2006

A Brief History of Information Privacy Law

Daniel J. Solove
George Washington University Law School, dsolove@law.gwu.edu

Chapter 1

A Brief History of Information Privacy Law

Daniel J. Solove*

George Washington University Law School

* I would like to thank Paul Schwartz for his comments on this chapter and John Spaccarotella for his research assistance. More extensive information about the topics discussed in this article can be found in DANIEL J. SOLOVE, MARC ROTENBERG, & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW (2d ed. 2006).

§ 1:1 Introduction

In recent years, information privacy has emerged as one of the central issues of our times. Today, we have hundreds of laws pertaining to privacy: the common law torts, criminal law, evidentiary privileges, constitutional law, at least twenty federal statutes, and numerous statutes in each of the fifty states. To understand the law of information privacy more completely, it is necessary to look to its origins and growth. Technology has played a large role in the story of the emergence of information privacy law. Frequently, new laws emerge in response to changes in technology that have increased the collection, dissemination, and use of personal information.

§ 1:2 Colonial America

To the colonists, America afforded unprecedented privacy. As David Flaherty notes, "[s]olitude was readily available in colonial America."[1] From the crowded towns and cities of Europe, America's endless expanse provided significantly more space and distance from other people.[2] But many people still lived in small towns, where everybody knew each other's business. As Flaherty observes: "The population in the early years was still so small that no person could escape the physical surveillance of others without special efforts."[3]

Even in the early days of colonial America, there was some limited legal protection of privacy. The law had long protected against eavesdropping, which William Blackstone defined as "listen[ing] under walls or windows, or the eaves of a house, to hearken after discourse, and thereupon to frame slanderous and mischievous tales."[4] The common law also sanctioned being a common scold, a law that applied only to women.[5]

The law had long protected one's home. The maxim that the home is one's castle appeared as early as 1499.[6] Better-known is a judicial pronouncement in *Semayne's Case*[7] in 1604 that "the house of every one is to him as his castle and fortress."[8] According to William Blackstone, the law has "so particular and tender a regard to the immunity of a man's house that it stiles it his castle, and will never suffer it to be violated with impunity."[9]

At the time of the Revolutionary War, the central privacy issue was freedom from government intrusion. The Founders detested the use of general warrants and writs of assistance.[10] Writs of assistance authorized "sweeping searches and seizures without any evidentiary basis"[11] and general warrants "resulted in 'ransacking' and

---

1. DAVID H. FLAHERTY, PRIVACY IN COLONIAL NEW ENGLAND 1 (1972).
2. *Id.* at 33.
3. *Id.* at 2.
4. 4 WILLIAM BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND 168 (1769).
5. *See* DAVID J. SEIPP, THE RIGHT TO PRIVACY IN AMERICAN HISTORY 6–7 (1978).
6. Note, *The Right to Privacy in Nineteenth Century America*, 94 HARV. L. REV. 1892, 1894 n.18 (1981).
7. Semayne's Case, 77 Eng. Rep. 194 (K.B. 1604).
8. *Id.* at 195.
9. 4 BLACKSTONE, *supra* note 4, at 223.
10. Tracey Maclin, *When the Cure for the Fourth Amendment Is Worse Than the Disease*, 68 S. CAL. L. REV. 1, 8 (1994); *see also* LEONARD W. LEVY, ORIGINS OF THE BILL OF RIGHTS 158 (1999).
11. Silas J. Wasserstrom & Louis Michael Seidman, *The Fourth Amendment as Constitutional Theory*, 77 GEO. L.J. 19, 82 (1998).

seizure of the personal papers of political dissenters, authors, and printers of seditious libel."[12] As Patrick Henry declared: "They may, unless the general government be restrained by a bill of rights, or some similar restrictions, go into your cellars and rooms, and search, ransack, and measure, everything you eat, drink, and wear. They ought to be restrained within proper bounds."[13]

The framers' distaste for excessive government power to invade the privacy of the people was forged into the Bill of Rights in the Third, Fourth, and Fifth Amendments. The Third Amendment protects the privacy of the home by preventing the government from requiring soldiers to reside in people's houses: "No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law."[14]

The Fourth Amendment provides broad limitations on the government's power to search and to seize:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[15]

The Fourth Amendment prevents the government from conducting "unreasonable searches and seizures."[16] Government officials must obtain judicial approval before conducting a search through a warrant supported by probable cause.

