5-1-2000

At the Intersection of Visible and Invisable Worlds: United States Privacy Law and the Internet

Dorothy J. Glancy
Santa Clara University School of Law, dglancy@scu.edu

AT THE INTERSECTION OF VISIBLE AND INVISIBLE WORLDS: UNITED STATES PRIVACY LAW AND THE INTERNET

Professor Dorothy Glancy[†]

TABLE OF CONTENTS

I. INTRODUCTION

"You already have zero privacy—get over it," warned Scott McNealy, chief executive of Sun Microsystems at the launch of his company's Jini consumer networking software.[1] In fact, laws protecting privacy are everywhere in the United States. These privacy laws intersect with the Internet in more ways than even Mr. McNealy might imagine. The problem is that thinking about how United States privacy law interacts with the Internet can be perplexing. Just as the British poet, Stephen Spender wondered at "understanding the intersection of visible with invisible worlds," observers of privacy and the Internet can be bewildered by the complexity of the intersecting elements. Of course, unlike Spender's image, aspects of invisibility and visibility, concreteness and abstraction, are woven into both the Internet and privacy laws.

The purpose of this essay is to consider some characteristics of

† Professor of Law, Santa Clara University School of Law; B.A. Wellesley College; J.D. Harvard Law School. This essay is based on remarks prepared for the symposium, *Privacy in the Next Millennium*, February 11-12, 2000 at Santa Clara University.

1. John Markoff, *Growing Compatibility Issue: Computers and User Privacy*, N.Y. TIMES, Mar. 3, 1999, at A1.

United States privacy law that contribute to the obscurity of many intersections between the Internet and privacy law. This discussion is not an exhaustive catalogue of all of the ways in which United States privacy law may apply to Internet activities. Nor is it intended to be an evaluation of the effectiveness of this privacy law. Rather, the point here is to explore why the application of privacy law to the Internet is a matter of considerable complexity and some uncertainty. The focus is on certain characteristics of privacy law that can mislead even very smart people into believing that privacy is not here.

Both the Internet and United States privacy law operate in varied ways across many dimensions. Just as the Internet is an interconnection of digital networks that operates in multiple ways to communicate data and other information worldwide, United States privacy law embraces many types of laws that protect and vindicate individual self-determination with regard to personal activities, private decisions, and personal information about an individual.[2] With regard to the Internet, a varied assortment of privacy laws function in different ways to protect and to vindicate individual control over personal activities, decisions, and information. The complexities of the potential interactions between privacy law and the Internet may be difficult to visualize. But it is a mistake to count privacy, and the laws which protect it, as zero.

II. THREE CHARACTERISTICS OF UNITED STATES PRIVACY LAW

Three main characteristics of United States privacy law help to explain why it can be difficult to understand how privacy law intersects with the Internet. First, United States privacy law is diverse. Second, United States privacy law is decentralized. Third, United States privacy law is dynamic. As privacy law has evolved over the past century or so, these characteristics have resulted in a myriad of specific privacy laws applicable in the United States. Only a few of the details of these privacy laws can be noted here.

Consider an average Internet user, Irene.[3] During a typical week,

2. Warren & Brandeis first described the right to privacy as a right to an "inviolate personality." *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy,* 4 HARV. L. REV. 193, 205 (1890). The article argued that: "The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others... fix[ing] the limits of the publicity which shall be given to them." *Id.* at 198.

3. See results of a recent study by the Stanford Institute for the Quantitative Study of Society. Norman H Nie & Lutz Erbing, *Internet and Society: A Preliminary Report* (visited Feb. 18, 2000) <http://www.stanford.edu/group/siqss>. The survey was based on a nationwide

Irene is on-line for five hours or so, reading and sending e-mail to friends and business associates, doing research and writing reports. Sometimes Irene participates in Internet auctions or purchases books or airline tickets from Internet companies. She subscribes to a couple of Usenet groups and occasionally visits chat rooms and on-line forums. Irene probably believes that her Internet activities are private. But she is most likely unaware of the multitude of privacy laws applicable to her activities on the Internet. Although these privacy laws may not perfectly protect Irene's on-line privacy,[4] if Irene were aware of the many ways in which privacy laws affect her on-line, she would be amazed.[5]

A. *Diverse*

Understanding United States privacy law begins with the recognition that privacy law is not an "it." Instead, United States privacy law is a very diverse collection of many different types of privacy laws. The tendency of these privacy laws to focus on specific, even narrow, privacy concerns or contexts has generated widespread criticism of privacy laws in the United States as "piecemeal" or fragmented.[6] A number of years ago a federal appeals court judge described United States privacy law as like a "haystack in a hurricane."[7] In an opinion for the United States Supreme Court, Chief Justice Rehnquist criticized privacy as "defying categorical description."[8] Even the distinguished privacy advocate, Arthur R.

random sample of 4,113 individuals over the age of 18 in 2,689 households. Over a third (36%) of those responding reported being on-line at least five hours each week. Almost half of the respondents reported Internet use of between one and five hours per week. *See* John Markoff, *A Newer, Lonelier Crowd Emerges in Internet Study*, N.Y. TIMES, Feb. 16, 2000, at A1 fig.

4. Indeed, aspects of privacy law may well be antiquated, out of sync with modem life, not to mention Internet technologies. Since most privacy law was not designed with the Internet in mind, loopholes and misfits are to be expected. However, privacy law's many imperfections are not the focus of this discussion. Rather the point here is to demonstrate that, although a great deal of privacy law does apply to Irene's on-line activities, understanding that privacy law can be difficult.

5. Professor Lawrence Lessig has ably addressed different, but no less intriguing, issues regarding the architecture of the Internet and whether the Internet is being designed and built with acceptable respect for privacy values in mind. *See generally* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999). Chapter 11 discusses the value of privacy and the importance of building it into the architecture of the Internet. *See id.* at 142-63.

6. Almost every imaginable imagery of a heterogeneous mixture has been used to describe United States privacy law. Many of these metaphors seem to be based on food—from hodgepodge (stew) to succotash (mixed vegetables).

7. Ettore v. Philco Television Broadcasting Corp., 229 F.2d 481, 485 (3d Cir. 1956), *cert. denied* 351 U.S. 926 (1956).

8. Paul v. Davis, 424 U.S. 693, 713 (1976).

Miller, described United States privacy law as "a thing of threads and patches."[9] And yet the very diversity that makes privacy law seem difficult to pin down also contributes to its vitality and makes its application to the Internet interesting.

Three aspects of the diversity of United States privacy laws are particularly important: (i) the tendency of modern privacy law to divide into at least two main branches of privacy interests: privacy concerns about autonomy and privacy concerns about personal information; (ii) the variety of different types of privacy laws; and (iii) the specific, context-dependent nature of many privacy laws. These characteristics of privacy law account for much of the internal diversity and complexity of United States privacy law.

1. Autonomy and Personal Information

As United States privacy law evolved over the past century, two general branches developed. These two branches reflect what are perceived to be different types of privacy concerns: On the one hand, privacy law is concerned about an individual's autonomous control over personal activities and decisions. On the other hand, privacy law is also concerned about an individual's control over personal information about that individual.[10] For example, the California Supreme Court has described the guarantee of an "inalienable right to privacy" in the California constitution as divided into two separate areas of privacy interests: "(1) interests in precluding the dissemination or misuse of sensitive and confidential information ('informational privacy'); and (2) interests in making intimate personal decisions or conducting personal activities without observation, intrusion or interference ('autonomy privacy')."[11] Depending on the category into which a particular privacy case fits, a different privacy analysis applies.

