PROTECTING PRIVACY IN THE DIGITAL AGE

By Will Thomas DeVries

"You have zero privacy anyway . . . . Get over it."[1]

With this proclamation, Scott McNealy, founder of Sun Microsystems, anchored the radical edge of the privacy debate for the digital world.[2] He viewed it as a foregone conclusion that, in the information age, any "secret" thing committed to digital form was subject to instant and inevitable distribution. But while digital technology has drastically changed the privacy landscape, reports of the death of privacy have been greatly exaggerated.

Nevertheless, Mr. McNealy's statement speaks some truth in that the conceptions of "privacy" carried over from the analog world have not aged gracefully. For example, the Fourth Amendment protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures . . . ."[3] These words conceive personal privacy in physical terms, but in the digital world, many of one's most private things, such as medical records, may be stored in a database far from one's "person" or "house." How can one tell if a search of such a database is unreasonable?

Mr. McNealy also intuited correctly that the existing legal framework for privacy is failing. As digital technology renders obsolete the theories on which the laws are based, the legal protections themselves become at best incomplete and at worst perverse. Privacy law has traditionally developed in tandem with technology—reshaping itself to meet the privacy threats embodied in new technology.[4] The information revolution, however, is occurring so fast and affects so many areas of privacy law that the old, adaptive process is failing to address digital privacy problems.[5]

---

1. Polly Sprenger, *Sun on Privacy: 'Get Over It'*, WIRED NEWS, Jan. 26, 1999, *at* http://www.wired.com/news/politics/0,1283,17538,00.html.

2. *See, e.g.*, A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1462 (2000) (discussing, with reference to Mr. McNealy's quotation, the question of whether privacy is indeed dead or dying); *see also infra* Part I.B.

3. U.S. CONST. amend. IV.

4. *See* Dennis F. Hernandez, *Litigating the Right to Privacy: A Survey of Current Issues*, 446 PLI/PAT 425, 429 (1996).

5. *See* Jerry Berman & Deirdre Mulligan, *The Internet and the Law: Privacy in the Digital Age: A Work in Progress*, 23 NOVA L. REV. 549, 554 (1999).

Fortunately for those who value privacy, most people cannot "get over it" so easily. Even if attempts at theoretical and substantive adaptation in this new era are so far preliminary and halting, progress is underway. In the last few years, we have seen an explosion of new laws (both state and federal), development of new business practices, new diligence on the part of regulatory agencies, new international mandates, and more sensitive judicial decisions on privacy.

This Note attempts to survey the state of privacy in the midst of the digital age. Part I summarizes the current status and theoretical roots of the two most distinct "branches" of privacy law—*autonomy* (both physical and decisional) and *informational* privacy. This Part will also outline the technology and developments of the digital age. Part II will survey the impact of digital technology on these two areas of privacy law. Part III will examine the ways in which the old, analog conception of privacy breaks down in these areas. This Part discusses why the distinction between privacy-as-autonomy and privacy-as-information-control is inadequate in the face of new technology.

I. THE EVOLUTION OF PRIVACY

Privacy interests are as old as civilization,[6] though modern conceptions of privacy *per se* are far more recent.[7] Traditionally, privacy interests were implicit in legal or social protection of personal property and space,[8] intimate settings,[9] or personal effects.[10] But by the Twentieth century, scholars had distilled privacy into an independent concept—breathing life into

6. Scholars have noted proto-privacy rights in the Qur'an, the sayings of Mohammed, and the Old Testament. *See* Electronic Privacy Information Center & Privacy International, Privacy and Human Rights: An International Survey of Privacy Laws and Developments 5 (2002) [hereinafter Privacy and Human Rights]; Chris Hoofnagle, *Colloquium on Privacy & Security*, 50 Buff. L. Rev. 703, 726 (2002).

7. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

8. For example, the Talmud prescribed a certain height for walls between houses in order to prevent peering through the windows of neighbors. *See* Hernandez, *supra* note 4, at 429.

9. *See, e.g.*, PRIVACY AND HUMAN RIGHTS, *supra* note 6, at 5 (noting that early English law protected against "peeping toms").

10. *See, e.g., id.* (noting Victorian age protection against seizure of personal papers without a warrant).

one of the most discussed yet poorly understood areas of modern legal thought.[11]

The modern evolution of the privacy right is closely tied to the story of industrial-age technological development[12]—from the telephone[13] to flying machines.[14] As each new technology allowed new intrusions into things intimate, the law reacted—slowly—in an attempt to protect the sphere of the private.[15] Digital technology—computing, databases, the Internet, mobile communications, and the like—thus calls for further evolution of privacy rights, both conceptually and in law. Unlike previous technological changes, however, the scope and magnitude of the digital revolution is such that privacy law cannot respond quickly enough to keep privacy protections relevant and robust.

A. The Branches of American Privacy Law

Perhaps because privacy development has been tied to specific technological change, the legal framework for privacy in the United States is disjointed and piecemeal. Privacy provisions exist in common law, in the Federal and state constitutions, and in a mishmash of statutes.[16] The legal theory connecting the various privacy protections is similarly disjointed.[17] Several "branches" of law have developed—all growing from the seed of "privacy," but based on differing theories of what should be protected. The following sections discuss the two most prominent branches, their pre-digital status, and the privacy rights they seek to protect: (1) the traditional physical and decisional "right to be let alone"; and, (2) the more recent notion of control over (or rights concerning) personal information.[18]

---

11. *See* Warren & Brandeis, *supra* note 7; *see also* ALAN WESTIN, PRIVACY AND FREEDOM 7 (Atheneum 1967) (lamenting that "[f]ew values so fundamental to society as privacy have been left so undefined in social theory").

12. Hernandez, *supra* note 4, at 429.

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

14. *See* Florida v. Riley, 488 U.S. 445, 448 (1989) (involving police surveillance with a helicopter); California v. Ciraolo, 476 U.S. 207, 209 (1986) (involving police surveillance with a spy-plane).

15. Hernandez, *supra* note 4, at 429.

16. *Id.*

17. *See* Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1088-89 (2002).

18. It must be noted that while this division is rooted in history, such categories are not the only way of dividing this legal spectrum. *E.g.*, Anita L. Allen-Castellitto, *The Origins of Growth of U.S. Privacy Law*, 701 PLI/PAT 83, 16 (2001) (identifying four areas of privacy: informational, physical, decisional, and proprietary); Hernandez, *supra* note 4, at 429 (dividing the privacy right into common law, constitutional, and statutory pieces); Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV.

1. Privacy as Autonomy: The Right to Be Let Alone

Samuel Warren and Louis Brandeis, the first to systematically describe a legal right to privacy, defined it as essentially a right to protect one's "inviolate personality" from intrusion or unwanted revelation.[19] In essence, they argued for a "right to be let alone."[20] At least with respect to state intrusions, Brandeis' conception of privacy eventually became accepted Constitutional law, rooted in the Bill of Rights' explicit protection against government intrusion into the home and personal effects[21] and implicit protection of autonomy and free choice.[22] Protection against similar unwarranted intrusions by private parties evolved into common law tort claims.[23] Broadly speaking, the test became whether the victim had a "reasonable expectation of privacy" and whether the other party or state entity violated it without justification.[24]

Two major sub-branches have developed: physical or spatial privacy and decisional privacy. The privacy of physical space or things receives strong protection. The Court has sharply limited the government's ability to intrude upon the "reasonable expectation of privacy" that all citizens have in their persons and effects.[25] Physical privacy also gets strong pro-

---

1193, 1202-03 (1998) (describing three privacy areas as relating to physical space, choice, and information); Robert C. Post, *Three Concepts of Privacy*, 89 GEO. L.J. 2087, 2087 (2001) (noting three conceptions of privacy: creation of knowledge, dignity, and freedom). Moreover, though the two "branches" herein cover the most common areas of privacy law, they are incomplete. *See generally* JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA (2000).

19. Warren & Brandeis, *supra* note 7, at 205.

20. *Id.* at 195. Later, on the Supreme Court, Justice Brandeis described this as "the most comprehensive of rights and the right most valued by civilized men." Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

21. *See* U.S. CONST. amends. III, IV, XIV; Mapp v. Ohio, 367 U.S. 643, 656 (1961) (applying the federal privacy rights embodied in the Bill of Rights to the states).

22. *See* U.S. CONST. amends. I, V, IX; Griswold v. Connecticut, 381 U.S. 479, 484 (1965).

23. RESTATEMENT (SECOND) OF TORTS § 652A-652E (1977) (defining the four privacy torts as (1) intrusion upon seclusion, (2) public disclosure of private facts, (3) false light publicity, and (4) misappropriation of a person's name or likeness). *Accord* William L. Prosser, *Privacy*, 48 CAL. L. REV. 381, 389 (1960).

24. *See* California v. Ciraolo, 476 U.S. 207, 211 (1986) (Harlan, J., concurring) (citing Katz v. United States, 389 U.S. 347, 360 (1967)).