The Fifth Amendment affords individuals a privilege against being compelled to testify about incriminating information.[17] In other words, the government cannot compel individuals to divulge inculpatory information about themselves.

---

12. DAVID M. O'BRIEN, PRIVACY, LAW, AND PUBLIC POLICY 38 (1979); *see also* William Stuntz, *The Substantive Origins of Criminal Procedure*, 105 YALE L.J. 393, 406 (1995).
13. THE DEBATES IN SEVERAL CONVENTIONS ON THE ADOPTION OF THE FEDERAL CONSTITUTION 448–49 (Jonathan Elliot ed., 1974).
14. U.S. CONST. amend. III.
15. U.S. CONST. amend. IV.
16. *Id.*
17. *See* U.S. CONST. amend. V.

§ 1:3 The Nineteenth Century

§ 1:3.1 New Threats to Privacy

The nineteenth century experienced a series of new threats to privacy and a growing concern about protecting privacy.

[A] The Census and Government Records

For much of the nineteenth century, state and federal governments did not keep extensive information about citizens.[18] During the late nineteenth century, government record-keeping at the state and local level began to increase with the rise of progressive regulation.[19]

The primary form of information gathering by the federal government was the census. The first census in 1790 asked only four questions.[20] The number of questions increased with each census, growing to 142 questions in 1860.[21] These questions were increasingly delving into personal details. To make matters worse, since 1790, copies of the census were posted in public places so people could check errors.[22] This practice stopped in 1870.[23]

When the 1890 census asked about diseases, disabilities, and finances, it created a public outcry, which ultimately lead to the passage in the early twentieth century of stricter laws protecting the confidentiality of census data.[24] For example, in 1919, Congress made it a felony to publicize census information illegally.[25]

[B] The Mail

Since colonial times, the privacy of the mail was a significant problem. Sealing letters was difficult.[26] Benjamin Franklin, who was in charge of the colonial mails, required his employees to swear an oath not to open mail.[27] And in 1782, Congress passed a law that mail should not be opened.[28]

---

18. ROBERT ELLIS SMITH, BEN FRANKLIN'S WEB SITE: PRIVACY AND CURIOSITY FROM PLYMOUTH ROCK TO THE INTERNET 12 (2000).
19. Note, *The Right to Privacy in Nineteenth Century America*, 94 HARV. L. REV. 1892, 1906-07 (1981).
20. *See* PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 46 (1995).
21. *See id.*
22. *See* SEIPP, *supra* note 5, at19.
23. *See id.*
24. *See* REGAN, *supra* note 20, at 47.
25. *See id.*
26. SMITH, *supra* note 18, at 23–25.
27. *Id.* at 49; REGAN, *supra* note 20, at 46–49.
28. SMITH, *supra* note 18 at 50.

Nevertheless, significant concerns persisted about postal clerks reading people's letters. Thomas Jefferson, Alexander Hamilton, and George Washington frequently complained about the lack of privacy in their letters, and they would sometimes write in code.[29] As Thomas Jefferson wrote: "[T]he infidelities of the post office and the circumstances of the times are against my writing fully and freely."[30]

These problems persisted in the nineteenth century, and the law responded. Congress passed several laws protecting the privacy of the mail.[31] In 1825, Congress enacted a statute that provided:

> Whoever takes any letter, postal card, or package out of any post office or any authorized depository for mail matter, or from any letter or mail carrier, . . . before it has been delivered to the person to whom it was directed, with design to obstruct the correspondence, or to pry into the business or secrets of another, or opens, embezzles, or destroys the same, shall be fined . . . or imprisoned.[32]

In 1877, in *Ex parte Jackson*,[33] the Supreme Court held that the Fourth Amendment prohibited government officials from opening letters without a warrant: "The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be."[34]