Although often treated as separate categories, autonomy privacy and informational privacy are in fact intimately intertwined, particularly when privacy law intersects with the Internet. For example, assume that our average Internet user, Irene, objects to

9. ARTHUR R. MILLER, THE ASSAULT ON PRIVACY 169 (1971).

10. In *Whalen v. Roe*, 429 U.S. 589, 598-99 (1977), Justice Stevens noted that: "The cases sometimes characterized as protecting 'privacy' have in fact involved at least two different kinds of interests. One is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions."

11. Hill v. National Collegiate Athletic Ass'n, 7 Cal. 4th 1, 35, 865 P.2d 633, 654, 26 Cal. Rptr. 2d 834, 856 (1994); *see also* discussion in *American Academy of Pediatrics v. Lungren*, 16 Cal. 4th 307, 332, 940 P.2d 797, 812, 66 Cal. Rptr. 2d 210, 225 (1997) (plurality opinion).

surreptitious electronic surveillance of her Internet activities through the collection of personal information about her on-line activities. Such an objection is partly classified as a concern about autonomy privacy—her ability to control her life and her choices about how to live that life. This privacy concern is about her "right to be let alone," frequently associated with the autonomy right to privacy.[12] At the same time, Irene is also concerned about whether personal information about her is stored, manipulated, connected up with other information or disseminated to others. For example, Irene may well be concerned about a marketing company's collecting information about the web sites she visits, about the company's manipulating this information into an "Irene" on-line profile, about the company's connecting that profile with other information (such as her address and telephone number), and also about the company's selling the whole consumer picture of Irene to a marketing firm. These informational privacy concerns are, of course, interrelated with her autonomy privacy concerns. Internet users, such as Irene, object to collection of information about their on-line activities both because such surveillance interferes with their individual autonomy and because they have an informational privacy interest in controlling the use of such information. Nevertheless, United States privacy law often places these concerns in separate categories and applies different analysis to each of them.

Because the Internet is an information network, most Internet observers look at Internet activities as involving primarily informational privacy concerns about controlling the collection, storage, manipulation, and dissemination of personal information. For example, Irene is concerned about unauthorized disclosure of her credit card numbers or her bank account balance. But such concerns are only part of the picture. In fact, for Irene and other Internet users, autonomy privacy interests in preventing the collection of such information in the first place may well be of even greater practical importance. After all, personal information that is not collected cannot be stored, manipulated or disclosed.

Autonomy privacy interests are often associated with such issues as decisions regarding contraception[13] and abortion.[14] But autonomy

12. *See* Warren & Brandeis, *supra* note 2, at 195. The notion of a "right to be let alone" is usually attributed to Judge Thomas Cooley, who described it as "[t]he right to one's person may be said to be a right of complete immunity: the right to be let alone." THOMAS M. COOLEY, COOLEY ON TORTS 29 (1879).

13. *See, e.g.*, Griswold v. Connecticut, 381 U.S. 479 (1965).

14. *See, e.g.*, Roe v. Wade, 410 U.S. 113 (1973).

privacy also extends to an individual's self-determination regarding who will have how much access to that individual.[15] In the Internet context, Irene's autonomy privacy concerns include her ability to control whether or not her purchases of various types of goods and services from Internet sites are compiled into her consumer profile, since that profile is likely to be a "stand-in" or alter-ego for her with regard to future transactions. Autonomy privacy concerns also arise when censors or snoopers interfere with Irene's choices to send and to receive information over the Internet.[16] Surreptitious surveillance of Irene's Internet activities, for example through "cookies" or by creation of an on-line profile of her browsing habits, also raise autonomy concerns about her privacy on the Internet. Another example of autonomy privacy is Irene's choice to visit web sites anonymously. She might, for example, decide to participate in a Usenet group for expectant mothers under a pseudonym without revealing her actual identity. Irene might also choose to interact with the Internet through a persona or avatar. Her screen name might be "Inez" or "Ike" in a chat room, for example. Such autonomous self-redefinition illustrates a slightly different, and controversial, form of autonomy privacy, sometimes called anonymity[17] or pseudonymity. Although privacy tort actions have for a long time protected an individual's autonomy privacy right to self-definition and redefinition,[18] the extent to which such autonomy privacy concerns

15. The initial argument for recognizing a right of privacy in the United States defined privacy as based on the principle of "an inviolate personality" associated with "the right to be let alone." Warren & Brandeis, *supra* note 2, at 205; *see also* Dorothy J. Glancy, *The Invention of the Right to Privacy*, 21 ARIZ. L. REV. 1, 21-28 (1979).

16. *See* Stanley v. Georgia, 394 U.S. 557 (1969). In this case involving the seizure of obscene film from a person's home, Justice Marshall insisted that the

> Right to receive information and ideas, regardless of their social worth, is fundamental to our free society .... [T]he right to be free, except in very limited circumstances, from unwanted governmental intrusions into one's privacy .... If the First Amendment means anything, it means that a State has no business telling a man, sitting alone in his own house, what books he may read or films he may watch. Our whole constitutional heritage rebels at the thought of giving government the power to control men's minds.

Id. at 564-65.

17. *See generally* Anne W. Branscomb, *Anonymity, Autonomy, Accountability: Challenges to the First Amendment in Cyberspaces*, 104 YALE L.J. 1639 (1995).

18. *See, e.g.*, Melvin v. Reid, 112 Cal. App. 285, 297 P. 91 (1931). This damage action for invasion of privacy was brought in the 1930s by a reformed prostitute against film makers who made a movie, "The Red Kimono," in which they used both the facts of her former life as a prostitute and her maiden name. The court found that, having reformed and redefined herself as a respectable married woman, she had a recognizable cause of action based on "the right to live one's life in seclusion, without being subjected to unwarranted and undesirable publicity. In

can or should be translated into privacy law applicable to the Internet remains controversial.[19]

2. Reasonable Expectations of Privacy

Legal protections for both autonomy privacy interests and informational privacy interests often depend in part on whether expectations of privacy are considered reasonable in a particular setting.[20] For example, legal protection for Irene's privacy is likely to depend in part on whether she reasonably expects privacy when she accesses the Internet. Since Internet users, such as Irene, would be reluctant to log onto the Internet if they could not reasonably expect at least some degree of privacy with regard to their on-line activities, they appear to have at least some reasonable expectation of privacy on the Internet. Assurances of privacy protection by e-commerce vendors[21] and Internet service providers[22] demonstrate that the

short, it is the right to be let alone." *Id.* at 289, 297 P. at 92 (1931).

19. Objections to Internet anonymity are typically based on concerns about the potential for untraceable criminal activity such as money laundering, misappropriation of intellectual property, or drug trafficking. *See* United States Department of Justice, THE ELECTRONIC FRONTIER: THE CHALLENGE OF UNLAWFUL CONDUCT INVOLVING THE USE OF THE INTERNET, (Mar. 2000) <http://www.usdoj.gov/criminal/cybercrime/unlawful.htm> (Report of the President's Working Group on Unlawful Conduct on the Internet).

20. *See, e.g.*, Katz v. United States, 389 U.S. 347 (1967). Katz was a wiretapping case involving Fourth Amendment objections to interception of Katz's telephone calls from a public telephone booth. The majority opinion is famous for its ruling that the privacy protections in the Fourteenth Amendment protect "people and not simply 'areas.'" *Id.* at 353. Justice Harlan stated in his concurring opinion that whether there was a search for Fourth Amendment purposes depended on two factors, "first, whether the person involved exhibited an actual, subjective, expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable'." *Id.* at 361 (Harlan, J., concurring).