25. *See, e.g., id.* at 359 (holding that the government cannot listen to phone booth conversations without a warrant); Kyllo v. United States, 533 U.S. 27, 40 (2001) (same for use of thermal imaging equipment to monitor movement through the walls of a house). *But see, e.g.*, Bd. of Educ. v. Earls, 536 U.S. 822, 122 S. Ct. 2559, 2562 (2002) (finding that school policy of mandating drug tests for all high-school students participating in extracurricular activities does not violate the student's privacy).

tection against private intrusion through privacy tort claims. Though the torts have been used most notably by public figures seeking to protect their private lives,[26] they do protect against especially egregious intrusions even for common folk.[27] Finally, most states protect some specific physical privacy rights through statute; for instance, California bans two-way mirrors[28] and New York prohibits hidden cameras in bathrooms or hotel rooms.[29]

In the 1970s, the Court extended the Brandeis conception of privacy to state intrusion upon certain intimate decisions, such as those affecting marriage, procreation, and the family.[30] Thus the state cannot intrude too deeply into decisions regarding such things as use of birth control,[31] abortion,[32] and interracial marriage.[33] Unlike the physical right to be let alone, however, this view of privacy has no tort corollary or statutory support. The Court, too, seems wary of extending this marginally textual substantive right too far.[34]

---

26. This is likely due to the fact that famous people often face larger monetary harms due to the privacy loss than others. *See, e.g.*, Galella v. Onassis, 533 F. Supp. 1076, 1106 (S.D.N.Y. 1982) (finding that the privacy of former First Lady Jacqueline Kennedy Onassis was invaded by an "overzealous" news reporter who followed her about).

27. *See, e.g.*, Miller v. Brooks, 472 S.E.2d 350, 354 (N.C. Ct. App. 1996) (holding a private investigator liable for the tort of intrusion upon seclusion for installing hidden cameras in the house of the nonfamous plaintiff).

28. CAL. PENAL CODE § 653n (West 1969); *see also* Cramer v. Consol. Freightways Inc., 255 F.3d 683, 688 (9th Cir. 2001) (applying the California law to a company that installed cameras behind the mirrors in employee washrooms).

29. N.Y. GEN. BUS. § 395-b (McKinney 1996).

30. *See, e.g.*, Griswold v. Connecticut, 381 U.S. 479, 485 (1965). Justice Goldberg, writing for the majority, found the basis for decisional privacy in the "penumbras" or "emanations" of specific provisions of the Bill of Rights. *Id.* at 484. The Court today seems to prefer to ground this right in the "basic values 'implicit in the concept of ordered liberty'" and the Fourteenth Amendment. *See id.* at 500 (Harlan, J., concurring); *see also* Cruzan v. Director, Missouri Dep't of Health, 497 U.S. 261, 279 n. 7 (1990).

31. *Griswold*, 381 U.S. at 485.

32. Roe v. Wade, 410 U.S. 113, 153 (1973) (finding "the right to privacy . . . broad enough to encompass a woman's decision whether or not to terminate her pregnancy").

33. Loving v. Virginia, 388 U.S. 1, 12 (1967) (holding that "[u]nder our Constitution, the freedom to marry, or not marry, a person of another race resides with the individual and cannot be infringed by the State").

34. *See* Bowers v. Hardwick, 478 U.S. 186 (1986) (refusing to find a privacy right to protect certain intimate sexual practices from state criminal sanction). Recently, the Court granted certiorari on a challenge to the Texas anti-sodomy statute, *Lawrence v. State*, 41 S.W.3d 349 (Tex. App. 2001), which will provide an opportunity to revisit *Bowers*. Lawrence v. Texas, 123 S. Ct. 661 (2002) (granting petition for cert.)

2. *Informational Privacy*

A more recently developed "branch" of privacy law concerns personal information. While privacy in one's private facts was part of Warren and Brandeis' original conception of privacy,[35] and is implicit in the Fourth Amendment's protection of personal "papers,"[36] the idea of "personal information" as physically separable from the information's subject took longer to formulate. Even before the development of digital data, however, informational privacy interests surfaced.[37] As the modern, industrial society developed, various third parties—governments, banks, schools, and the like—regularly came into possession of the personal information of citizens, customers, and pupils. While this information was often intimate, the individual's right to protect it was unclear.

Common law and constitutional protection for informational privacy is sparse. The privacy torts are not readily applicable to misuse of personal information unless the information was taken from the victim directly or from some other private source, such as the victim's bank account.[38] Such a rule does not map well to situations in which one's personal information surfaces in the hands of a third party, such as a marketer.[39] The Constitution protects personal information against government intrusion, but this interest in "avoiding disclosure of personal matters" does not seem very broad.[40] As with the privacy torts, to receive protection, the information must be both subjectively and objectively 'private.'[41] While a few lower courts have found violations of informational privacy rights based on the Federal Constitution,[42] the Court seems inclined to take governments at their word as to the justification for collecting certain personal information.[43] State constitutions, while often containing stronger textual support

35. *See* Warren & Brandeis, *supra* note7, at 206.

36. U.S. CONST. amend. IV.

37. *See* Whalen v. Roe, 429 U.S. 589, 598-600 (1977).

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

39. Courts are unlikely to find misuse of "non-private" personal information to be "highly offensive to a reasonable person"—the general standard for the privacy torts. *Id.* at §§ 652B-E.

40. *See Whalen*, 429 U.S. at 599. In *Whalen v. Roe*, the Court refused to find that the government's recording of personal drug prescription information violated the constitutional right to privacy because the information was adequately protected. *Id.* at 600-02.

41. *See* Smith v. Maryland, 442 U.S. 735, 740 (1979) (stating no expectation of privacy in personal telephone call log, as possessed by the phone company);

42. *See, e.g.*, Doe v. Borough of Barrington, 729 F. Supp. 376, 382 (D.N.J. 1990) (concerning disclosure of Plaintiff's AIDS infection).

43. *See* Nixon v. Adm'r of Gen. Servs., 433 U.S. 425, 458 (1977); *Whalen*, 429 U.S. at 602.

for informational privacy,[44] have not been invoked often for that purpose.[45]

Statutes have filled in many of the holes left by the insufficiencies of common and constitutional law, but the myriad state and federal privacy statutes affecting informational privacy address narrow, specific issues rather than the breadth of the problem.[46] Commentators note that the statutory landscape is "riddled with exceptions" that often render the laws "ineffective."[47] At the federal level, the most complete statutory attempt to address the problem of misuse of information was also the first: the Privacy Act of 1974.[48] But while the Privacy Act sets out admirable and often-emulated[49] fair "information practices" (FIPs)[50] with which the gov-

---

44. Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina, and Washington all have privacy provisions in their constitutions that can arguably be applied to informational privacy. *See* Elbert Lin, Article, *Prioritizing Privacy: A Constitutional Response to the Internet*, 17 BERKELEY TECH. L.J. 1085, 1130 & n.276 (2002).

45. *Id.* at 1131. *But see, e.g.*, Tattered Cover, Inc. v. City of Thornton, 44 P.3d 1044, 1059 (Colo. 2002) (finding that the Colorado Constitution requires the government to show a compelling need for the specific personal information in order to lawfully collect it).

46. *See generally* MARC ROTENBERG, THE PRIVACY LAW SOURCEBOOK: UNITED STATES LAW, INTERNATIONAL LAW, AND RECENT DEVELOPMENTS (2002); ROBERT ELLIS SMITH, COMPILATION OF FEDERAL AND STATE PRIVACY LAWS (2002).

47. *See, e.g.*, Flavio K. Komuves, *We've Got Your Number: An Overview of Legislation and Decisions to Control the Use of Social Security Numbers as Personal Identifiers*, 16 J. MARSHALL J. COMPUTER & INFO. L. 529, 535 (1998) (discussing the statutory protection of privacy concerning Social Security Numbers).

48. 5 U.S.C. § 552a (2000).

49. *See* European Commission Council Directive 95/46/EC 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) 31, http://europa.eu.int/comm/internal_market/en/dataprot/law/dir1995-46_part1_en.pdf (adopting similar "fair information practices").

50. The Privacy Act FIPs are based on the Code of Fair Information Practices, developed in 1972 by the Department of Health, Education, and Welfare. The Code is based on five principles: (1) There must be no personal data record-keeping systems whose very existence is secret; (2) there must be a way for a person to find out what information about the person is in a record and how it is used; (3) there must be a way for a person to prevent personal information that was obtained for one purpose from being used or made available for other purposes without the person's consent; (4) there must be a way for a person to correct or amend a record of identifiable personal information; and, (5) any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data. SEC'Y'S ADVISORY COMM. ON AUTOMATED PERSONAL DATA SYSTEMS, U.S. DEP'T OF HEALTH, EDUC. & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS xxiii-xxvi (1973), *available at* http://aspe.hhs.gov/datacncl/1973privacy/tocprefacemembers.htm; *see* 5 U.S.C. § 552a(d).

ernment must comply, the Act only applies to such state-issued or — collected information as welfare benefit data and Social Security Numbers.[51] Furthermore, the Privacy Act is limited by exceptions for "routine use"[52] and by the Freedom of Information Act.[53]

Other federal laws vary in usefulness, but all are limited in scope to their own narrow swath of informational privacy.[54] Other than the Privacy Act, the most important laws in this area are the Fair Credit Reporting Act (FCRA),[55] portions of the Computer Fraud and Abuse Act (CFAA),[56] and the Electronic Communications Privacy Act (ECPA).[57] These laws are all valuable in limited circumstances, but cannot serve as the basis for a generalized protection of informational privacy.[58] The clearest example of this piecemeal statutory approach recently is the Children's Online Privacy Protection Act (COPPA).[59] The COPPA, the only law to specifically target online informational privacy,[60] applies only to websites that collect information from children.[61]

---

51. 5 U.S.C. § 552a(a) (limiting the application of the Privacy Act to government agencies keeping certain types of personal records).