[C] Telegraph Communications

The burgeoning use of the telegraph raised a number of privacy problems. Shortly after the telegraph's invention in 1844,[35] technology to tap into telegraph communications emerged. As Priscilla Regan observes:

---

29. *Id.* at 50–51; *see also* DAVID H. FLAHERTY, PRIVACY IN COLONIAL NEW ENGLAND 115-27 (1972).
30. Thomas Jefferson in 1798, *quoted in* SEIPP, *supra* note 5, at 1.
31. *Id.* at 50–51.
32. 42 U.S.C. § 1702. This law is still valid today. *See* SMITH, *supra* note 18, at 51.
33. *Ex parte* Jackson, 96 U.S. 727 (1877).
34. *Id.* at 733.
35. *See* SMITH, *supra* note 18 at 123.

> During the Civil War, the Union and Confederate armies tapped each other's telegraph communications to ascertain battle plans and troop movements. Rival press organizations tapped each other's wire communications in order to be the first to report major news items.[36]

After the Civil War, Congress began to seek access to telegraph messages maintained by Western Union for various investigations.[37] This raised a considerable outcry among some members of Congress.[38] Additionally, a *New York Times* editorial decried the practice as "an outrage upon the liberties of the citizen."[39] Another editorial in the *New York Tribune* complained that the seizure of telegrams "violates the commonest legal maxims as to the right to call for papers, and outrages every man's sense of his right to the secrets of his own correspondence."[40] A *New York Sun* editorial stated that "the idea that every curious and prying legislative committee may cause to be spread before the public everything that has been sent over the wires will be hateful and repulsive to the people in general."[41]

These problems resulted in a growing congressional debate about whether telegrams should be accorded similar privacy protections to letters.[42] A bill to protect the privacy of telegrams was introduced into Congress in 1880.[43] The bill would ultimately be abandoned. But beyond congressional attempts to obtain telegraph communications, the law responded to restrict other entities from breaching the privacy of telegrams. Several courts quashed subpoenas for telegrams, analogizing them to letters.[44] As the Missouri Supreme Court stated in quashing a grand jury subpoena for telegrams: "Such an inquisition, if tolerated, would destroy the usefulness of this most important and valuable mode of communication."[45] State legislatures also responded by passing laws to prohibit the disclosure of telegraph messages by telegraph company employees.[46] More than half the states enacted laws.[47]

---

36. REGAN, *supra* note 20, at 111.
37. *See* SMITH, *supra* note 18 at 69; SEIPP, *supra* note 5, at 30.
38. *See* SEIPP, *supra* note 5, at 31.
39. *Id.* at 31.
40. *Id.* at 35.
41. *Id.* at 36.
42. SMITH, *supra* note 18, at 69.
43. SEIPP, *supra* note 5, at 40.
44. *Id.*
45. *Ex parte* Brown, 72 Mo. 83, 95 (1880).
46. SEIPP, *supra* note 5, at 65.
47. *Id.*

§ 1:3.2 The Fourth and Fifth Amendments

Ex parte Jackson was not the only major development in Fourth Amendment law in the nineteenth century. In 1886, the Court decided the landmark case of *Boyd v. United States*.[48] The government wanted to compel a merchant to produce documents in a civil forfeiture proceeding. The Court, however, held that the documents could not be compelled, basing its conclusion on both the Fourth and Fifth Amendments:

> It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offence; but it is the invasion of his indefeasible right to personal security, personal liberty and private property. . . . [A]ny forcible and compulsory extortion of a man's own testimony or of his private papers to be used as evidence to convict him of crime or to forfeit his goods, is within the condemnation of that judgment. In this regard the Fourth and Fifth Amendment run almost into each other.