21. For example, American Express begins its Internet Privacy Statement with the assertion: "Protecting your privacy is important to us." *American Express Customer Internet Privacy Statement* (visited Apr. 2, 2000) <http://home3.americanexpress.com/corp/consumerinfo/privacy/privacystatement.asp>. The "Lycos Privacy Policy" page features not only a statement about Lycos's subscription to the TRUSTe privacy protection program but also "Our Privacy Vow." *See Lycos Privacy Page* (visited Apr. 2, 2000) <http://www.lycos.com/privacy/>. Unfortunately the content of this "privacy vow" seems to have more to do with collecting information than with respecting privacy. The vow states:

> Our goal at Lycos is to be 'Your Personal Internet Guide' by providing you with the information and services that are most relevant to you. To achieve this goal, we need to collect information to understand what differentiates you from each of our millions of other unique users. We collect this information in two ways.

Id.

The bottom line of the Lycos Privacy Policy, its last element, is entitled "Delete/Delist," and states, "[i]t is not currently possible for a Lycos customer to delete his or her information from the database." *Id.* A personal request to be removed from the database will, however, be honored, according to the Lycos Privacy Policy. *See id.*

commercial side of the Internet recognizes that respect for privacy is a significant expectation of Internet users.

Although the Internet may appear to some as a wide open and not very private environment, not every bit of digital data on the Internet is open to anyone who knows how to access it.[23] For example, encryption, fire walls and other data security techniques can make certain Internet information inaccessible as a practical matter. Moreover, simply declaring the Internet non-private does not necessarily make it so;[24] nor does such a declaration eliminate reasonable privacy expectations on the part of Internet users. In reality, Internet users, such as Irene, reasonably expect some degree of privacy on the Internet, both because they are repeatedly assured that their privacy is being respected, and because privacy laws of many types protect and vindicate privacy rights with regard to both their autonomy and their control over personal information.

3. Types of Privacy Laws

Many types of privacy laws, both civil and criminal, protect and vindicate privacy interests in the United States. Although mostly developed before the Internet, these various types of privacy laws can apply to on-line activities of Internet users. A detailed description of all of these types of privacy laws is beyond the scope of this essay. But it is useful to highlight some of the major types including constitutional law, common law, statutory law, regulatory law, as well as self-regulatory measures.

22. For example, see AOL's "Privacy Policy," which states "America Online, Inc. is strongly committed to protecting the privacy of consumers of its interactive products and services." *AOL.com, Privacy Policy* (visited Apr. 2, 2000) <http:\\www.aol.com/info/privacy.html>.

23. Lawrence Lessig has argued that the Internet can and should be even better organized and constructed to respect privacy. *See* LESSIG, *supra* note 5, at 142-63 (discussing the issue of privacy in Chapter 11).

24. The United States Supreme Court frowned on what the Court called "conditioning" expectations of privacy in *Smith v. Maryland*, 442 U.S. 735, 740 (1979) (finding no search when the government used a pen register to record numbers dialed from a telephone). In a footnote, the Court noted that the government cannot eliminate legitimate expectations of privacy by suddenly

> [A]nnounc[ing] on nationwide television that all homes henceforth would be subject to warrantless entry [so that] individuals thereafter might not in fact entertain any actual expectation of privacy regarding their homes, papers, and effects .... In such circumstances, where an individual's subjective expectations had be 'conditioned' by [extraneous] influences ... a normative inquiry would be proper.

Id. at 740 n.5.

As an example, consider the privacy laws applicable to electronic surveillance of Irene's Internet activities of the complex layers of different types of privacy laws. Irene is logged on to the Internet at home through a modem. Assume that Gill, a law enforcement officer, intercepts Irene's Internet communications, without a warrant or intercept order, and records Irene's e-mail messages and Internet transactions without her knowledge or consent. Gill's invasion of Irene's privacy is illegal under federal statutes prohibiting wiretapping without a warrant, as well as under the Fourth Amendment to the United States Constitution and other civil and criminal laws regulating electronic surveillance by government agencies and agents.[25] Assume further that Paul, a private investigator, similarly taps and records Irene's on-line communications and transactions. Paul's invasion of Irene's Internet privacy would subject Paul to both civil and criminal penalties under different provisions of federal electronic surveillance statutes, as well as under privacy laws of most states.[26] As will be discussed further with regard to the decentralized nature of privacy law, a combination of both federal and state privacy laws, including both civil and criminal statutes and state common law, would make electronic surveillance of Irene's Internet communications illegal on many levels.

Of the various types of privacy laws, those relating to constitutional privacy rights are probably the most controversial.[27] According to Justice William O. Douglas's expansive view of constitutional rights to privacy, the penumbras of several provisions

25. *See, e.g.*, Electronic Communications Privacy Act, 18 U.S.C. §§ 2701-2711 (1994); Privacy Protection Act, 42 U.S.C. §§ 2000aa to 2000aa-12 (1994); McVeigh v. Cohen, 983 F. Supp. 215 (D.D.C. 1998). Gill may also be in violation of state constitutional provisions and statutes. *See, e.g.*, CAL. CONST. art. 1, § 13; CAL. PENAL CODE § 630 (West 1999).

26. Federal statutes include the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-2522 (1994) and the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (1994). An example of a state criminal statue penalizing wiretapping is CAL. PENAL CODE § 631 (West 1999). The common law tort of intrusion, discussed *infra* at notes 36, 47-55, may also provide a basis for damage liability.

27. The reasons for the controversial status of federal constitutional privacy rights are many. *See* Dorothy J. Glancy, *Douglas's Right of Privacy: A Response to His Critics*, *in* "HE SHALL NOT PASS THIS WAY AGAIN:" THE LEGACY OF JUSTICE WILLIAM O. DOUGLAS 155 (Stephen L. Wasby ed., 1990). In the first place, the United States Constitution does not contain the word "privacy." Moreover, there is a broad range of many types of implicit constitutional privacy rights—from rights to receive information to rights to make decisions about procreation. Some of these privacy rights involve matters of deep-seated social and religious disagreement. For a critical discussion of Douglas' expansive view of the constitutional right of privacy see William H. Rehnquist, *Is an Expanded Right of Privacy Consistent with Fair and Effective Law Enforcement?*, 23 U. KAN. L. REV. 21 (1974).

of Bill of Rights, including the First, Third, Fourth, Fifth, and Ninth Amendments, and the Fourteenth Amendment as it applies to the states, all protect privacy.[28] These federal constitutional privacy rights are safeguarded against governmental action interfering with an individual's privacy. Most of them focus on the autonomy branch of privacy law. For example, Gill's warrantless electronic surveillance of Irene's Internet activities would violate her Fourth Amendment right against unreasonable searches.[29] In addition, government interference with Irene's rights to unhindered communication with others, and against surveillance of her reading habits would most likely be unconstitutional under the First Amendment. Regarding government collection of personal information about Irene's Internet activities and storing it in a database, the United States Supreme Court has suggested that, government mandated databases of personal information where the information is not lawfully collected nor adequately safeguarded, may violate federal constitutional privacy guarantees.[30]

Most state constitutions contain search and seizure provisions similar to those in the federal constitution.[31] A few state constitutions also contain provisions explicitly protecting privacy. For example, the California Constitution expressly guarantees "an inalienable right to privacy."[32] Moreover, California's state constitutional privacy provision applies broadly to prohibit interference with privacy both by governmental and by private-sector invaders.[33]

As a result, if Irene were on-line in California, her Internet activities would be protected under California's constitution against both misuse of personal information about her and interferences with her autonomy. This state constitutional privacy protection would apply to invasions of privacy both by government agents, such as

28. *See, e.g.*, Griswold v. State of Connecticut, 381 U.S. 479 (1965) (holding unconstitutional a Connecticut criminal statute which penalized the distribution of birth control information or devices to married persons).

