., INC., July 21, 1998, *available in* LEXIS, News Library, Curnws File (describing a broad-based coalition of on-line companies and associations proposed framework to enforce on-line privacy).

The on-line industry's self-regulatory efforts have failed; now it is merely a question of whether or not the government is willing to follow through with its threat of intervention. It seems clear that individuals are in danger of privacy invasions every time they surf[95] the Internet. As one commentator stated, "when you hear the lifeguards saying that even the sharks should be left to self-regulate, you know it's every surfer for himself."[96]

IV. INTERNET DATA PROTECTION REGULATIONS IN THE EUROPEAN UNION

The European Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (Directive)[97] was adopted by the European Union's Council of Ministers on October 24, 1995. The Directive is clearly "the most important international development in data protection in the last decade."[98]

In an effort to secure a measure of harmonization, the new legislation required changes to existing data protection laws in the individual Member States.[99] Each of the Member States were given three years (until October 24, 1998) to amend their respective laws to comply with the Directive's requirements.[100]

---

95. To "surf" means "to browse or 'look at' information on the World Wide Web by pointing and clicking and navigating in a nonlinear way (meaning anywhere you want to go at anytime)." Vincent James and Erin Jansen, *Netlingo: The Internet Language Dictionary* (visited Aug. 12, 1999) <http://www.netlingo.com>.

96. *Junkbusters Upgrades Free Software for Internet Privacy*, BUS. WIRE, INC., July 15, 1998, *available in* LEXIS, News Library, Curnws File.

97. *See* Council Directive 95/46 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, 1995 O.J. (L 281) [hereinafter Directive].

98. Graham Greenleaf, *The European Privacy Directive—Completed*, PRIVACY L. & POL'Y REP., (1995) 2 PLPR 81 (visited Jan. 17, 1999) <http://www2.austlii.edu.au/~graham/ PLPR_EU_1.html>.

99. *See The European Union Directive on Data Privacy and Its Impact on Global Information Systems in US Corporations* (visited Jan. 17, 1999) <http://www.hunter-group.com/thg/ART/white_data.htm> [hereinafter *European Directive Impact*].

100. *See* Directive at para. 69. By the deadline at midnight on Oct. 24, 1998, only the UK, Greece, Italy, Portugal, and Sweden were in compliance with the Directive. *See* Chris Nuttall, *Privacy Laws Protect Personal Data* (visited October 24, 1998) <http://news.bbc.co.uk/hi/english/sci/tech/newsid_200000/200284.stm>. Most of the Member States already had some form of data privacy legislation prior to the adoption of the Directive, and need to make amendments to their existing laws to be in compliance with the new legislation. All of the Member States are anticipated to have fully

Aside from its internal impact, the Directive contains provisions regarding the transborder flow of data that will be felt worldwide.[101]

A. European Union Directive on Data Protection

Article 1 of the Directive states, "Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right of privacy, with respect to the processing[102] of personal data."[103] Through this Article, the European Union has boldly deemed informational privacy a fundamental human right.

1. General Rules

The Directive requires all of the European Union Member States to enact comprehensive privacy legislation that implements the following personal data policies:

a. Data Quality Requirements

1) *Fairness/Lawfulness*: Personal data must be "processed fairly and lawfully."[104]

2) *Purpose Limitation*: Personal data must be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes."[105]

---

implemented the Directive by the end of 1999. *See European Directive Impact, supra* note 99.

101. *See* Directive at arts. 25–26. *See generally European Directive Impact, supra* note 99 (describing the Directive's impact on U.S. companies that do business with, or in, the European Union).

102. Processing is defined as "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction." Directive at art. 2(b).

103. *Id.* at art. 1, para. 1. Personal data is defined as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, mental, economic, cultural, or social identity." *Id.* at art. 2(a).

104. *Id.* at art. 6, para. 1(a).

105. *Id.* at art. 6, para. 1(b).

3) *Relevant*: Personal data must be "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or for which they are further processed."[106]

4) *Accuracy*: Personal data must be "accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they are collected or for which they are further processed, are erased or rectified."[107]

5) *Timely*: Personal data must be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed."[108]

b. Legitimate Processing Requirements

1) *Consent*: Personal data may be processed only if "the data subject has given his consent[109] unambiguously."[110]

2) *Contract*: Personal data may be processed only if "processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject entering the contract."[111]

3) *Legal Obligation*: Personal data may be processed if "processing is necessary for compliance with a legal obligation to which the controller[112] is subject."[113]

---

106. *Id.* at art. 6, para. 1(c).
107. *Id.* at art. 6, para. 1(d).
108. *Id.* at art. 6, para. 1(e).
109. "Consent" is defined as "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed." *Id.* at art. 2(h).
110. *Id.* at art. 7(a).
111. *Id.* at art. 7(b).
112. "Controller" is defined as the "person, public authority, agency or any other body that determines the purposes and means of the processing of personal data. Where the[se] purposes and means . . . are determined by national or Community laws . . . , the controller or the specific criteria for his nomination may be designated by a national or Community law." *Id.* at art. 2(d).
113. *Id.* at art. 7(c).