52. This language allows the government significant leeway to determine what uses of information are necessary in the administration of its duties. *See* PRIVACY AND HUMAN RIGHTS, *supra* note 8, at 384.

53. 5 U.S.C. § 552.

54. *See, e.g.*, Video Privacy Protection Act, 18 U.S.C. § 2710 (2002) (passed to protect video rental records in reaction to the disclosure of Judge Robert Bork's rental list by a Washington, D.C. paper during his ill-fated Senate confirmation hearings). Notably, the Act does not extend protection to similar records for rental of video games, and its applicability to Digital Video Disks (DVDs) and online streaming video is unresolved. *See* Video Privacy Protection Act (VPPA), Electronic Privacy Information Center, *at* http://www.epic.org/privacy/vppa/ (last updated Aug. 6, 2002).

55. 15 U.S.C. § 1601 (limiting use of certain personally identifiable financial information in the credit and financial industries, and requiring credit agencies to make personal credit histories and ratings available to their owners).

56. 18 U.S.C. § 1030 (creating criminal and civil penalties for certain computer-related intrusions into personal property).

57. 18 U.S.C. §§ 2510-2520, 2701 (1997) (encompassing the Wiretap Act (Title I) and the Stored Communications Act (Title II), both designed to protect private communications, such as email, from unwarranted government and private intrusion). *See also* Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002) (finding employer's serendipitous viewing of employee union website and private postings thereon did not violate the ECPA).

58. *See, e.g.*, Jonathan P. Cody, Comment, *Protecting Privacy Over the Internet: Has the Time Come to Abandon Self-Regulation?*, 48 CATH. U.L. REV. 1183, 1200 (1999) (describing the failure of the ECPA to broadly protect communications privacy).

59. 15 U.S.C. §§ 6501-6506.

60. Lin, *supra* note 44, at 1112.

61. *Id.*; *see also* 15 U.S.C. § 6502.

State legislatures have been, on the whole, the most promising venue for new informational privacy protections, but even when statutory language suggests broad, general privacy protections, state laws are proscribed by jurisdictional limits and the states' weak enforcement abilities.[62] Specific state laws, while often stronger than equivalent protections at the federal level, are often difficult to enforce in a world where in-state violations are committed by persons located out-of-state.[63] Even if a state were to pass an omnibus, cohesive package of privacy protections, such a law would be incapable of addressing what is (at the least) a national problem.

B. The Impact of Digital Technology

The last generation has seen technological change on a scale matching or exceeding that of the industrial revolution.[64] This "digital revolution" has not left privacy untouched.[65] Jerry Berman and Deirdre Mulligan note three major digital developments that deeply affect privacy: (1) the increase in data creation and the resulting collection of vast amounts of personal data—caused by the recording of almost every modern interaction; (2) the globalization of the data market and the ability of anyone to collate and examine this data; and (3) lack of the types of control mechanisms for digital data that existed to protect analog data.[66]

These three developments all concern the changes wrought by digital technology on the ability to manipulate information. First, the amount of digital information generated is breathtaking.[67] Every interaction with the Internet, every credit card transaction, every bank withdrawal, every

62. For example, a new California law provides residents with stronger protection of their Social Security Numbers and against credit fraud. CAL. PENAL CODE §§ 530.5-530.7 (2002). A new Georgia law prevents businesses from discarding records that may contain their customers' personal information. GA. CODE ANN. §§ 16-9-121, 127 (2002). *See generally* SMITH, *supra* note 46.

63. Even were the states to expand their prosecutory resources, they are limited by state sovereignty and the federal Constitution's Commerce Clause. *See* Lin, *supra* note 44, at 1117.

64. *See* Eugene R. Quinn, Jr., *Tax Implications for Electronic Commerce over the Internet*, 4.3 J. TECH. L. & POL'Y 1, 50 (1999) (claiming that the "so-called 'digital revolution' has the potential to cause societal change on a magnitude that is even greater than that caused by the Industrial Revolution").

65. *See* Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1394 (2001) (describing the impact of digital technology on "the way we shop, bank, and go about our daily business").

66. Berman & Mulligan, *supra* note 5, at 554-56.

67. *See* Froomkin, *supra* note 2, at 1468-1501.

magazine subscription is recorded digitally and linked to specific individuals. In the analog world, these transactions were either not recorded at all[68] or recorded on paper in a single location. Second, all this information, once it is collected in networked databases, can be sent instantly and cheaply around the globe.[69] In this newly-commoditized information market, buyers anywhere can collate and manipulate the data for marketing,[70] profiling,[71] or more sinister[72] purposes. Third, individuals have little ability to control this collection or manipulation. Not only does much of this happen far from the reach of regulators, but most people are not even aware what information has been collected or how it is being used.[73]

But while all of these changes affect information, not only informational privacy has been affected. Autonomy, too, faces threats from digital technology.[74] When almost every activity leaves a digital trail, government and private monitoring become less about analog surveillance and more a matter of "data mining."[75]

---

68. Compare old-fashioned cash commerce with "e-commerce" in which a website tracks your "clickstream" through use of "cookies," ad-servers track your viewing, and credit companies record your purchase. *See In re* DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 497, 501-05 (S.D.N.Y. 2001).

69. *See* Berman & Mulligan, *supra* note 5, at 555.

70. *See* Trans Union v. FTC, 81 F.3d 228 (D.C. Cir. 1996) (holding that the sale of consumer credit reports for marketing purposes violated the FCRA).

71. *See* Privacy and Consumer Profiling, Electronic Information Privacy Center, *at* http://www.epic.org/privacy/profiling/ (last updated Oct. 3, 2002) (describing data profiling, the market for it, and associated privacy concerns).

72. *See* Remsburg v. Docusearch, Inc., 2003 N.H. LEXIS 17 at *4-7 (N.H. 2002) (describing stalker's collection of his victim's personal financial and location information for use in carrying out murder of the victim).

73. *See* Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1095 (2002).

74. As do other areas of privacy. For example, digital technology threatens the ability to participate anonymously in digital society because every digital interaction leaves personally identifiable fingerprints. *See generally* Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981 (1996). Technologies like digital rights management could prevent consumers from watching movies or listening to music online without being monitored. *See* Megan E. Gray & Will Thomas DeVries, *The Legal Fallout from Digital Rights Management Technology*, COMPUTER & INTERNET LAWYER (forthcoming April 2003) (manuscript on file with author). Lawsuits against anonymous Internet posters employ discovery to compel ISPs to reveal user identities. *See, e.g.*, Doe v. 2themart.com, Inc., 140 F. Supp. 2d 1088, 1094 (W.D. Wash. 2001).

75. *See generally* Joseph S. Fulda, *Data Mining and Privacy*, 11 ALB. L.J. SCI. & TECH. 105 (2000). Professor Fulda defines data mining as "the intelligent search for new knowledge in existing masses of data"). *Id.* at 106. Data mining shows the difficulty of easy categorization of privacy harms; the informational privacy "branch" is obviously

The impact of digital technology on privacy superficially seems like the same pattern seen with older technologies; the law will attempt to evolve in response to the privacy threats posed by the digital revolution,[76] just as it did with the telephone[77] or the VCR.[78] But the impact of the digital age is so deep and pervasive that expansion of a single area of privacy law is unlikely to adequately address the problems. In essence, the *scale* is different. Since the digital age affects every aspect of privacy, it requires an evolution not just in the existing framework, but in the very conceptual and legal status of privacy. Current battles over privacy rights illustrate this.

II. PRIVACY BATTLES IN THE DIGITAL AGE

The conceptually discrete branches of privacy on their own fail to adequately address the privacy concerns of the digital age. This Part examines current activity in each of the three branches of privacy law described above with respect to the development of digital technology.

A. Reviving Big Brother

Digital technology has revived the most pervasive privacy metaphor of the last fifty years:[79] Orwell's infamous Big Brother.[80] As developed in *Nineteen Eighty-Four*, Orwell's vision of an all-seeing, ever-searching, omnipresent eye of government has dominated the metaphoric landscape

---

implicated by technology that allows the collection and possible misuse of such vast amounts of data. *See* Froomkin, *supra* note 2, at 1468-1501.

76. *See* Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1374 (2000); Hernandez, *supra* note 4, at 429.

77. *Compare, e.g.*, Olmstead v. United States, 277 U.S. 438, 464 (1928) (finding no reasonable expectation of privacy in phone conversations), *with* Katz v. United States, 389 U.S. 347, 353, 359 (1967) (criticizing *Olmstead* and finding a right to privacy in telephone booth conversations).