29. *See* Katz v. United States, 389 U.S. 347 (1967).

30. *See* Whalen v. Roe, 429 U.S. 589, 605 (1977). Justice Stevens' majority opinion included "[a] final word about issues we have not decided. We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files." *Id. Cf.* Nixon v. Administrator of General Services, 433 U.S. 425 (1977) (concerning former president's constitutional privacy interest in avoiding disclosure of personal matters).

31. *See, e.g.*, CAL. CONST. art. 1, § 13.

32. *Id.* § 1.

33. *See* Porten v. University of San Francisco, 64 Cal. App. 3d 825, 134 Cal. Rptr. 839 (1976).

Gill, and by private investigators, such as Paul.

A second type of privacy law is part of the common law of torts. The origins of common law protection for privacy in the United States date back to a famous 1890 law review article, *The Right to Privacy*, largely written by Louis Brandeis, later a United States Supreme Court Justice.[34] Almost all states now allow such damage actions for invasion of privacy. In fact, the common law of most states recognizes four different privacy torts. The Restatement (Second) of Torts Sections 652A—652I, adopted by the American Law Institute in 1977 provides a conventional description of the four privacy torts:[35]

- Unreasonable intrusion upon seclusion (commonly referred to as "Intrusion")[36]
- Appropriation of another's name or likeness (commonly referred to as "Appropriation")[37]
- Unreasonable Publicity given to another's private life (commonly referred to as "Private Facts")[38]
- Publicity unreasonably placing another person in a false light (commonly referred to as "False Light")[39]

These four privacy torts are "personal" in the sense that only the living individual whose privacy has been invaded has the right to bring a lawsuit based on them.[40] Privacy tort actions are also generally limited by absolute and conditional privileges similar to those applicable in defamation actions, such as consent and First Amendment protection for freedom of expression.[41] In most cases involving these privacy torts, liability requires the privacy invasion to have been unreasonable.

34. Warren & Brandeis, *supra* note 2. The article described invasion of privacy as interference with an individual's "inviolate personality" and argued that the common law should allow damage actions to redress and punish invasions of privacy. *See id.* at 198, 205. *See generally* Glancy, *supra* note 15.

35. RESTATEMENT (SECOND) OF TORTS §§ 652A-I (1977). The Restatement (Second) of Torts [hereinafter "Restatement"] categories reflect an analysis of privacy cases by William Prosser, who was the Reporter for that Restatement. *See generally* William L. Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960).

36. RESTATEMENT (SECOND) OF TORTS § 652B (1977).

37. *Id.* § 652C. Sometimes this privacy tort is described as vindicating a right to publicity.

38. *Id.* § 652D.

39. *Id.* § 652E.

40. *See id.* § 652I. In some states, statutes provide for the survival of privacy tort causes of action. *See, e.g.*, CAL. CIV. CODE § 3344.1 (West 2000).

41. *See* RESTATEMENT (SECOND) OF TORTS §§ 652F-652G (1977).

So far, only a few reported decisions have applied the Restatement's categories of common law privacy torts to the Internet, and only in regards to the Fourth and Fifth Amendments.[42] In the context of computer networks, reported decisions include *Wood v. National Computer Systems, Inc.*[43] and *Morrow v. II Morrow, Inc.*[44] In both of these cases, summary judgment for defendants was held appropriate because the allegedly privacy-invading material was not sufficiently published to the public at large, but rather was disclosed within a restricted network. Although distribution on a local area network (LAN) might not satisfy the "publication" required for liability under the privacy torts involving publicity, Internet distribution of information does seem to provide sufficient publicity for the appropriation, private facts and false light privacy torts. For example, in *Michaels v. Internet Entertainment Group, Inc.*, the Federal District Court granted a preliminary injunction preventing an adult entertainment Internet content provider from distributing over the Internet a videotape of celebrity plaintiffs, Bret Michaels and Pamela Anderson Lee, engaged in sexual activity.[45]

It is interesting to consider how each of the common law privacy torts might apply to an Internet user such as Irene, who is accessing the Internet from her home.[46] For the purposes of the intrusion privacy tort, whether or not Irene can be said to have seclusion on the Internet depends in part on the extent to which the Internet can be considered a private place. Generally, the Restatement's concept of seclusion depends on whether a plaintiff's expectations of privacy are reasonable in that particular setting.[47] Public opinion polls about privacy concerns with regard to Internet activities seem to suggest that at least some on-line activities, such as those involving healthcare information or personal financial information communicated in e-

42. *See, e.g.*, Davis v. Gracey, 111 F.3d 1472 (10th Cir. 1997); McVeigh v. Cohen, 983 F. Supp. 215 (D.D.C. 1998).

43. 643 F. Supp. 1093, 1098 (W.D. Ark. 1986) (teacher's competency examination report mistakenly sent to another teacher did not constitute public disclosure of private facts).

44. 139 Or. App. 212, 911 P.2d 964 (Or. App. 1996) (false-light invasion of privacy action against employer who posted critical evaluation of employee on hard drive accessible company-wide was not established because employer did not distribute personal information to public generally).

45. 5 F. Supp. 2d 823 (C.D. Cal. 1998). Although the preliminary injunction was based on both invasion of privacy and copyright infringement, the court specifically found that the plaintiffs were likely to prevail on privacy claims based on appropriation and publicity given to private life. *See id.* at 840.

46. Different privacy law analysis would apply if Irene were on-line in her employer's offices.

47. *See* discussion *supra* notes 20-24.

commerce transactions, are considered reasonably secluded.[48] The commentary to Restatement Section 652B suggests that protected seclusion covers "private concerns" such as an individual's "private and personal mail, searching his safe or his wallet, examining his private bank account."[49] It seems unlikely that the Internet venue for such matters as personal mail or personal bank account records would render such information any less secluded. The illustration to the Restatement section 652B that focuses on repeated annoying promotional telephone calls to a person's home despite repeated requests to desist seems to suggest that personally targeted "push" technology might constitute an unreasonable intrusion on seclusion.[50] Even if the Internet were considered a public place, the intrusion privacy tort[51] may still apply in cases of intrusion into "a private seclusion that the plaintiff has thrown about his person or affairs."[52] The comment to this part of the Restatement notes that: "Even in a public place . . . there may be some matters about the plaintiff, such as his underwear or lack of it, that are not exhibited to the public gaze; and there may still be invasion of privacy when there is intrusion upon these matters."[53] There are often issues regarding consent in intrusion cases.[54] But the privacy tort that vindicates seclusion generally requires that the determination of the individual be respected with regard to matters that the particular individual considers personal.[55]

Irene's status as an Internet user does not affect her general privacy right to prevent having her name or likeness appropriated for the use or benefit of someone else.[56] Most of the decisional law regarding tort liability for invasion of privacy by appropriation involves commercial use, such as advertising. When commercial use

48. *See, e.g.*, Mary J. Culnan, GEORGETOWN INTERNET PRIVACY POLICY STUDY: REPORT TO THE FEDERAL TRADE COMMISSION (Mary J. Culnan, study director, 1999); Janlori Goldman et al., PRIVACY: REPORT ON THE PRIVACY POLICIES AND PRACTICES OF HEALTH WEB SITES (Feb. 2000) <http://ehealth.chcf.org/priv_pol3/index_show.cfm?doc_id=333>. As noted, *supra* notes 21-22, privacy policies, vows and assurances by Internet companies reinforce expectations of seclusion. Images of locks visually enhance such an expectation of privacy.

49. RESTATEMENT (SECOND) OF TORTS § 652B cmt. b (1977).

50. *Id.* at illus. 5.

51. *See* RESTATEMENT (SECOND) OF TORTS § 652B cmt. b (1977)..