Boyd and subsequent cases created a powerful protection of one's papers and personal information. In the twentieth century, this protection increasingly interfered with the growing administrative state. As William Stuntz notes, "[g]overnment regulation required lots of information, and *Boyd* came dangerously close to giving regulated actors a blanket entitlement to nondisclosure. It is hard to see how modern health, safety, environmental, or economic regulation would be possible in such a regime."[49] As a result, the Court began to retreat from *Boyd* throughout the twentieth century.[50]

§ 1:3.3 Privacy of the Body

Another important Supreme Court privacy case of the 19th century established protection against physical bodily intrusions. In 1891, the Court held in *Union Pacific Railway Co. v. Botsford*,[51] that a court could not compel a female plaintiff in a civil action to submit to a surgical examination:

---

48. Boyd v. United States, 116 U.S. 616 (1886).
49. William J. Stuntz, *Privacy's Problem and the Law of Criminal Procedure*, 93 MICH. L. REV. 1016, 1050 (1995).
50. *See* section 1:4.2[E], *infra*.
51. Union Pac. Ry. Co. v. Botsford, 141 U.S. 250 (1891).

> The inviolability of the person is as much invaded by a compulsory stripping and exposure as by a blow. To compel any one, and especially a woman, to lay bare the body, or to submit it to the touch of a stranger, without lawful authority, is an indignity, an assault, and a trespass. . . .[52]

This case is one of the earliest recognitions of what would later come to be called "substantive due process privacy."

The sanctity of the body was also recognized in the common law, even prior to the birth of the privacy torts following Samuel Warren and Louis Brandeis's article. In *De May v. Roberts*,[53] an 1881 case, a physician allowed a "young unmarried man" not schooled in medicine to be present while the plaintiff gave birth. The court reasoned:

> It would be shocking to our sense of right, justice and propriety to doubt even but that for such an act the law would afford an ample remedy. To the plaintiff the occasion was a most sacred one and no one had a right to intrude unless invited or because of some real and pressing necessity.[54]

§ 1:3.4 Warren and Brandeis's the Right to Privacy

The most profound development in privacy law was the publication in 1890 of Warren and Brandeis's article "The Right to Privacy."[55] According to Roscoe Pound, the article did "nothing less than add a chapter to our law."[56] And Harry Kalven, Jr. referred to it as the "most influential law review article of all."[57]

The article was inspired, in part, by a vastly expanding form of media—the newspaper. In the second latter half of the nineteenth century, newspapers were the most rapidly growing type of media. Circulation of newspapers rose about 1,000% from 1850 and 1890, from 100 newspapers with 800,000 readers in 1850 to 900 papers with over 8 million readers by 1890. Increasingly, newspapers reported on sensationalistic topics such as scandals and gossip about

52. *Id.* at 252.
53. De May v. Roberts, 9 N.W. 146 (1881).
54. *Id.* at 148–49.
55. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).
56. ALPHEUS MASON, BRANDEIS: A FREE MAN'S LIFE 70 (1946).
57. Harry Kalven, Jr., *Privacy in Tort Law—Were Warren and Brandeis Wrong?*, 31 L. & CONTEMP. PROBS. 326, 327 (1966).

people's lives, a type of journalism that became known as "yellow journalism."[58] As Warren and Brandeis observed: "The press is overstepping in every direction the obvious bounds of propriety and decency. Gossip is no longer the resource of the idle and of the vicious, but has become a trade, which is pursued with industry as well as effrontery."[59]

Warren and Brandeis were also concerned about a new technology: "instantaneous photograph[y.]"[60] Cameras had been large, expensive, and not very portable. In 1884, the Eastman Kodak Company produced the "snap camera," a hand-held camera for general public use. People could now take candid pictures in public places.[61] Warren and Brandeis anticipated a dangerous mix between this new technology and the sensationalistic press: "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.'"[62]

These new threats required a remedy. The difficulty was that the existing common law did not currently afford much of a legal protection of privacy. Defamation law—the torts of libel and slander—protected against false information, not true private information. Contract law could protect privacy within relationships formed between parties, but it could not protect against privacy invasions by third parties outside of the contract. Warren and Brandeis observed:

> While, for instance, the state of the photographic art was such that one's picture could seldom be taken without his consciously "sitting" for the purpose, the law of contract or of trust might afford the prudent man sufficient safeguards against the improper circulation of his portrait; but since the latest advances in photographic art have rendered it possible to take pictures surreptitiously, the doctrines of contract and of trust are inadequate to support the required protection.[63]

---

58. William L. Prosser, *Privacy, in* PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 104 (Ferdinand David Schoeman ed., 1984) (noting rising popular dismay over "yellow journalism" at the time of Brandeis's and Warren's article).
59. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).
60. *Id.* at 195.
61. *See* DANIEL J. SOLOVE, MARC ROTENBERG & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 10 (2d ed. 2006).
62. *Id.*
63. Warren & Brandeis, *supra* note 59, at 211.