78. The Video Privacy Protection Act, 18 U.S.C. § 2710, was passed subsequent to the development of the VCR and video rental industry. Lawmakers feared misuse of movie rental lists, which were preserved on an individual basis as never before. *See* Video Privacy Protection Act (VPPA) website, *supra* note 54. While some might argue that privacy law is often passed in anticipation of (not in reaction to) new technological developments, even when laws are passed in anticipation of new technological threats, the driving force is still technology. *See, e.g.*, Cable Communications Act of 1984, Pub. L. No. 98-549, 98 Stat. 2779 (1984) (codified as amended in scattered sections of 47 U.S.C.).

79. *See* Solove, *supra* note 65, at 1395-96.

80. GEORGE ORWELL, NINETEEN EIGHTY-FOUR (New American Library 1983) (originally published 1949).

of the modern privacy debate.[81] The Big Brother metaphor lives on in the digital age—and now Big Brother actually possesses the technological and legislative tools to prevent any meaningful escape from his gaze. Indeed, use of digital technology by the government has caused many to lament the growing irrelevancy of the Fourth Amendment and the "right to be let alone."[82]

1. 'Carnivore' and Digital Surveillance

Crime has gone high tech, and crime-fighting has followed. The digital age has changed crime and criminal investigation much as it has every other sector of the law and society.[83] New tools of digital surveillance allow more effective and complete monitoring by police than has ever been possible before. The digital trail each individual generates can be tracked by investigators, both public[84] and private, easily and cheaply.[85] Beyond physical surveillance, police can use digital technology to search a suspect's ISP for incriminating information without leaving headquarters[86] or to spot possible criminals at the Superbowl using face recognition software.[87]

To address the changing times, the Federal Bureau of Investigation (FBI) developed "Carnivore,"[88] digital monitoring software that allows

---

81. *See* Solove, *supra* note 65 at 1395-96.

82. See generally Steven A. Osher, Privacy, Computers and the Patriot Act: The Fourth Amendment Isn't Dead, But No One Will Insure It, 54 FLA. L. REV. 521 (2002).

83. *See generally* Aaron Burstein, Note, *A Survey of Cybercrime in the United States*, 18 BERKELEY TECH. L.J. ___.

84. This section discusses Federal law-enforcement, but it should be noted that state officials are by far the larger consumers of surveillance technologies. *See* Title III Electronic Surveillance 1968-1999, Electronic Privacy Information Center, *at* http://www.epic.org/privacy/wiretap/stats/wiretap_stats.html (last visited Dec. 19, 2002).

85. The federal government is planning an extensive "data mining" operation called Total Information Awareness. *See infra* Part II.B.4.

86. *See* United States v. Bach, 310 F.3d 1063 (8th Cir. 2002), *reh'g denied*, 2003 U.S. App. LEXIS 141 (8th Cir. 2003) (allowing officers to execute a warrant for search of records stored at an out-of-state ISP remotely).

87. Alexander T. Nguyen, *Here's Looking at You, Kid: Has Face-Recognition Technology Completely Outflanked the Fourth Amendment?*, 7 VA. J.L. & TECH. 2, ¶ 8 (2002).

88. This Note refers to the software as "Carnivore," though the FBI renamed the newest version "DCS-1000." *See* Aaron Y. Strauss, Note, *A Constitutional Crisis in the Digital Age: Why the FBI's "Carnivore" Does Not Defy the Fourth Amendment*, 20 CARDOZO ARTS & ENT. L.J. 231, 232 n.6 (2002) (noting that "because the name conjured up 'so many unflattering images of flesh-eating animals' the FBI decided to switch the name").

FBI officers to monitor suspects' online communications.[89] The FBI "taps" into Internet Service Providers (ISPs) using Carnivore. The software then scans huge volumes of communications for those fitting the search criteria—flagging and storing any messages meet those criteria.[90] Carnivore thus allows the monitoring of vast amounts of personal information without a dramatic increase in marginal costs.[91]

Carnivore, contends the FBI, is not as privacy invasive as other "packet-sniffing" tools, which generally search digital data for certain criteria, because Carnivore can screen out irrelevant or privileged communications.[92] It analyzes the content of the data (e.g., email messages) that meets the search criteria and saves only those relevant to the investigation and within the scope of a court order.[93] It is unclear how true these claims are in practice, however, since little data are available on Carnivore's actual use. Notably, in one of the few publicized incidents, FBI documents revealed that in one investigation, Carnivore mistakenly flagged emails belonging to non-targeted individuals.[94] The FBI technician, knowing the emails were not covered by the court order, erased all of the search results, including emails to and from the target—a suspected terrorist linked to Osama Bin Laden.[95]

2. *The USA PATRIOT Act*

Until September 11, 2001, the rules governing digital surveillance of digital data were in legislative limbo. Government prosecutors and civil libertarians had been haggling over the correct standards to apply to "taping" of digital communications for several years, and meanwhile the old

---

89. E. Judson Jennings, *Carnivore: US Government Surveillance of Internet Transmissions*, 6 VA. J.L. & TECH. 10, ¶ 3 (2001).

90. *See id.* at ¶ 5; Orin. S. Kerr, *Internet Surveillance Law After the USA PATRIOT Act: The Big Brother that Isn't*, 97 NW. U.L. REV. (forthcoming 2003) (manuscript at 55-57, on file with author).

91. While privacy advocates are concerned about the possibilities for misuse of Carnivore, *see* Jennings, *supra* note 89 at ¶ 6, it has yet to generate any privacy litigation. The only published opinion discussing Carnivore, as of this writing, concerns the disclosure of information by the FBI about the program with respect to the Freedom of Information Act. *See* Judicial Watch, Inc. v. FBI, 190 F. Supp. 2d 29 (D.D.C. 2002).

92. *See* Kerr, *supra* note 90 (manuscript at 57).

93. *See* MARK LEMLEY ET. AL., SOFTWARE AND INTERNET LAW 911 (2d ed., 2003).

94. *See* Press Release, Electronic Privacy Information Center, FBI's Carnivore System Disrupted Anti-Terror Investigation (May 28, 2002), *at* http://www.epic.org/privacy/carnivore/5_02_release.html.

95. *See id.*; Electronic Privacy Information Center, *FBI Memo on 'FISA Mistakes'*, *at* http://www.epic.org/privacy/carnivore/fisa.html (memo dated April 5, 2000).

rules for telephone and other surveillance had been applied to the Internet by default.[96] Then things changed. Within weeks of September 11th, Congress passed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act—more often known by its intentional acronym, USA PATRIOT Act, or just as the Patriot Act.[97]

With very little congressional debate, the Patriot Act sped through Congress[98]—the haste in response to the perceived inability of authorities to track and uncover terrorist plots.[99] The laws overall effect, however, has had less to do with terrorism than with easing restrictions on government surveillance of digital communications.[100] The effect of September 11th was thus to preempt the ongoing debate over these standards and resolve it firmly in favor of the government prosecutors.[101]

The Patriot Act, an amalgam of provisions of several earlier bills,[102] generally loosens the procedural and substantive limits regarding government investigative and surveillance powers, both foreign and domestic.[103] It allows broader sharing of gathered information between law enforcement and intelligence agencies,[104] amends the Foreign Intelligence Surveillance Act (FISA) to expand the federal government's ability to investigate and search foreign entities and organizations,[105] allows law enforcement to install "roving wiretaps"[106] and to obtain "pen registers" and

---

96. *See* Kerr, *supra* note 90 (manuscript at 34-35).

97. Pub. L. No. 107-56, 115 Stat. 272 (2001).

98. *See* Kerr, *supra* note 90 (manuscript at 2).

99. *See* The USA PATRIOT Act, Electronic Privacy Information Center, *at* http://www.epic.org/privacy/terrorism/usapatriot/ (last updated Oct. 31, 2002) [hereinafter EPIC USA PATRIOT Act Web page].

100. *See* John Podesta, *USA Patriot Act: The Good, the Bad, and the Sunset*, ABA NETWORK, Winter 2002, *at* http://www.abanet.org/irr/hr/winter02/podesta.html.

101. *See id.* Clinton White House Chief-of-Staff John Podesta notes that "[m]any of the electronic surveillance provisions in the Patriot Act faced serious opposition prior to September 11 from a coalition of privacy advocates, computer users, and elements of the high-tech industry." *Id.*

102. *See* EPIC USA PATRIOT Act Web page, *supra* note 99 (noting that "[m]any of the provisions of the Act relating to electronic surveillance were proposed before September 11th").

103. *Id.*

104. USA PATRIOT Act §§ 203, 504, 701.

105. *Id.* §§ 214-18. *See also* Global Relief Found., Inc. v. O'Neill, 207 F. Supp. 2d 779, 807 (N.D. Ill. 2002) (dismissing Global Relief's privacy claims based on interception of its digital communications on the grounds that the plaintiff, despite being a U.S. corporation, was now considered a foreign entity under the revised FISA).