52. *Id.* at cmt. c.

53. *Id.*

54. *See* RESTATEMENT (SECOND) OF TORTS § 652F cmt. b. (1977).

55. *Cf.* Massachusetts v. Source One Assoc., Inc., No. CIV.A.98-0507-H, 1999 WL 975120 (Mass. Super. Oct 12, 1999) (unauthorized acquisition of personal financial information).

56. *See* RESTATEMENT (SECOND) OF TORTS § 652C (1977).

of a person's name or likeness takes place on-line, the liability analysis developed in cases involving other commercial media would apply. For example, using Irene's picture on BrowserCo's web site as the image of a "happy BrowserCo user" without her consent would probably be actionable. In addition, as commentary to the Restatement suggests, there may be liability for appropriation of Irene's personality even in the absence of commercial use "and even though the benefit sought to be obtained is not a pecuniary one."[57] According to the Restatement, passing oneself off as someone else or "otherwise seek[ing] to obtain for [one]self the values or benefits of the plaintiff's name or identity," is actionable.[58] If another person uses Irene's identity to gain benefits, such as credit from an Internet retailer, or to gain access to valuable Internet services to which Irene is a subscriber, that person may be liable for invading Irene's privacy for appropriating her name or likeness.

There are a number of unanswered questions regarding application of the appropriation privacy tort in the Internet context. For example, whether Irene's "personal image" in the form of her on-line profile of browsing habits and purchasing patterns constitutes a likeness of her for the purposes of the appropriation privacy tort remains an open question.[59] The privacy rights of an Internet user, such as Irene, to consent or not to consent to transfers of her on-line profile by Internet retailers or marketing firms is central to the debate over opt-in, as opposed to opt-out, consumer control over information reflecting a person's Internet use. Whether Internet users in the United States must be asked to consent to each appropriation of information about their on-line activities (opt-in) or, rather, whether Internet users have implicitly consented to general use of digitized profiles of their Internet activities so that each Internet user must expressly withdraw consent to sale of such information (opt-out), remains a very contentious privacy issue.[60] In privacy tort cases,

57. *Id.* at cmt. b.

58. *Id.* at cmt. c. Whether it would be actionable under the common law appropriation privacy tort to use a famous, or infamous, screen name or Internet persona to advertise an Internet security service is an intriguing matter which has yet to be litigated. Logically if the name refers to an individual person, the common law tort should apply. Alternative grounds for liability in such cases might be based on copyright or trademark, if the persona or screen name were copyrighted or trademarked.

59. *See* Zacchini v. Scripps-Howard Broad. Co., 433 U.S. 562 (1977). In this case the United States Supreme Court upheld privacy tort liability for appropriation despite First Amendment protection of freedom of expression, when a television station broadcasted the performer's entire act as a human cannon ball. *Id.* at 575.

60. For example, Financial Services Legislation of 1999, Pub. L. No. 106-102, § 502, 113

consent is often construed narrowly so that a deliberate decision to opt-in would ordinarily be required.

Both private facts and false light privacy torts require publicity in the form of widespread dissemination that goes beyond mere "disclosure" or "publication" as these terms are understood in the law of defamation. With regard to publicity over the Internet, the *Michaels* case, *supra*, is an example of an actionable invasion of privacy for publicity regarding private facts over the Internet. Posting Irene's tax returns on an Internet bulletin board or surreptitiously webcasting digital pictures of Irene privately celebrating a family birthday would probably also constitute tortious public disclosure of private facts, if done without her consent. If digital pictures of Irene's family celebration were accompanied by misleading references, such as to "the secret problem of inebriation at home," common law tort liability for false light invasion of privacy might arise. Even certain kinds of Internet spoofing by posting slanted information regarding an individual, for example by describing Irene, who is a gregarious person with a happy family and many friends, as a "lonely woman seeking affection on-line," might give rise to false light privacy tort liability.[61]

Privacy statutes are even more numerous and varied than the common law privacy tort actions. Some state privacy statutes enact particular versions of the privacy torts. For example, in some states statutory rights of publicity authorize causes of action against exploitation of celebrity personalities.[62] These statutory publicity rights are similar to privacy rights vindicated by the appropriation tort, but often provide more extensive privacy protection.[63] Other statutes have enacted new forms of privacy rights against invasions of privacy, such as cyberstalking, that were arguably not actionable

Stat. 1338, 1437 (Nov. 12, 1999) adopted an opt-out approach with regard to transfer of information within a financial institution, but an opt-in approach with regard to disclosures outside of that financial institution. Given the conglomerate nature of many financial institutions, which may now include insurance, investments, credit reporting and other services under the 1999 Financial Services Legislation, the opt-out provisions applicable to transfers within a financial institution, may result in a much wider presumption of consent to transfer than is realistic.

61. *See* Cantrell v. Forest City Publ'g Co., 419 U.S. 245 (1974). *Cf.* Time, Inc. v. Hill, 385 U.S. 374 (1967).

62. *See* CAL. CIV. CODE § 3344 (West 1997). According to the Ninth Circuit, these statutory rights are in addition to the common law tort privacy rights. *See* Midler v. Ford Motor Co., 849 F.2d 460 (9th Cir. 1988).

63. *See* CAL. CIV. CODE § 3344.1 (West 2000) which provides for survival of the statutory publicity rights of deceased persons.

under the common law.[64] Another example is California Civil Code section 1708.8(b), regarding constructive invasion of privacy, which penalizes use of visual or auditory devices to capture images of personal or familial activities.[65] Many privacy statutes focus on particular types of information, such as consumer credit records protected under the Fair Credit Reporting Act,[66] or Drivers License Records,[67] or on particular databases, such as federal agencies' systems of records containing personal information, protected under the Federal Privacy Act.[68] These privacy statutes are not specifically directed at Internet activities, but rather would apply to the Internet when the specified personal information or privacy invading conduct occurs on the Internet.

A few statutes target Internet invasions of privacy. For example, the Children's Online Privacy Protection Act[69] is directed at protecting the privacy rights of children who access the Internet. This statute would protect the privacy of Irene's eight and ten-year old children, James and Jennifer, who are each on-line about an hour a day. Another example of a type of state statute directed at Internet invasions of privacy is the cyberstalking statute such as California's amendments to its anti-stalking statute noted above.[70] If Irene were on-line in California, for example, the cyberstalking statute would make it illegal for someone to follow her about by shadowing her activities on the web and sending her threatening e-mail messages.

In addition to privacy statutes, privacy laws also include agency

64. *See* CAL. CIV. CODE § 1708.7 (West 2000) (establishing liability for stalking, including threats communicated by means of electronic communication devices).

65. *Id.* § 1708.8(b). This statute states:

> A person is liable for constructive invasion of privacy when the defendant attempts to capture, in a manner that is offensive to a reasonable person, any type of visual image, sound recording, or other physical impression of the plaintiff engaging in a personal or familial activity under circumstances in which the plaintiff had a reasonable expectation of privacy, through the use of a visual or auditory enhancing device, regardless of whether there is a physical trespass, if this image, sound recording, or other physical impression could not have been achieved without a trespass unless the visual or auditory enhancing device was used.

Id.

66. 15 U.S.C. §§ 1681-1681t (1994); *see also In re* TransUnion Corp., No. 9255 (FTC Mar. 29, 2000) < http://www.ftc.gov/os/2000/03/transunionrestay.htm>.

67. The Driver's Privacy Protection Act, 18 U.S.C. §§ 2721-2725 (1994); *see also* Reno v. Condon, 120 S. Ct. 666 (2000) (upholding the Act's validity).

68. 5 U.S.C. § 552a (1994).