Property law was also inadequate to protect privacy. As Warren and Brandeis observed: "[W]here the value of the production is found not in the right to take profits arising from publication, but in the peace of mind or the relief afforded by the ability to prevent any publication at all, it is difficult to regard the right as one of property."[64]

Warren and Brandeis argued that the common law could readily develop a remedy for protecting privacy. The authors noted: "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."[65] These rights were not based upon property. Rather, they were based upon "the more general right of the individual to be let alone."[66] From this more general right, protections against privacy violations could be derived in the common law.[67] Warren and Brandeis discussed a number of remedies to protect privacy, with the principal remedy being "[a]n action of tort for damages in all cases."[68]

§ 1:4 The Twentieth Century

§ 1:4.1 1900 to 1960

[A] Warren and Brandeis's Privacy Torts

[A][1] Early Recognition

In 1902, the New York Court of Appeals confronted the issue in *Roberson v. Rochester Folding Box Co*.[69] An advertisement by Franklin Mills Flour used a lithograph of Abigail Roberson without her consent. Roberson sued, alleging that she had been "greatly humiliated by the scoffs and jeers of persons who have recognized her face and picture on this advertisement, and her good name has been attacked, causing her great distress and suffering, both in body and mind."[70] The court, however, refused to recognize a cause of action because there was "no precedent for such an action to be found in the decisions of this court" and the creation of such an action would more appropriately be achieved by the legislature because the courts were "without authority to legislate."[71]

64. *Id.* at 200.
65. *Id.* at 198.
66. *Id.* at 205.
67. *See id.* at 205.
68. *Id.* at 219.
69. Roberson v. Rochester Folding Box Co., 64 N.E. 442 (N.Y. 1902).
70. *Id.* at 442.
71. *Id.* at 447–48.

The *Roberson* decision sparked a significant debate. A *New York Times* editorial criticized the decision, observing that it "excited as much amazement among lawyers and jurists as among the promiscuous lay public."[72] A note in the *Yale Law Journal* attacked the decision for not recognizing a remedy for the "undoubted injury to the plaintiff."[73] Another law review article declared that *Roberson* "shocks and wounds the ordinary sense of justice of mankind."[74] As a result of this wave of criticism, one of the judges in *Roberson* defended the opinion in the *Columbia Law Review*.[75]

In 1903, just one year after the decision, New York enacted a statute establishing a cause of action for invasion of privacy.[76] The law still remains on the books today.[77]

A couple of years later, in 1905, the Georgia Supreme Court recognized a common law tort for privacy invasions in *Pavesich v. New England Life Insurance Co*.[78] In facts similar to *Roberson*, a life insurance advertisement used the plaintiff's image without his consent. The court concluded that a "right of privacy in matters purely private is . . . derived from natural law."[79] As the court reasoned:

> One who desires to live a life of partial seclusion has a right to choose the times, places, and manner in which and at which he will submit himself to the public gaze. Subject to the limitation above referred to, the body of a person cannot be put on exhibition at any time or at any place without his consent. . . . It therefore follows from what has been said that a violation of the right of privacy is a direct invasion of a legal right of the individual.[80]

---

72. N.Y. TIMES, Aug. 23, 1902, Editorial, *reprinted in* Denis O'Brien, *The Right to Privacy*, 2 COLUM. L. REV. 437, 437 (1902).
73. Comment, *An Actionable Right to Privacy?*, 12 YALE L.J. 34, 36 (1902).
74. 36 AM. L. REV. 636, *quoted in* Pavesich v. New England Life Ins. Co., 50 S.E. 68, 79 (Ga. 1905).
75. Denis O'Brien, *The Right to Privacy*, 2 COLUM. L. REV. 436 (1902).
76. *See, e.g.*, Irwin R. Kramer, *The Birth of Privacy Law: A Century Since Warren and Brandeis*, 39 CATH. U. L. REV. 703, 704 (1990).
77. *See* N.Y. CIV. RIGHTS LAW §§ 50–51.
78. Pavesich v. New England Life Ins. Co., 50 S.E. 68 (Ga. 1905).
79. *Id.* at 70.
80. *Id.*