106. A "roving" wiretap is a wiretap order allowing investigators to monitor communications from a suspect regardless of the instrument of communication (telephone, mo-

"trap and trace"[107] orders for telephones—and now for computers—with less procedural barriers.[108] The Patriot Act also implicitly enshrines Carnivore into law by defining the digital surveillance provisions to include the type of search Carnivore performs.[109] Most importantly, the Act *requires* judges to sign orders authorizing these searches without allowing the court to review the efficacy or legitimacy of the request.[110]

Privacy advocates, not surprisingly, are unhappy with the Patriot Act. They point out the possibilities for prosecutorial misuse and limited judicial oversight.[111] But the new law's impact on privacy rights is not as clear as its media image would indicate.[112] First, the Act contains an explicit sunset provision affecting many of the surveillance provisions.[113] Moreover, even where the Act allows secret searching and broader sharing of information, government agents must submit (under seal) the results of their activities to a reviewing judge.[114] Also, the FISA amendments expressly prohibit using the new surveillance power expressly to interfere with a citizen's First Amendment rights.[115] Orin Kerr, who drafted sub-

---

bile phone, etc.). *See* USA PATRIOT Act § 206 (amending the FISA to allow broader use of such surveillance).

107. "A pen register collects the outgoing phone numbers placed from a specific telephone line; a trap and trace device captures the incoming numbers placed to a specific phone line—a caller-id box is a trap and trace device"). *See* EPIC USA PATRIOT Act Web page, *supra* note 99.

108. USA PATRIOT Act §§ 214-218. In May 2002, the "secret" Foreign Intelligence Surveillance Court struck many of the new wiretap provisions as unconstitutional violations of the Fourth Amendment, but a three-judge panel of the Court of Appeals for the District of Columbia overturned the ruling and upheld the new provisions. In re Sealed Case No. 02-001, slip op. (United States Foreign Intelligence Surveillance Court of Review 2002), *available at* http://www.cadc.uscourts.gov/common/newsroom/02-001.pdf. The case is unlikely to be taken by the Supreme Court, since the Patriot Act does not provide for appeals beyond this secret appellate court composed of D.C. Circuit judges. *See id.* § 412.

109. *See id.* § 216.

110. *See, e.g., id.* § 216 (requiring that "the court *shall* enter an ex parte order authorizing the installation and use of a pen register or trap and trace device within the jurisdiction of the court, if the court finds that the State law enforcement or investigative officer *has certified to the court* that the information likely to be obtained by such installation and use is *relevant to an ongoing criminal investigation*") (emphasis added).

111. *See* EPIC USA PATRIOT Act Web page, *supra* note 99.

112. *See, e.g.*, Stefanie Olsen, *Patriot Act draws privacy concerns*, CNET, Oct. 26, 2001, *at* http://news.com.com/2100-1023-275026.html.

113. USA PATRIOT Act § 224.

114. *Id.* § 203. Even privacy advocates admit that this amendment "provides vital judicial oversight of the use of this enhanced surveillance authority." EPIC USA PATRIOT Act Web page, *supra* note 99.

115. *Id.* § 214.

stantial portions of the language that became the Patriot Act,[116] argues that, on the whole, the Patriot Act does not endanger privacy and in fact may bolster it.[117] In addition to the above elements, he points out that the types of digital surveillance allowed are necessary to deal with modern crime and anyway are tightly constrained so as to protect privacy.[118] While Professor Kerr's views appear to be in the minority, the full impact of this law on privacy is to be determined.

B. From Orwell to Kafka: The Ubiquity of Personal Information

The power of Orwell's Big-Brother metaphor is so powerful that writers have attempted to graft it onto other privacy areas.[119] With respect to the digital aggregation, collation, and distribution of personal information, however, Daniel Solove suggests that the better metaphor is Franz Kafka's *The Trial*.[120] The problem is less the all-seeing eye of Big Brother (or any other family member) and more the "dehumanization" of having one's most intimate information circulated by an indifferent and faceless infrastructure without any control over the process or content.[121] In *The Trial*, the protagonist faced a bureaucracy whose rules he did not understand and could not control, yet who knew every intimate fact and could exercise authority over him.[122] This metaphor seems appropriate to the problem of informational privacy.

1. Financial Information

Banks and financial institutions have gradually realized that they sit atop a horde of digital gold: their customers' personal information.[123] Information like customer names, addresses, Social Security Numbers (SSNs), income bracket, and credit status are increasingly valuable to marketers and other parties.[124] Since current constitutional doctrine does not extend the "reasonable expectation of privacy" to information not

---

116. Kerr, *supra* note 90 (manuscript at 4).

117. *Id.* at 2-3.

118. *Id.*

119. For example, private sector monitors are often referred to as "Little Brothers." *See* Solove, *supra* note 65, at 1398 & n.12.

120. FRANZ KAFKA, THE TRIAL (Willa & Edwin Muir trans. 1937); *see* Solove, *supra* note 65, at 1398.

121. *See* Solove, *supra* note 65, at 1398-99.

122. KAFKA, *supra* note 120, at 147-48.

123. *See* Neal R. Pandozzi, *Beware of Banks Bearing Gifts: Gramm-Leach-Bliley and the Constitutionality of Federal Financial Privacy Legislation*, 55 U. MIAMI L. REV. 163, 163 (2001).

124. *See* Janet Dean Gertz, Comment, *The Purloined Personality: Consumer Profiling in Financial Services*, 39 SAN DIEGO L. REV. 943, 950-51 (2002).

strictly within the control of the individual,[125] statutory regulation provides the only legal privacy guidelines for this industry.[126]

The financial information market has been the subject of increased scrutiny recently, as a result of the increasing ease of transferring and re-using personal information and the resulting danger of misuse. In 1999, Congress passed the Financial Services Modernization Act, known as the Gramm-Leach-Bliley Act (GLBA) after its eponymous Senate sponsors.[127] The GLBA was intended primarily to "eliminate many Federal and State law barriers to affiliations among" financial institutions,[128] but it also contained new privacy regulations to protect "nonpublic personal information."[129] In response, the Federal Trade Commission (FTC) promulgated fairly strong new privacy regulations under the GLBA.[130]

In response to the FTC's regulations, the credit reporting agency Trans Union, a company with a long history of questionable use of personal financial information,[131] sued the FTC. Trans Union alleged that the FTC's definition of personal information was overbroad and that limits on their distribution and reuse of information such as name, address, and SSN was

125. *See* Smith v. Maryland, 442 U.S. 735, 740 (1979).

126. Until 1999, the most important federal regulation of this industry was the Fair Credit Reporting Act of 1970 (FCRA), 15 U.S.C. § 1681 (2000), which placed some limits on the distribution of personal credit information, but excluded "credit headers," which includes name, address, and SSN, from protection. *See* Trans Union LLC v. FTC, 295 F.3d 42, 50-51 (D.C. Cir. 2002) [hereinafter *Trans Union II*].

127. Pub L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 U.S.C. and 15 U.S.C.). *See generally* Jolina C. Cuaresma, Note, *The Gramm-Leach-Bliley Act*, 17 BERKELEY TECH. L.J. 497 (2002).

128. H.R. CONF. REP. NO. 106-434, at 1 (1999).

129. *See* 15 U.S.C. §§ 6801-09 (2002); *Trans Union II*, 295 F.3d at 46 (noting the new requirements that consumers be permitted to "opt-out" of certain information disclosures and allowing various agencies to further regulate the industry).

130. The FTC broadly defined "personally identifiable financial information" (PIFI) to include "credit headers," which thus required the same consumer opt-out provisions as other financial information, and limits the ability of financial institutions to re-use customer data for new purposes without additional opt-out permission. *See* Privacy of Consumer Financial Information, 16 C.F.R. §§ 313.3, 313.11; *Trans Union II*, 295 F.3d at 49-52.

131. *See In re* Trans Union Corp. Privacy Litig., 2002 U.S. Dist. LEXIS 17209 (N.D. Ill.) (dismissing Plaintiffs' class-action FCRA claim alleging privacy violations arising from the sale of their information to a tele-marketer on the basis that the statutory damages involved—$19 billion—would bankrupt the Defendant); Trans Union Corp. v. FTC, 245 F.3d 809 (D.C. Cir. 2001) [hereinafter *Trans Union I*], *cert. denied* 122 S. Ct. 2386 (2002) (dismissing Trans Union's claims that the FTC had infringed their freedom of speech by banning the sale of "consumer reports" without approval under the FCRA).

a violation of their free speech rights.[132] The district court dismissed all claims and granted summary judgment to the FTC.[133] On appeal, the D.C. Circuit affirmed, noting that the FTC acted within its discretion in broadly defining personal information.[134] The court breezed through Trans Union's free speech claim, noting that speech was purely "commercial," and its restriction supported by legitimate state interests.[135]

This case illustrates how financial privacy vexes traditional notions of privacy. First, the court implicitly recognized the important role the FTC is playing in protecting informational privacy, but had trouble expressing the legal basis for such a role.[136] If the Constitution does not recognize a privacy right in financial information,[137] and the authorizing statute does not expressly include the right to limit the distribution of information such as the SSN,[138] how can the FTC suddenly have such power? Second, the court dismisses the free speech claim, but cannot articulate clearly why informational privacy interests (the protection of which has not been defined as a compelling state interest) can trump the right to disseminate ostensibly "public" information.[139] The court recognized the privacy interest, but given the status of informational privacy, it had to grasp for a way to protect it.[140]

2. *Public Records and the Decline of Practical Obscurity*

One of the most treasured aspects of the modern American system of government is the openness with which all proceedings occur. A necessary

---

132. Individual References Serv. Group, Inc. v. FTC, 145 F. Supp. 2d 6 (D.D.C.) [hereinafter *ISRG*], *aff'd*, *Trans Union II*, 295 F.3d 42 (D.C. Cir. 2001).