69. 15 U.S.C.A. §§ 6501-6506 (West 1999).

70. *See* CAL. CIV. CODE § 1708.7 (West 2000).

regulations that provide privacy protection.[71] For example, each federal agency subject to the Federal Privacy Act is required to publish regulations with regard to the nature of that agency's systems of records containing personal information about individuals.[72] These Privacy Act regulations provide Irene both a way to discover which federal agencies maintain databases containing personal information about her and a process for accessing that information.[73] Other examples of regulatory privacy law affecting the Internet are the Federal Trade Commission's proposed regulations implementing the Children's Online Privacy Protection Act[74] and the Department of Health and Human Services proposed regulations regarding medical records.[75]

In addition to constitutional, common law, statutory and regulatory privacy laws, non-governmental self-regulatory measures can also be the bases for legal privacy rights for Internet users such as Irene. Theses self-regulatory measures commonly take the form of a company's own privacy principles. Sometimes companies adopt codes of fair information practices put forward by trade associations. For example, Irene might encounter Amazon.com's privacy principles[76] or those of American Express[77] when she buys books or airline tickets over the Internet. These on-line privacy measures may be given legal effect to the extent that non-compliance would constitute a deceptive trade practice. For example, Internet retailers often make privacy promises to induce customers, such as Irene, to engage in electronic commerce with these companies. If an Internet retailer promises not to disclose Irene's Internet purchasing records to any other company, and then turns around and sells Irene's purchasing history to a direct marketing firm, the Internet retailer may be liable under deceptive trade practices laws. The Federal Trade Commission has taken unfair trade practices actions against companies that have announced privacy principles to attract

71. *See, e.g.*, 34 C.F.R. § 99.1-.67 (2000) (Department of Education regulations implementing the Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g (1994)).

72. 5 U.S.C. § 552a(e)(4), (f) (1994).

73. *Id.* at (d).

74. *See* Children's Online Privacy Protection Rule, 64 Fed. Reg. 59888 (1999) (to be codified at 16 C.F.R. pt. 312) (proposed Apr. 27, 1999).

75. Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59918 (1999) (to be codified at 45 C.F.R. pts. 160-64) (proposed Nov. 3, 1999).

76. *See Amazon.com: Your Privacy* (visited Mar. 5, 2000) <http://www.amazon.com/exec/obidos/subst/misc/policy/privacy.html/>.

77. *See American Express Customer Internet Privacy Statement*, *supra* note 21.

customers, but then failed to abide by their avowed privacy protection promises.[78] Such enforcement under deceptive trade practices laws means that if Internet companies falsely represent to Irene that they will protect her privacy, they may face potential legal liability for interfering with the privacy protection promised in gaining her business.

4. Context-dependent

Particular on-the-web applications of privacy laws frequently depend on the contexts of alleged invasions of privacy. This context-dependency is at least partly explained by the way privacy law has evolved over the past century or so, often in reaction to particular invasions of privacy. For example, when Brandeis first argued that the common law should recognize a damage action for invasion of privacy, he pointed to the notorious case of Marion Manola, an actress photographed in tights against her will.[79] More recently, the use of motor vehicle license records by murderers of young women has led to the enactment of statutes restricting the availability of such records.[80] Although a few privacy laws apply broadly to a general form of invasion of privacy, such as electronic surveillance,[81] privacy laws typically focus on a particular situation or type of personal information. For example, the federal Video Privacy Protection Act provides for the privacy protection of video rental records.[51] This statute was enacted into federal law after the records of Judge Robert Bork's videotape rentals surfaced in Senate hearings regarding his nomination to the United States Supreme Court.[83] Because privacy law has characteristically evolved by solving a particular type of

78. *See In re* Geocities, Inc., No. C-3849, 1999 FTC LEXIS 17 (FTC Feb. 5, 1999) (ordering Geocities to cease deceptive trade practices in the form of misrepresentations regarding the use and collection of personal information).

79. *See* Warren & Brandeis, *supra* note 2, at 195. The lawsuit, Manola v. Stevens & Meyers, is discussed in Dorothy J. Glancy, *Privacy and the Other Miss M*, 10 N. ILL. U. L. REV. 401, 402-19 (1990).

80. The Driver's Privacy Protection Act, 18 U.S.C. §§ 2721-2725 (1994), was prompted by the 1989 murder of actress Rebecca Schaeffer, star of the hit television series, "My Sister Sam." *See* 139 CONG. REC. S15745-01, *515762 (1993) (statement of Sen. Boxer); *see also* Ellen Barry, *Killer's Dreams Bared on the Internet N.H. Man Took to Web to Boast and To Stalk*, BOSTON GLOBE, Nov. 29, 1999, at B1; *Killer Plotted Murder Through Internet*, S.F. CHRON., Nov. 30, 1999, at A12.

81. *See* discussion *supra* notes 26-27.

82. 18 U.S.C. § 2710 (1994).

83. *See* S. REP. NO. 100-599, at 5-6 (1988); *see also House OKs Video Privacy Protection Bill*, L.A. TIMES, Oct. 20, 1988, at I2; ETHAN BRONNER, BATTLE FOR JUSTICE: HOW THE BORK NOMINATION SHOOK AMERICA 274 (1989).

privacy problem or by reacting to a notorious invasion of privacy, or by protecting a particular type of personal information, it is not surprising that context plays an important role in the diversity of privacy law.

For the most part, the privacy laws applicable to Irene's on-line activities were not designed for the Internet context, but rather can be applied to her Internet activities by extrapolation from other settings. In considering extrapolation of privacy laws to the Internet, two contextual factors are particularly noteworthy. First, different privacy laws will apply depending on whether the invasion of privacy involves collection of personal information or manipulation of personal information or dissemination of personal information. Second, different privacy laws will apply depending on whether privacy is invaded by the government or by the private sector.

Some privacy laws concentrate on controlling collection of personal information. For example, the constitution and federal statutes restrict unauthorized electronic surveillance of Irene's on-line activities without a warrant or intercept order.[84] The intrusion privacy tort also provides a basis for imposing liability for improper collection of such personal information. And yet the collection of information about Irene's Internet browsing remains controversial. Marketing companies maintain that placing cookies in Irene's browser or identification numbers in her microprocessor has nothing to do with Irene's privacy, because the information collected does not personally identify Irene. Rather, the information collected only identifies hardware or software, not any identified person who may be manipulating the hardware or software. The potential that records of Internet activities can be combined with other information to identify Irene as the user of the identified microprocessor or software cookie has, however, raised serious privacy concerns.[85] Whether such information is personal to Irene at the time it is collected, or only potentially personally identifiable after it is connected to other information, is among the privacy questions posed by the nearly infinitely replicable, manipulable and aggregateable qualities of

84. *See* discussion *supra* notes 25-26; *see also supra* notes 82-83.

85. For example, plans by DoubleClick to integrate its web-browsing records with the consumer database of Abacus, a direct marketing company acquired by DoubleClick raised a storm of protest, first from privacy advocates and later from Wall Street. *See* Jeri Clausing, *Privacy Adovcates Fault New DoubleClick Service*, N.Y. TIMES, Feb. 15, 2000, at C2; *Privacy on the Internet*, N.Y. TIMES, Feb. 22, 2000, at A26; Bob Tedeschi, *In a Shift, DoubleClick Puts Off Its Plan for Wider Use of the Personal Data of Internet Consumers*, N.Y. TIMES, Mar. 3, 2000, at C5.

digitized information. What is certain is that the Internet's global network magnifies the consequences for individual privacy when a vast range of such digitized information is collected about people and their on-line activities.