[A][2] William Prosser and the Restatement

In 1960, renowned tort scholar William Prosser surveyed the over 300 privacy cases that were spawned by the Warren and Brandeis article.[81] Prosser concluded that the cases recognized four distinct torts:

(1) intrusion upon seclusion;

(2) public disclosure of private facts;

(3) false light or "publicity"; and

(4) appropriation.[82]

Today, the vast majority of states recognize most of these torts.[83] The most recent state to do so was Minnesota in *Lake v. Wal-Mart Stores, Inc.*,[84] where the state Supreme Court finally recognized the Warren and Brandeis torts in 1998.[85]

[A][2][a] Intrusion upon Seclusion

As defined by the *Restatement of Torts*, intrusion upon seclusion provides:

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.[86]

Intrusion upon seclusion protects against electronic eavesdropping into conversations in the home,[87] as well as the deceitful entry and clandestine photographing of activities in the home. The tort is not limited to intrusions into the home.[88] In a case involving well-known consumer advocate Ralph Nader, the court held that an attempt by General Motors to hire people to "shadow" him and "keep him under surveillance" could be tortious if the surveillance was "overzealous."[89]

---

81. William L. Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960).
82. *Id.*
83. *See* Lake v. Wal-Mart Stores, Inc., 582 N.W.2d 231, 235 (Minn. 1998).
84. *Id.*
85. *Id.* at 235.
86. RESTATEMENT (SECOND) OF TORTS § 652B.
87. Hamberger v. Eastman, 206 A.2d 239 (N.H. 1964).
88. Dietemann v. Time, Inc., 449 F.2d 245 (9th Cir. 1971).
89. Nader v. Gen. Motors Corp., 255 N.E.2d 765 (N.Y. 1970).

[A][2][b] Public Disclosure of Private Facts

The tort of public disclosure of private facts provides:

> One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public.[90]

In an early case, *Melvin v. Reid*,[91] the court held that the use of an ex-prostitute's maiden name in the movie "The Red Kimono" could give rise to a public disclosure action. Courts have sustained public disclosure suits for publishing a photograph of a woman whose dress was blown up involuntarily by air jets;[92] for the publication of an article describing a person's unusual disease;[93] and for posting a large sign in a window stating that the plaintiff owed a debt.[94]

The Supreme Court has curtailed the scope of the public disclosure tort. In *Cox Broadcasting v. Cohn*,[95] the Court held that "[o]nce true information is disclosed in public court documents open to public inspection, the press cannot be sanctioned for publishing it."[96] In *Smith v. Daily Mail*,[97] the Court held unconstitutional a statute prohibiting the publication of the names of juvenile offenders: "If a newspaper lawfully obtains truthful information about a matter of public significance then state officials may not constitutionally punish publication of the information, absent a need to further a state interest of the highest order."[98] And in *Florida Star v. B.J.F.*,[99] the Court held that a newspaper could not be liable for publishing the name of a rape victim obtained from a police report.[100] These decisions notwithstanding, the Court has repeatedly avoided addressing the constitutionality of the public disclosure tort, and it has confined its holdings to relatively narrow contexts.

---

90. RESTATEMENT (SECOND) OF TORTS § 652D.
91. Melvin v. Reid, 297 P. 91 (Cal. 1931).
92. Daily Times Democrat v. Graham, 162 So. 2d 474 (Ala. 1964).
93. Barber v. Time, Inc., 159 S.W.2d 291 (Mo. 1942).
94. Brents v. Morgan, 299 S.W. 967 (Ky. 1927).
95. Cox Broad. v. Cohn, 420 U.S. 469 (1975).
96. *Id.* at 496.
97. Smith v. Daily Mail, 443 U.S. 97 (1979).
98. *Id.* at 103.
99. Fla. Star v. B.J.F., 491 U.S. 524 (1989).
100. *Id.* at 532.