133. *Id.*

134. *Trans Union II*, 295 F.3d at 51.

135. *Id.* at 52. The court held similarly with respect to the free speech claims brought by Trans Union against the FTC a year earlier in *Trans Union I*. 245 F.3d at 818-19. Notably, two justices dissented to the denial of the *certiorari* petition in that case, arguing that the financial information at issue here was "speech" that "touches upon matters of public concern," and thus deserved strict scrutiny. Trans Union LLC v. FTC, 122 S. Ct. 2386, 2387 (2002) (denial of cert.) (Kennedy, J., dissenting).

136. *See Trans Union II*, 295 F.3d at 47 (describing the power granted to the FTC under the GLBA and the Federal Trade Commission Act).

137. *See* Smith v. Maryland, 442 U.S. 735, 740 (1979).

138. *See Trans Union II*, 295 F.3d at 49-50.

139. *See id.* at 52; *Trans Union I*, 122 S. Ct. 2386, 2387 (2002) (Kennedy, J., dissenting from denial of cert.) *See generally* Paul M. Schwartz, *Free Speech vs. Information Privacy: Eugene Volokh's First Amendment Jurisprudence*, 52 STAN. L. REV. 1559 (2000).

140. The court employed the "commercial speech doctrine." *See Trans Union II*, 295 F.3d at 52-53; *see generally* Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749 (1985).

corollary of this system is the creation of a vast array of public records documenting the ongoing affairs of government—from the federal to the very local.[141] These records are often intimately personal: by the end of his life, an individual may have generated public records ranging from their birth certificate, immunization records, and school loans to driving records, marriage certificate, divorce proceedings, bankruptcy filings, and collection of social security benefits.[142] The records for those involved in direct court or criminal proceedings can be especially revealing.[143]

Digital technology is turning the asset of open government into a privacy nightmare. In the analog age, public records were all available, but languished in "practical obscurity" in courthouse basements or isolated file cabinets.[144] The records were difficult to locate or assemble into a useful dossier short of hiring a team of investigators to traipse into government offices around the country.[145] The digital age changed this rubric. Government records are stored digitally, and often linked to the Internet or other networks.[146] Specialized companies regularly compile these databases and allow, for a fee, customers to search and download the records they want.[147] Even worse, many state governments (like financial institutions) have attempted to profit through the sale of publicly held personal information, such as driving records.[148]

"Megan's Law" statutes are a troubling example of the privacy problems resulting from open records. Megan's Laws require sex offenders to register their names and addresses in order to alert local residents to the

---

141. *See* Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1142-43 (2002).

142. *See id.* at 1143-44.

143. *See id.* at 1147-48.

144. *See* DOJ v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 762 (1989).

145. *See* Matthew D. Bunker et. al., *Access to Government-Held Information in the Computer Age: Applying Legal Doctrine to Emerging Technology*, 20 FLA. ST. U.L. REV. 543, 583 (1993).

146. *See* Solove, *supra* note 141, at 1152-53; *see generally* Ctr for Democracy & Tech., *A Quiet Revolution in the Courts: Electronic Access to State Court Records: A CDT Survey of State Activity and Comments on Privacy, Cost, Equity and Accountability*, *at* http://www.cdt.org/publications/020821courtrecords.shtml (last visited Nov. 21, 2002).

147. See Solove, *supra* note 141, at 1153.

148. For example, many states were, until recently, in the business of selling personal information from state departments of motor vehicles. *See id.* at 1150. The Driver's Privacy Protection Act (DPPA) was passed in 1994 to curtail this practice. 18 U.S.C. §§ 2721-25 (2000). The Supreme Court later upheld the statute as a valid exercise of Commerce Clause power. Reno v. Condon, 528 U.S. 141, 144-45 (2000).

dangers such offenders may pose.[149] Increasingly, states are publishing their Megan's Law lists on the Internet—making them available to anyone in the world, not just the offender's neighbors.[150] Privacy challenges to traditional Megan's Law registries have failed.[151] A recent Supreme Court challenge to Internet Megan's Law registries, which argued that the *ex post facto* penalties inherent in such wide dissemination are unconstitutional, was no more successful.[152]

3. *Medical Privacy*

Medical information is almost always sensitive. Having the world learn about one's Prozac prescription can be embarrassing;[153] having the world learn about one's HIV-positive status can be life-shattering.[154] While digital technology can save money and allow life-saving medical information to be instantly sent between hospitals and doctors, the same technology also heightens the possibility of mistake or misuse.[155]

The legal framework around medical privacy is a patchwork. The Supreme Court did not elevate privacy rights in medical information to the same level as for physical privacy or decisional autonomy, though the Court acknowledges the existence of the privacy right.[156] Recognizing a

149. Megan's Laws get their name from the highly publicized murder of a young girl by a convicted sex-offender who lived nearby. *See* Elec. Privacy Info. Ctr., *The Supreme Court Set to Review Alaska's Megan's Law*, *at* http://www.epic.org/privacy/meganslaw/ (last updated Nov. 14, 2002). All 50 states and the federal government have Megan's Laws. *See* Solove, *supra* note 141, at 1148-49.

150. *See, e.g.*, Doe v. Otte, 259 F.3d 979, 984 (9th Cir. 2001), *rev'd*, Smith v. Doe, 123 S. Ct. 1140, 2003 U.S. LEXIS 1949 (Mar. 5, 2003) (describing Alaska's Megan's Law registry, which is posted on the Internet).

151. *See* Paul P. v. Verniero, 170 F.3d 396, 404 (3d Cir. 1999) (upholding New Jersey's Megan's Law); Russell v. Gregoire, 124 F.3d 1079, 1093-94 (9th Cir. 1997) (upholding Washington's Megan's Law on the basis that the information is already public).

152. *See* Smith v. Doe, 2003 U.S. LEXIS 1949 at *40.

153. *See In re* Eli Lilly & Co., FTC No. 012 3214, Agreement Containing Consent Order (2002) (describing Eli Lilly's disclosure of the email addresses of many of its Prozac customers).

154. *See* Doe v. Borough of Barrington, 729 F. Supp. 376, 379 (D.N.J. 1990) (describing how, after his HIV status was made public, the Plaintiff "suffered harassment, discrimination, and humiliation" and was "shunned by the community"); Doe v. SEPTA, 72 F.3d 1133, 1136-37 (3d Cir. 1995) (describing the social ostracism Plaintiff experienced after his HIV status was revealed through examination of his drug prescription records).

155. *See* Paul M. Schwartz, *Privacy and the Economics of Personal Health Care Information*, 76 TEX. L. REV. 1, 3, 12-14 (1997).

156. *See* Whalen v. Roe, 429 U.S. 589, 598-600 (1977).

need for protection in the face of digital distribution of health information, Congress passed the Health Insurance Portability and Accountability Act (HIPAA) in 1996.[157] Though the HIPAA was passed primarily to enable employees to switch employers without losing health coverage for existing conditions, it also requires states to enact certain privacy protections, such as obtaining consent prior to distributing personal information to marketers.[158] Plaintiffs have sought to employ other privacy laws, such as the ECPA and CFAA, to pursue claims related to misuse of digital medical data, but with little success.[159]

Two medical privacy problems are telling examples of the impact of the digital world. First, individual genetic information increasingly is stored in personal medical files.[160] Misuse of such information can often lead to discrimination in employment or in other circumstances.[161] Second, drug prescription information, stored by retail chains, HMOs, and drug companies, is often unintentionally released or misused.[162] The FTC recently settled with drug giant Eli Lilly for accidentally disclosing the email addresses of hundreds of users of its Prozac.com website.[163] Though the FTC's action was laudatory, the lack of any civil remedy for those injured by the disclosure is evidence of the failure of the current informational privacy regime to cope with the digital age.

4. Digital Dossiers and 'Total Information Awareness'

During World War II, Josef Stalin was asked about German proclamations that, though his army may be great in numbers, the German soldiers

157. Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 18, 26, 29 and 42 U.S.C.).

158. *See* §§ 701, 1177.

159. For example, a recent class action suit against the pharmaceutical industry alleged that the industry was using "cookies" to monitor Internet use by customers—often revealing other companies from which the customers were buying drugs. *In re* Pharmatrak, Inc. Privacy Litig., 220 F. Supp. 2d 4, 9 (D. Mass. 2002). The resulting database included "names, addresses, telephone numbers, dates of birth, sex, insurance status, medical conditions, education levels, and occupations" of individual customers. *Id.*

160. At this point, such information is usually genetic pre-disposition to certain conditions, but soon, one's entire DNA sequence may be stored in databases. *See* Radhika Rao, *A Veil of Genetic Ignorance? Protecting Privacy as a Mechanism to Ensure Equality*, 54 HASTINGS L.J. (forthcoming 2003) (manuscript at 1, on file with author).