4) *Vital Interests*: Personal data may be processed if "processing is necessary in order to protect the vital interests of the data subject."[114]

5) *Public Interest/Official Authority*: Personal data may be processed if "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in the third party[115] to whom the data are disclosed."[116]

6) *Legitimate Interests*: Personal data may be processed if processing is "necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection under Article 1(1)."[117]

c. Rights of Data Subject

1) *Right of Access*: Every data subject has the right to obtain from the controller "confirmation as to whether or not data relating to him are processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed."[118]

2) *Correct/Block Information*: Every data subject has the right to obtain from the controller "the rectification, erasure, or blocking of data, the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data."[119]

---

114. *Id.* at art. 7(d).

115. "Third party" is defined as "the natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process data." *Id.* at art. 2(f).

116. *Id.* at art. 7(e).

117. *Id.* at art. 7(f).

118. *Id.* at art. 12, para. 1.

119. *Id.* at art. 12, para. 2.

3) *Right to Object*: Every data subject has the right "to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him."[120]

d. Security

The Directive requires the Member States to "implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss and against unauthorized alteration, disclosure or access."[121] The appropriate level of security is determined by balancing the nature of the data against the amount of risk involved in the processing of that data.[122]

2. Transfer of Personal Data to Third Countries

The Directive not only governs the movement of personal data between European Union Member States, but also the transfer of such data to third countries (Non-European Union). Article 25 of the Directive permits the transfer of personal data to third countries only if the recipient country in question ensures an "adequate" level of protection.[123] The Member States determine whether a third country has an adequate level of protection based on all the factors surrounding a data transfer operation, particularly taking into account the nature of the data, the proposed processing operation's duration, and the existence of data protection laws and security measures in the third country.[124]

Under certain conditions, however, the Directive allows Member States to transfer personal data to a third country that does not meet the adequate level of protection.[125] Such transfers may take place if one of the following conditions are met:

---

120. *Id.* at art. 14(a).
121. *Id.* at art. 17, para. 1.
122. *See id.*
123. *See id.* at art. 25, para. 1.
124. *See id.* at art. 25, para. 2.
125. *See id.* at art. 26, para. 1.

1) *Consent*: The data subject unambiguously consents to the proposed transfer.[126]

2) *Contract with Data Subject*: The transfer is necessary for the performance of a contract with the data subject or for the execution of a contract at the request of the data subject.[127]

3) *Contract with Third Party*: The transfer is necessary for the conclusion or the performance of a contract with a third party in the data subject's interest.[128]

4) *Public Interest/Legal Claims*: The transfer is necessary because of important public interest or for the exercise, establishment, or defense of legal claims.[129]

5) *Interests of Data Subject*: The transfer is necessary for the protection of the vital interests of the data subject.[130]

6) *Public register*: The transfer is made from a public register according to the applicable laws and regulations.[131]

V. EFFECT OF EUROPEAN UNION DIRECTIVE ON THE UNITED STATES

The European Union views data privacy as a fundamental right that is best protected by legislation and federal policing.[132] The United States, in contrast, relies largely on a self-regulatory approach to effective data privacy and protection.[133] It was inevitable that this underlying difference in ideologies would lead to a confrontation between the European Union and the United States regarding the transfer of personal data.

The cornerstone of this struggle lies in Article 25 of the European Union Directive that became effective on October 25,

---

126. *See id.* at art. 26, para. 2(1).
127. *See id.* at art. 26, para. 2(2).
128. *See id.* at art. 26, para. 2(3).
129. *See id.* at art. 26, para. 2(4).
130. *See id.* at art. 26, para. 2(5).
131. *See id.* at art. 26, para. 2(6).
132. *See European Directive Impact, supra* note 99.
133. *See id.*

1998. This Article prohibits data transfers to any country lacking an "adequate" level of protection, as determined by the European Union.[134] In the European Union's opinion, the United States is one country that does not meet its standards for the protection of data privacy.