[A][2][c] False Light

The tort of false light is defined as:

> One who gives publicity to a matter concerning another that places the other before the public in a false light is subject to liability to the other for invasion of his privacy, if
>
> (a) the false light in which the other was placed would be highly offensive to a reasonable person, and
>
> (b) the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed.[101]

[A][2][d] Appropriation

Pursuant to the *Restatement*:

> One who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy.[102]

In the mid twentieth century, an offshoot of the appropriation tort emerged, referred to as the "right of publicity."[103] The right of publicity originated in *Haelan Laboratories v. Topps Chewing Gum, Inc.*,[104] where the court declared that "in addition to and independent of that right of privacy . . . a man has a right in the publicity value of his photograph, *i.e.*, the right to grant the exclusive privilege of publishing his picture, and that such a grant may validly be made 'in gross,' that is, without an accompanying transfer of a business or of anything else."[105] According to Thomas McCarthy, "while the appropriation branch of the right of privacy is invaded by an injury to the psyche, the right of publicity is infringed by an injury to the pocket book."[106]

---

101. RESTATEMENT (SECOND) OF TORTS § 652E.
102. *Id.* § 652C.
103. J. THOMAS MCCARTHY, THE RIGHTS OF PUBLICITY AND PRIVACY (2000); Melville B. Nimmer, *The Right of Publicity*, 19 LAW & CONTEMP. PROBS. 203 (1954).
104. Haelan Labs. v. Topps Chewing Gum, Inc., 202 F.2d 866 (2d Cir. 1953).
105. *Id.* at 868.
106. MCCARTHY, *supra* note 103, § 5:61, at 5-110.

The emergence of the right of publicity is often viewed as distinct from appropriation, but is sometimes viewed as merely a dimension of the appropriation tort. William Prosser did not recognize a distinct tort of publicity, and neither did the *Restatement*.[107]

[B] The Emergence of the Breach of Confidentiality Tort

Beyond the Warren and Brandeis privacy torts, the tort of breach of confidentiality developed to protect disclosures of information in violation of trust within certain relationships. For example, in 1920, in *Simonsen v. Swenson*,[108] the court recognized that

> [t]he relation of physician and patient is necessarily a highly confidential one. It is often necessary for the patient to give information about himself which would be most embarrassing or harmful to him if given general circulation. This information the physician is bound, not only upon his own professional honor and the ethics of his high profession, to keep secret. . . . A wrongful breach of such confidence, and a betrayal of such trust, would give rise to a civil action for the damages naturally flowing from such wrong.[109]

The *Simonsen* court concluded that the breach of confidentiality tort is not absolute, and it does not apply when disclosure is mandated by statute or when disclosure will protect the health and safety of others. As one court has stated: "A majority of the jurisdictions faced with the issue have recognized a cause of action against a physician for the unauthorized disclosure of confidential information unless the disclosure is compelled by law or is in the patient's interest or the public interest."[110]

Some courts have held that because the breach of confidentiality tort emerges from the patient-physician relationship, analogous to a fiduciary one, the tort extends to a third party who "induces a breach of a trustee's duty of loyalty, or participates in such a breach, or knowingly accepts any benefit from such a breach, becomes directly liable to the aggrieved party."[111]

---

107. *See* SOLOVE ET AL., *supra* note 61, at 189–91.
108. Simonsen v. Swenson, 177 N.W. 831 (Neb. 1920).
109. *Id.* at 832.
110. McCormick v. England, 494 S.E.2d 431 (S.C. Ct. App. 1997); *see also* Biddle v. Warren Gen. Hosp., 715 N.E.2d 518 (Ohio 1999).
111. Hammonds v. Aetna Cas. & Sur. Co., 243 F. Supp. 793 (D. Ohio 1965).