161. *See* Schwartz, *supra* note 155, at 1. In 2000, President Clinton issued an executive order to "Prohibit Discrimination in Federal Employment Based on Genetic Information," which banned such discrimination by federal agencies. Exec. Order No. 13,145, 65 Fed. Reg. 6,877 (Feb. 10, 2000).

162. *See, e.g.*, *SEPTA*, 72 F.3d at 1136-37.

163. *In re* Eli Lilly & Co., FTC No. 012 3214, Agreement Containing Consent Order.

would prevail due to their superior quality. He supposedly replied that "*quantity* has a quality all its own." So, too, with personal data. While occasionally the unwanted revelation of a single private fact can be disastrous, informational privacy harms are today more likely to result from the aggregation and distribution of vast amounts of the daily detritus of digital life—from the most intimate fact to the most banal.[164]

The collection of "digital dossiers," as Daniel Solove calls this information aggregation,[165] is done by public and private actors—each for their own purposes. Private entities collect this information for "profiling" and marketing purposes.[166] Legal relief for misuse of accumulated personal information by private actors has been spotty at best.[167] In 2001, a lawsuit claiming misuse of aggregated web-browsing information by Internet ad-server DoubleClick was summarily dismissed by the trial court.[168] More encouragingly, the FTC announced in the summer of 2002 a settlement with software giant Microsoft based on misuse of personal data collected by its Passport service.[169] The FTC found that Microsoft had defrauded customers by convincing them to give up their information under the pretext of privacy,[170] and required the company to submit to 20 years of annual privacy audits.[171] It seems unlikely, though, that customers would have had any redress had the FTC not acted.

---

164. *See* Solove, *supra* note 17, at 1089-90.

165. *Id.*

166. *See supra* note 71 and accompanying text.

167. Compare the European Commission Council Directive 95/46/EC, 1995 O.J. (L 281) 31, which requires private parties in Europe to comply with certain Fair Information Practices in their handling of personal data, to the American approach.

168. *In re* DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 497, 500 (S.D.N.Y. 2001). The court found the plaintiff class' ECPA and CFAA claims unpersuasive because they could not meet the statutory plateau for demonstrated damages. *Id.* at 526. The court also noted the "absence of evidence in the legislative or judicial history of any of these Acts to suggest that Congress intended to prohibit conduct like DoubleClick's." *Id.* The plaintiffs threatened an appeal, but soon settled on terms favorable to DoubleClick. *See* Stefanie Olsen, *DoubleClick Nearing Privacy Settlements*, CNET News.com, *at* http://news.com.com/2102-1023-871654.html (March 29, 2002); Elec. Privacy Info. Ctr., *Cookies*, *at* http://www.epic.org/privacy/cookies/ (last updated Nov. 5, 2002).

169. Passport is a virtual wallet that stores personal information usable through Microsoft's ".Net" initiative. *See In re* Microsoft Corp., FTC No. 012 3240, Complaint at 1-2 (2002) [hereinafter Passport Complaint], *available at* http://www.ftc.gov/os/2002/08/microsoftcmp.pdf.

170. *Id.* at 2-6.

171. Specifically, the settlement agreement with Microsoft requires the company to bring their treatment of personal information in line with their privacy policy and to develop technical methods of protecting the data, as well as submit to annual reviews of their privacy compliance for the next twenty years. *In re* Microsoft Corp., FTC No. 012

Governments build digital dossiers for monitoring and criminal investigative purposes. Such efforts have renewed energy following the September 2001 terrorist attacks. The Pentagon, as part of the Defense Advanced Research Projects Agency, or DARPA, is developing a project called "Total Information Awareness" (TIA) to monitor digital data as part of the anti-terrorism effort.[172] Of course, the database created by TIA will do more than help the military locate terrorists—it will allow the assemblage of excruciatingly detailed digital dossiers on every American, which could be used for monitoring or investigative purposes having nothing to do with terrorism.[173] Like the dossiers assembled by DoubleClick and Microsoft, TIA is the epitome of the digital information privacy problem: seemingly innocuous information accumulated and used in privacy-invasive ways.

III. THE FAILURE OF THE OLD PRIVACY FRAMEWORK

Protecting privacy in discrete, subject-area "branches" has always had problems, but because conceptions of "privacy" developed independently in response to particular social and technological pressures, such an approach was organic, if not necessary.[174] The adaptation of privacy theory under this approach may not have been ideal, but over time the branches

---

3240, Agreement Containing Consent Order at 3-7 (2002) [hereinafter Passport Agreement], *available at* http://www.ftc.gov/os/2002/08/microsoftagree.pdf.

172. Total Information Awareness (TIA) System, Information Awareness Office, DARPA, *at* http://www.darpa.mil/iao/TIASystems.htm (last visited Nov. 22, 2002) (describing the goal of TIA: to "revolutionize the ability of the United States to detect, classify and identify foreign terrorists"). The TIA's technical functionality essentially will be aggregation of data and data mining:

> [T]he TIA program is focusing on the development of: 1) architectures for a large-scale counter-terrorism database, for system elements associated with database population, and for integrating algorithms and mixed-initiative analytical tools; 2) novel methods for populating the database from existing sources, create innovative new sources, and invent new algorithms for mining, combining, and refining information for subsequent inclusion into the database; and, 3) revolutionary new models, algorithms, methods, tools, and techniques for analyzing and correlating information in the database to derive actionable intelligence.

Id.

173. *See* William Safire, *You Are a Suspect*, N.Y. TIMES, Nov. 14, 2002, at A35 (warning that "[e]very purchase you make with a credit card, every magazine subscription you buy and medical prescription you fill, every Web site you visit and e-mail you send or receive, every academic grade you receive, every bank deposit you make, every trip you book and every event you attend—all these transactions and communications will go into" the TIA database).

174. Solove, *supra* note 17, at 1088-89.

would generally adapt.[175] The changes wrought by digital technology, however, are so deep and broad that the old laws and theories are not adapting fast enough. New, privacy invasive technological practices may solidify into new social norms, and future generations will not know to challenge them. This Part reviews how the division between privacy-as-autonomy and informational privacy is breaking down, as evidenced by the new laws, litigation, and events described above.

Many of the privacy issues of the digital age either cross over multiple "branches" or simply do not fit at all into the old rubric. First, government digital surveillance and monitoring blurs the line between physical and informational privacy. Many of the privacy harms fall through the cracks, especially in the current state of perpetual fear. Second, the ubiquity of personal information in the digital age and its use by private parties causes problems that the current discrete legal regime cannot control. Attempts by the FTC and isolated courts to redress harms in this area are inadequate.

A. The Problem of Government Digital Surveillance

The Fourth Amendment protects against "unreasonable searches and seizures"[176] by any state entity. This standard would seem on its face to protect against misuse of digital government surveillance and data aggregation such as Carnivore and Total Information Awareness. Though the process of the search involves digital bits concerning an individual rather than physical things belonging to an individual, the reasons for searching and the information sought are essentially the same.

Unfortunately for those who fear digital searches, Fourth Amendment rights have been closely circumscribed outside of the realm of physical privacy.[177] One's information, when accessed by the government, is similarly entitled to a "reasonable expectation of privacy," but State entities have not been held to the same exacting standard as applied to physical

175. For example, though it took 39 years, the rule in *Olmstead v. United States*, 277 U.S. 438, 464 (1928), was eventually overturned by *Katz v. United States*, 389 U.S. 347, 359 (1967).

176. U.S. CONST. amend. IV.

177. This problem is unique to digital information technology, not to new technology in general. *Compare* Kyllo v. United States, 533 U.S. 27, 40 (2001) (finding a reasonable expectation of privacy in the heat given off by one's body inside one's home), *with* United States v. Slanina, 283 F.3d 670, 680 (5th Cir. 2002) (finding search of Defendant's computer files at his office was reasonable). *See also supra* notes 21-27, 30-34 and accompanying text.

"searches and seizures."[178] Thus the constitutional protection against government misuse of government digital searching is minimal.[179]

Statutes fill in some of the gaps, but do not provide general protection.[180] Moreover, legislatures are unlikely to impose many new limits on government misuse of personal information in the current atmosphere of heightened national security and fear. In fact, the trend is in the other direction; new legislation is not encouraging,[181] and courts are generally dismissing privacy concerns when national security might be at stake.[182] It would seem that State search and seizure of personal information is limited mostly by the goodwill of the State.

B. Private Information Aggregation

Even private-party informational privacy concerns lack adequate consideration. The traditional tort remedies require proof that harm resulted from the disclosure of privately held information; courts have not been inclined to find that aggregated digital information is truly "private."[183] The myriad statutes regulating use of information are already obsolete—the technology and types of harms change too fast.[184] The underlying problem of informational privacy in the digital age is the ability to access and aggregate vast amounts of otherwise harmless personal data into a form that can do real damage to the individual's sense of self-

178. *See* Whalen v. Roe, 429 U.S. 589, 599 (1977).

179. *See generally* Osher, *supra* note 82.

180. *See, e.g.*, The Driver's Privacy Protection Act, 18 U.S.C. §§ 2721-25 (2000).

181. *See* Homeland Security Act of 2002, Pub. L. No. 107-296; 116 Stat. 2135 (2002) (codifying various new surveillance and security measures and creating the Department of Homeland Security).