If the United States is unable to meet the European Union standard of adequacy and the Directive is strictly enforced, the resulting conflict will have severe implications for the millions of data transfers occurring via the Internet between the United States and Europe every day. For example, a United States credit card company may be unable to bring the financial profile of an Italian customer back to its Los Angeles data processing facility. Likewise, a United States firm will face problems when trying to transfer the records of a European employee back to the head office in New York. Similar complications will arise in various other sectors of industry where personal data is gathered and processed. This includes the press, educational institutions, telephone networks, health care, airlines, direct marketing, and banking.[135]

Fortunately for these industries, the European Union temporarily agreed not to disrupt the flow of data between Europe and the United States.[136] The United States Department of Commerce and European Commission are currently attempting to negotiate a compromise in order to continue the flow of data between the two territories. The United States has proposed a voluntary approach for U.S. companies to meet the requirements of the European Union Directive, thereby deeming them "adequate" for the purposes of data transfers. Under this proposal, a "safe harbor" would be created for those U.S. companies that choose to adhere to certain privacy principles.[137] These so-called "safe harbor principles" deal with the areas of notice, choice, onward transfer, security, data integrity, access, and

---

134. *See* Directive, art. 25, para. 1.

135. *See European Privacy Law May Threaten U.S. Businesses, Expert Says* (visited Jan. 17, 1999) <http://www.osu.edu/osu/newsrel/Arc_ould_Threaten_U.S._Businesses.html>.

136. *See EU Agrees Not to Interrupt Data Flow for Time Being* (visited Nov. 9, 1998) <http://www.mediacentral.com?Magazi_ne?Archive?1998102801.htm>.

137. *See* U.S. Department of Commerce (last modified Nov. 4, 1998) <http://www.epic.org/privacy/intl/ doc-safeharbor-1198.html>.

enforcement.[138] The United States and European Union still disagree on various parts of the proposal, particularly the areas of access and enforcement.[139]

Despite widespread agreement on the importance of privacy and data protection, vast differences remain between the U.S. and European positions. Consequently, negotiations regarding U.S. compliance with the European Union Directive will apparently continue well into 1999.

VI. CONCLUSION

The development of the Internet has dramatically increased the quantity of information available in digital form. Our ability to acquire, process, send, and store this information has never been greater. Continuing advances in computer technologies will only enhance this capability.

The Internet promises enormous benefits. To name just a few, it offers the possibilities of purchasing a variety of products from around the world without ever leaving home, quickly and

---

138. The "Safe Harbor Principles" are:

1) *Notice*: An organization must inform individuals about what types of information it collects about them, how it collects that information, the purposes for which it collects such information, the types of organizations to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure.

2) *Choice*: An organization must give individuals the opportunity to choose (opt out choice) whether and how personal information they provide is used.

3) *Onward Transfer*: Individuals must be given the opportunity to choose the manner in which a third party uses the personal information they provide.

4) *Security*: Organizations creating, maintaining, using or disseminating records of personal information must take reasonable measures to assure its reliability for its intended use and must take reasonable precautions to protect it from loss, misuse, unauthorized access or disclosure, alteration, or destruction.

5) *Data Integrity*: An organization must keep personal data relevant for the purposes for which it has been gathered only. To the extent necessary for those purposes, the data should be accurate, complete, and current.

6) *Access*: Individuals must have reasonable access to information about them derived from non-public records that an organization holds and be able to correct or amend that information where it is inaccurate.

7) *Enforcement*: Effective privacy protection must include mechanisms for assuring compliance with the principles, recourse for individuals, and consequences for the organization when the principles are not followed.

Id.

139. *See* Courtney Macavinta, *EU-US Privacy Dispute Won't End Soon* (visited Jan. 14, 1999) <http://www.news.com/News/Item/0,4,30020,00.html>.

efficiently retrieving vast amounts of information on virtually any subject, advertising businesses and products to customers in different cities, states, and countries, and communicating with friends across the globe without ever picking up the phone or mailing a letter. These benefits, however, do not come without a price: the loss of privacy.

As a technological society, we cannot totally guarantee everyone's privacy. But imagine a world in which you had the right to obtain and confirm the accuracy of every piece of information being compiled about you, in which you had the right correct, erase, or block any personal data that was incomplete or inaccurate, and in which companies were barred from selling data about you without your consent. On October 25, 1998, that world effectively came into existence for the citizens of the European Union.

If only the United States had such imagination.

*Domingo R. Tan**

* J.D. candidate, Loyola Law School, 2000; B.A., Economics, *cum laude,* Loyola Marymount University, 1997. I dedicate this Comment to my mom, Imelda, who has been a constant source of love, inspiration, and support throughout my life. I also want to thank the other important women in my life: my aunt and second mother, Ampy, my two sisters, Marlo and Christina, and my best friend Shalee. I love you all. Special thanks to my dad and personal guardian angel who watches over me every day.