With regard to aggregation of personal information, the 1999 Financial Services Legislation permits considerable manipulation and aggregation of personal information within a financial institution.[86] As financial institutions become global providers of insurance, stock-trading, savings accounts and direct marketing, in addition to retail banking, there will be enhanced opportunities for widespread sharing and manipulation of personal data among the many subsidiaries and affiliates of modern financial institutions. It is interesting to contrast this permissive approach in the financial services legislation, allowing widespread sharing of personal information about customers within a financial institution, with the approach in the Privacy Act, which restricts the transfer of an individual's personal information among federal agencies.[87]

When dissemination of personal information is the context of privacy concerns, different privacy laws apply. Examples include the privacy torts of appropriation, private facts and false light as well as the Fair Credit Reporting Act. Different approaches to legal protection against improper dissemination of personal information are characteristic of these privacy laws. For example, the Fair Credit Reporting Act prohibits dissemination of Irene's credit history without her consent for all but a few restricted purposes.[88] The disclosure of private facts privacy tort, on the other hand, provides a basis for Irene to bring suit for damages against an Internet company from which she purchased exotic lingerie, if that company were to publicly post the details of her purchases on its web site.[89]

Another contextual factor that causes different privacy laws to apply is whether interference with privacy has been perpetrated by the government or by the private sector. It is interesting to note that Brandeis's initial discussion of privacy law was focused on non-governmental interferences with privacy, mostly by newspapers.[90] Later, Brandeis came to see government as posing an even greater

86. *See* Financial Services Legislation of 1999, Pub. L. No. 106-102, § 502, 113 Stat. 1338, 1437 (Nov. 12, 1999).

87. *See* 5 U.S.C. § 552a (1994).

88. 15 U.S.C. § 1681b-1681c (1994).

89. *See* discussion *supra* notes 38, 45. Common law tort liability is also possible under appropriation and false light privacy theories for Internet postings of personal information.

90. *See* Glancy, *supra* note 15, at 8-17.

danger to individual privacy:

> The progress of science in furnishing the government with means of espionage is not likely to stop with wiretapping .... Our government is the potent, the omnipresent teacher. For good or for ill, it teaches the whole people by its example. Crime is contagious. If the government becomes a lawbreaker, it breeds contempt for law; .... To declare that the government may commit crimes in order to secure the conviction of a private criminal would bring terrible retribution. Against that pernicious doctrine this court should resolutely set its face.[91]

Justice William O. Douglas agreed with Brandeis that the government's threat to privacy was much more serious than that posed by the private sector.[92]

Although concerns about government interference with privacy remain important,[93] at the turn of the twenty-first century, the focus of privacy concerns seems to have turned increasingly toward worries about invasion of privacy by private-sector hackers and crackers and telemarketers. Thomas Friedman calls this the "little brother" problem,[94] as distinguished from the problem of omnipresent government surveillance symbolized by "Big Brother" in George Orwell's novel, *1984*.[95] Internet users seem to be particularly concerned about private-sector collectors, manipulators and sellers of personal information in what is now a globalized marketplace. Privacy law has always been responsive when new threats to privacy are identified. The focus of primary concerns about government invasions of privacy, such as those associated with Watergate, seem to shifting toward enhanced concern about invasions of privacy by the private sector, such as those associated with disclosures of credit card numbers from Internet sites. Underlying concerns about protecting individual privacy from being overwhelmed by society, whether in the form of big government or in the form of big business, remains a strong force in American law.

91. Olmstead v. United States, 277 U.S. 438, 474-85 (1928) (Brandeis, J., dissenting). Eventually the United States Supreme Court agreed with Brandeis and reversed Olmstead. *See* Katz v. United States, 389 U.S. 347 (1967).

92. *See* WILLIAM O. DOUGLAS, THE RIGHT OF THE PEOPLE 123-24 (1958); *see also* Wyman v. James, 400 U.S. 309, 335 (1971) (Douglas, J., dissenting); Dorothy J. Glancy, *Getting Government Off the Backs of People*, 21 SANTA CLARA L. REV. 1047, 1050-51 (1981).

93. *See The Searchable Soul*, HARPER'S MAG., Jan. 1, 2000, at 57.

94. *See* Thomas L. Friedman, *Little Brother*, N.Y. TIMES, Sept. 26, 1999, Sec. 4 at 17; Thomas L. Friedman, *The Hackers' Lessons*, N.Y. TIMES, Feb. 15, 2000, at A31.

95. GEORGE ORWELL, 1984 (1950).

B. Decentralized

The decentralized nature of United States privacy law further complicates understanding the intersections of privacy law with the Internet. There are not only diverse types of privacy laws operating in many different contexts, but also many different sources of these laws. Federal law and state law provide the two primary sources of privacy law in the United States. In addition, as noted earlier, sometimes these state and federal privacy laws interact with private-sector representations regarding privacy policies and industry privacy standards. As a result, if Internet users such as Irene were suddenly to see the operation of the privacy laws potentially applicable to their Internet activities, they would see these privacy laws coming from several directions at once.

The decentralized pattern of United States privacy law is in marked contrast to the more centralized approach taken in Europe, associated with the 1995 European Union Data Protection Directive.[96] The overall purpose of the European Data Protection Directive is to harmonize within the European Union the law which applies to processing personal information relating to an identified or identifiable natural person[97] Under the Data Protection Directive, every member state in the European Union is required to adopt strict privacy laws providing privacy rights at minimum levels described in the directive. Such a centralized "harmonization" contrasts with the deliberately decentralized "cacophony" of United States privacy law.[98]

Federalism is the primary reason why United States privacy law has generally avoided the centralized one-size-fits-all approach exemplified by the European Data Protection Directive. Indeed, reflecting federalism, United States privacy law mixes both federal and state laws, and also accommodates a divergent pattern of state privacy laws that often vary considerably from state to state. In another context, Justice Brandeis insisted that it is important for states

96. *See* DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 24 OCTOBER 1995 ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA AND ON THE FREE MOVEMENT OF SUCH DATA (October 24, 1995) <http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html>. Effective October 25, 1998, the Directive is subject to continuing refinement.

97. *See id.* at arts. 2-3.

98. The European Data Protection Directive can have practical consequences with regard to Internet activities involving personal information if these activities take place in part in Europe. Difficult and still unresolved, issues with regard to jurisdiction over Internet activities to make it hard to predict which nation's privacy law will apply in any given circumstance involving transnational flows of personally identifiable data.

to be able to experiment with social and economic legislation. He noted that "it is one of the happy incidents of the federal system that a single courageous State may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments."[99] Although Brandeis was not discussing privacy law in *New State Ice Co. v. Liebmann*, one of the most interesting social and economic areas in which extensive experimentation has taken place across the states, as well as between the states and the federal government, is with regard to privacy laws.

A good example of the decentralized pattern of federal and state privacy law is the complex layering of federal and state privacy laws regarding electronic surveillance discussed earlier in this essay.[100] Initially based primarily on federal constitutional and statutory law, these electronic surveillance laws now include the variety of both state and federal privacy laws that are applicable to electronic surveillance of Internet communications. Consider how both federal and state laws protect the privacy of Irene's Internet communications. Recall that Gill is a federal law enforcement official who has tapped Irene's modem line to intercept her Internet communications without a warrant or intercept order and that Gill's invasion of Irene's privacy is illegal under federal law.[101] Recall also that interception of Irene's Internet communications by a private investigator, Paul, would violate different provisions of federal wiretap statutes, as well as provisions of state law in most states.[102] However, in some states, such non-governmental recording of Irene's Internet communications through use of an extension telephone on Irene's modem line would be illegal; but in many other states such interception would not be considered an invasion of privacy. For example, if Irene were on-line in California, use of the extension line would violate California's highly restrictive electronic surveillance laws.[103] But if Irene were on-line in New

99. New State Ice Co. v. Liebmann, 285 U.S. 262, 311(1932) (Brandeis, J., dissenting).

100. *See supra* text accompanying notes 25-26.