182. *See Global Relief Found.*, 207 F. Supp. 2d at 807 (accepting government claim that a U.S. corporation could be classified as a foreign entity under the FISA and Patriot Act due to possible links to terrorists); *In re* Sealed Case, No. 02-001 (United States Foreign Intelligence Surveillance Court of Review 2002), *available at* http://www.cadc.uscourts.gov/common/newsroom/02-001.pdf (upholding new Patriot Act provisions as constitutional).

183. *But see, e.g.*, Remsburg v. Docusearch, Inc., 2003 N.H. LEXIS 17 (2002), the family of a woman stalked and killed by a stalker sued the private investigation Web site that provided the stalker the information needed to track the woman down. *Id.* at ¶¶ 8-13. The New Hampshire Supreme Court ruled that the victim's Social Security Number, despite being available for sale to the public, could still be 'private' for purposes of tort law. *Id.* at ¶ 26.

184. *See, e.g.*, *In re* DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 497 (S.D.N.Y. 2001). The Plaintiffs sued under the ECPA and the CFAA, but had difficulty proving that either law was intended to prevent the specific harms alleged. *Id.* at 526. Further, the Plaintiffs couldn't meet the statutory damage minimums based on outdated views of what constitutes harm. *See id.* at 524-25.

determination and autonomy.[185] Since information privacy law is mired in a conception that dichotomizes information into the strictly private and the "public," even new laws applying the same framework are unlikely to be much help.

The perceived conflict between informational privacy and free speech similarly limits the ability of the current conceptual framework to embrace adequate privacy protections. The "conflict" is based on a simple syllogism: (1) distribution of public information can not be limited without a compelling state interest due to the First Amendment; (2) information about an individual becomes public when it legitimately passes beyond the individual's direct control; (3) digital data about individuals residing in distant databases is not under direct control; therefore, such information is public. This analysis rests on the faulty assumption that people understand what rights they lose when they give up information; though faulty, this assumption is nevertheless seductively appealing to jurists. The Supreme Court obliquely endorsed such an analysis, writing that "privacy concerns give way when balanced against the interest in publishing matters of public importance."[186] Under such a balancing test, privacy interests usually lose.

The *Trans Union* case illustrates the problems courts are facing with this conflict.[187] While the court of appeals recognized the privacy interests at the heart of the GLBA and the FTC's regulations, it had trouble reconciling the privacy interests with the First Amendment. The freedom to talk about anything "public" seemed in conflict with the GLBA's protection of ostensibly "public" financial records.[188] By defining information such as a personal "credit header" as "public," the court saw tension where no tension need be.[189]

Finally, the role of the FTC as *de facto* Privacy Protection Commission[190]—acting to oversee commercial use of personal information—is laudable but ultimately unsatisfactory. First, they are no more able to redefine the constitutional balance between speech and privacy than Congress.[191] Second, their legislative mandate is not privacy *per se*, but con-

185. *See* Cohen, *supra* note 76, at 1423-29.

186. Bartnicki v. Vopper, 532 U.S. 514, 534 (2001).

187. *Trans Union II*, 295 F.3d 42, 52 (D.C. Cir. 2002).

188. *See id.*

189. *See* Cohen, *supra* note 76, at 1408.

190. *See generally* Steven Hetcher, *The De Facto Federal Privacy Commission*, 19 J. MARSHALL J. COMPUTER & INFO. L. 109 (2000).

191. *See* Trans Union Corp. v. FTC, 122 S. Ct. 2386, 2387 (2002) (Kennedy, J., dissenting from denial of cert.)

sumer protection.[192] Thus, their concerns institutionally extend to privacy only so long as commercial privacy violations constitute unfair business practice. Third, the FTC's institutional mechanisms are limited. They enter into settlements with privacy offenders like Microsoft[193] and Eli Lilly,[194] but such agreements do not bind other offenders, and are often no more than slaps on the wrist.[195] A privacy protection commission is probably a good idea, but the FTC is not it.

In sum, the branches of privacy law—as a framework and as areas of protection in themselves—are not up to the challenge of the digital age. Physical privacy invasions are occurring through manipulation of digital data. The most sensitive of digital profiles are no more protected than one's last name. Those who wish to avoid Scott McNealy's world-view have much to do to ensure adequate protection for the future of privacy.

IV. CONCLUSION

There exists among privacy scholars a general consensus that privacy law and theory must change to meet the needs of the digital age.[196] Many, too, have suggested ways to fix it—ranging from the proposal of a new constitutional amendment[197] to discarding the very notion of privacy.[198]

Some scholars suggest practical solutions to the digital privacy problem. Robert Gellman proposes the creation of a federal privacy agency.[199] He suggests an agency with independent power and fact-finding functions, but no regulatory authority.[200] The agency would be guided by the Fair Information Principles (FIPs), established in the Privacy Act of 1974, in

---

192. Federal Trade Commission Act, 15 U.S.C. § 45 (2002).

193. Passport Agreement, FTC No. 012 3240 (2002), *supra* note 171.

194. *See In re* Eli Lilly & Co., FTC No. 012 3214, Agreement Containing Consent Order (2002).

195. *See id.* (requiring Eli Lilly to pay nothing for its privacy violations).

196. *See* Cohen, *supra* note 76, at 1375 (noting that "[t]here is much disagreement about what comes next, but there is also a growing (if still inchoate) consensus that something needs to be done").

197. *See* Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV. J.L. & TECH. 75, 77 (1994) (mentioning Professor Lawrence Tribe's proposal for a constitutional privacy amendment).

198. *See generally* DAVID BRIN, THE TRANSPARENT SOCIETY: WILL TECHNOLOGY FORCE US CHOOSE BETWEEN PRIVACY AND FREEDOM? (1998) (arguing that the impending complete loss of privacy due to digital technology is a positive thing).

199. Robert Gellman, *A Better Way to Approach Privacy Policy in the United States: Establish a Federal Privacy Protection Board*, 54 HASTINGS L.J. (forthcoming 2003) (manuscript at 1).

200. *Id.* at 13-19.

its investigations of private entities.[201] Others suggest the adoption of a general data protection law, as Europe has done.[202] Both of these proposals see the problem as largely one of incomplete legal authority.

Other commentators have defined new conceptions of privacy more attuned to the information age. Julie Cohen advances a "vision of data privacy" based on "zones of personal autonomy" rather than on the outdated "reasonable expectation of privacy."[203] She searches for a conception that embodies the values "data protection" seeks to protect, while simultaneously avoiding conflict with free flows of knowledge and expression.[204] Similarly, Robert Post finds, at the heart of all the "branches" of privacy, the sanctity of community norms.[205] Communities, he argues, build their own conceptions of the self through socialization. When these norms are threatened—say, by invasion of the socialized sphere of the private—the personal identity of the individual is at stake. Thus, privacy rights are protected by identifying and protecting norms, and requiring others to respect the norms of others.[206] Daniel Solove takes a more pragmatic approach.[207] He analyzes and rejects as insufficient or too rigid the existing conceptions of privacy, including the "right to be let alone" and "control over personal information. Judges could apply an ad hoc, contextual conception to see the nature of the privacy interests in a given situation.[208]

These suggestions, both practical and theoretical, hold out hope that privacy can grow to encompass meaningful protections in the digital age. They all address the shortcomings of the existing, dysfunctional framework. But whether the new conception of privacy is embodied in a new, flexible legal framework or simply provides a guiding theory to aid lawmakers and judges, the approach would ideally allow a systematic means of weighing privacy harms and remedies. Without such a guide, privacy violations often go unpunished and victims uncompensated.[209] Worse yet, the violators do not have a clear idea of how to act properly in the future.

This country will be facing tough privacy questions in the short and long term. The second round of the Patriot Act is already under discussion

---

201. *Id.* at 13.

202. *See* European Commission Council Directive 95/46/EC, 1995 O.J. (L 281).

203. Cohen, *supra* note 76, at 1377.

204. *Id.* at 1374-78.

205. Robert Post, Remarks at the Enforcing Privacy Rights Symposium (Nov. 15, 2002).

206. *Id.*

207. Solove, *supra* note 17, at 1091.

208. *Id.* at 1146-47.

209. *See generally In re* DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 497 (S.D.N.Y. 2001).

in Congress. The amount of digital information available continues to grow. The existence of a new privacy conception will not answer the tough questions: How can the public better understand what they give up when they provide their information on a credit application or a website? How can we differentiate between public and private information? How do we balance anti-terrorism efforts with respect for personal privacy? A new approach, one that adequately values privacy interests at a practical and conceptual level, will help.

Since September 11th, 2001, we have been in a crisis. The threat of terrorism means many are willing to trade privacy for the reassurance an informed government provides. The problem with this trade is less the privacy we voluntarily sacrifice and more that the ever-vigilant eyes of the watchers may become so commonplace as to evoke no concern or sense of loss. This is not an idle fear—the economic and political markets dictate that if no one demands privacy, no one will provide or protect it. Post-9/11 fears, if unchallenged, could crystallize into anti-privacy norms. Justice Brandeis described privacy as "the most comprehensive of rights and the right most valued by civilized men."[210] For the sake of civility if not civilization itself, we must defend that right.

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