101. *See* U.S. CONST. amend. IV; Electronic Communications Privacy Act, 18 U.S.C. §§ 2701-2711 (1994); Privacy Protection Act, 42 U.S.C. § 2000aa to 2000aa-12 (1994); McVeigh v. Cohen, 983 F. Supp. 215 (D.D.C. 1998). If Gill were a state law enforcement official, he might also be in violation of state constitutional provisions and statutes. *See, e.g.*, CAL. CONST. art. 1, § 13; CAL. PENAL CODE § 630 (West 1999).

102. *See, e.g.*, Biton v. Menda, 796 F. Supp. 631 (D.P.R. 1992). The Federal Electronic Communications Privacy Act, 18 U.S.C. §§ 2701-2711 (1994), does not preempt state statutes which provide more protection to the privacy of electronic communications. *See* 18 U.S.C. § 2516(2) (1994).

103. *See* CAL. CONST. art. 1, § 1; CAL. PENAL CODE § 630-37.2 (West 1999); Ribas v. Clark, 38 Cal. 3d 355, 696 P.2d 637, 212 Cal. Rptr. 143 (1985).

Hampshire, that state's more permissive electronic eavesdropping laws would permit use of the extension telephone line to record Irene's Internet transmissions.[104]

Although, privacy protection in the United States typically comes from a mixture of federal and state privacy laws, an interesting, and rare, exception to the decentralized pattern of federal and state privacy laws is the law that applies to the privacy of consumer credit records under the Federal Fair Credit Reporting Act.[105] With certain limited exceptions, only federal law applies with regard to matters covered by the Fair Credit Reporting Act.[106] Aside from the Fair Credit Reporting Act, state privacy laws are generally not preempted by federal law. For example, the 1999 Financial Services Legislation expressly allows states to adopt more stringent privacy protections.[107] So far, Internet users have not expressed interest in a unified federal privacy law that would preempt state experimentation with divergent approaches to privacy protection. Rather, Brandeis's notion of benign variation among state privacy laws, as well as between federal privacy laws and state privacy law seems likely to continue to be the preferred pattern of privacy laws in the United States.

C. Dynamic

Compounding the diversity and decentralization of United States privacy laws, is the remarkable dynamism of privacy law in the United States. From its inception in the nineteenth century, privacy law has evolved in response to new challenges to the privacy interests of individuals, particularly challenges posed by new technologies. This dynamic quality of privacy law is evident as old privacy laws confront new challenges posed by the Internet. Indeed, part of the original argument for recognition of the right to privacy in the United States was based on the need to respond to societal and technological change:

> Political, social and economic changes entail the recognition of new rights . . . Recent inventions and business methods call attention to the next step which must be taken for the protection of the person and for securing to the individual what Judge Cooley

104. *See* State v. Telles, 139 N.H. 344, 653 A.2d 554 (1995).

105. 15 U.S.C. § 1681-1681t (1994).

106. *Id.*

107. *See* Financial Services Legislation of 1999, Pub. L. No. 106-102, § 507(b), 113 Stat. 1338, 1442 (Nov.12, 1999).

> calls the right 'to be let alone.' Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'[108]

Among the privacy threatening technologies that worried Warren and Brandeis 1890 were the flash camera, plate glass, the telephone and telegraph.[109] Later, in his famous dissenting opinion in *Olmstead*, Brandeis expressed concern that "Discovery and invention have made it possible for the government by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet."[110] He speculated that

> The progress of science in furnishing the Government with means of espionage is not likely to stop with wire tapping. Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions.[111]

Had Brandeis imagined the Internet, he most likely would have predicted, and urged, further development of privacy law.

Contemporary society's voyeuristic interest in prying into the details of personal life, evident in such aspects of popular culture as talk radio and shock broadcasting,[112] pose a counter force against development of laws more protective of privacy.[113] Internet webcasting of activities including sexual intercourse, childbirth, working on homework and all sorts of other ordinary life activities, from the trivial to the profane, brings private life onto the web—on web cam, on-line, available virtually all of the time. Such challenges to privacy are not new. Even in 1890, Warren and Brandeis expressed outrage over the destructive impact of widespread

108. Warren & Brandeis, *supra* note 2, at 193, 195.

109. *See* Glancy, *supra* note 15, at 8.

110. Olmstead v. United States (Brandeis, J., dissenting), 277 U.S. 438, 473 (1928).

111. *Id.* at 474.

112. Typical examples are television's "The Jerry Springer Show," the film, "The Truman Show" and "Big Brother," which broadcasts the real lives of individuals over television in Holland and Germany.

113. Judge Richard Posner has described this voyeurism as the interest in prying, which weighs against the interest in privacy. *See* Richard Posner, *The Right of Privacy*, 12 GA. L. REV. 393, 394-97 (1978).

publication of the details of private life: "To satisfy a prurient taste the details of sexual relations are spread broadcast in the columns of the daily papers."[114] The Internet's proven capacity for even wider circulation of ever more personal and private information would undoubtedly have greatly troubled Warren and Brandeis, who counted the devaluation of private life through widespread disclosure as among the important policy reasons for legally protecting the right to privacy.

As the Internet itself rapidly evolves, new privacy challenges are certain. For example, a recent research report predicts that there will be more than 1.4 billion Internet participants world-wide by 2004.[115] What is perhaps even more remarkable is that the report predicts that by 2004 a majority of Internet participants will access the Internet over mobile terminals—both handheld and in vehicles. An estimated 670 million people will access the web through fixed or "wired" platforms. But 750 million people will access the web over wireless modems, PDAs such as Palm Pilots and Psions, and Internet access built into vehicles.[116] The suggestion is that the World Wide Web may well be rapidly transforming into a Wireless World Wide Web. As this transformation in Internet usage takes place, new privacy law issues will undoubtedly arise. These new privacy law issues not only include intensified privacy concerns with regard to the security of wireless Internet communications. They also will reflect privacy concerns about an individual's control over information that pinpoints an individual's geographical location as she accesses various sites on the Internet from changing locations.

III. CONCLUSION

Despite Scott McNealy's pessimistic views, privacy is unlikely to wither away in the United States. If the past is any guide to the future of privacy law, the American public is unlikely to "get over"

114. Warren & Brandeis, *supra* note 2, at 196. The article decried the publication and circulation of personal information as "potent for evil" and explained:

> It both belittles and perverts. It belittles by inverting the relative importance of things, thus dwarfing the thoughts and aspirations of a people. When personal gossip attains the dignity of print and crowds the space available for matters of real interest to the community, what wonder that the ignorant and thoughtless mistake its relative importance.

Id.

115. *See* THE ARC GROUP, WIRELESS INTERNET: APPLICATIONS, TECHNOLOGY & PLAYER STRATEGIES (1999). The contents of the report are also available at <http://www.the-arc-group.com/reports/wireless_internet/toc_wi/htm>.

116. *See id.*

privacy anytime soon. The privacy laws discussed in this essay already affect the Internet in remarkable ways. The future is likely to bring to bear even more privacy laws. These privacy laws may well remain invisible to most people. But there will be privacy laws intersecting with the Internet in more ways that even sophisticated Internet users may imagine. The wide spectrum of participants in the February 2000 symposium on Privacy in the Next Millennium sponsored by the Santa Clara Computer and High Technology Law Journal presented a clear demonstration that the interaction between privacy law and the Internet remains a matter of significant concern to those who think, write legislate and regulate about privacy in the twenty-first century.