[C] The Growth of Government Record Systems

The rise of the administrative state in the first half of the twentieth century resulted in the creation of elaborate systems of public records.[112] For example, the Social Security System, created in 1935, required that records be maintained about each employed individual's earnings. To administer the program efficiently, a unique nine-digit number was assigned to each citizen, known as the Social Security number (SSN). The number was only to be used for the Social Security system, and it was not designed as a general identifier, with social security cards stating that SSNs were "NOT FOR IDENTIFICATION."[113] As will be discussed later, this number soon was used for a myriad of other purposes.

[D] The Telephone and Wiretapping

[D][1] The Fourth Amendment: Olmstead v. United States

The early twentieth century witnessed the growth of telephone communication. Shortly after the telephone was patented in 1876, methods of intercepting communications through wiretapping were developed.[114] As with telegraph communications, there was a growing concern about the privacy of telephone communications. State legislatures responded with new legislation. For example, in 1905, California expanded its 1862 law against intercepting telegraph messages to telephone calls.[115]

In 1928, the Supreme Court in *Olmstead v. United States*[116] confronted the issue of whether the Fourth Amendment required a warrant before the government could engage in wiretapping. The Court concluded that the Fourth Amendment did not apply to wiretapping because it did not involve trespass inside a person's home: "There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants."[117]

---

112. *See* DAVID LYON, SURVEILLANCE SOCIETY: MONITORING EVERYDAY LIFE 73 (2001).
113. ROBERT ELLIS SMITH, BEN FRANKLIN'S WEB SITE: PRIVACY AND CURIOSITY FROM PLYMOUTH ROCK TO THE INTERNET 288 (2000).
114. PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 111 (1995).
115. SMITH, *supra* note 113, at 157.
116. Olmstead v. United States, 277 U.S. 438 (1928).
117. *Id.* at 464.

Justice Louis Brandeis dissented. Although he did not cite to his article "The Right to Privacy," his dissent reflects many of its central ideas. Brandeis argued that new technological developments necessitated revising traditional views of the Fourth Amendment in order to preserve its purpose of protecting privacy:

> Subtler and more far reaching means of invading privacy have become available to the government. 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.[118]

[D][2] Federal Communications Act Section 605

Despite the Court's opinion in *Olmstead*, wiretapping continued to be viewed with considerable distaste. Justice Holmes called it a "dirty business."[119] One year after *Olmstead*, J. Edgar Hoover, the head of the FBI, stated that "while it may not be illegal . . . [wiretapping] is unethical and it is not permitted under the regulations by the Attorney General."[120] Hoover declared that any FBI employee engaging in wiretapping would be fired.[121] Ironically, Hoover went on to become one of the greatest abusers of wiretapping.

Six years after *Olmstead*, Congress enacted section 605 of the Federal Communications Act of 1934.[122] Section 605 provided: "no person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communications to any person."[123] The statute only applied to federal, not state, officials. According to the Supreme Court, section 605 prohibited evidence obtained by wiretapping from being used in court.[124] But the statute did not restrict officials from engaging in wiretapping, only from disclosing intercepted communications in

---

118. *Id.* at 473.
119. *Id.* at 470 (Holmes, J., dissenting); *see also* RICHARD F. HIXSON, PRIVACY IN A PUBLIC SOCIETY: HUMAN RIGHTS IN CONFLICT 49 (1987).
120. Louis Fisher, *Congress and the Fourth Amendment*, 21 GA. L. REV. 107, 127 (1986).
121. *Id.*
122. Former 7 U.S.C. § 605.
123. *Id.*
124. *See* Nardone v. United States, 302 U.S. 379 (1937) (evidence directly obtained by wiretapping excluded from evidence); Nardone v. United States, 308 U.S. 338 (1939) (evidence obtained as the fruit of illegal wiretapping could not be used in court).

court proceedings.[125] As a result, wiretapping by the FBI and state law enforcement officials increased dramatically throughout the twentieth century.[126]

[E] The FBI and Increasing Domestic Surveillance

The FBI was originally formed in 1908 amid substantial opposition in Congress to a federal police force.[127] Indeed, Congress never directly authorized the creation of the FBI by legislation. At first, the FBI was known as the Bureau of Investigation (BI); it became the FBI in 1935.[128] Throughout the twentieth century, the FBI expanded in size and in the scope of its surveillance activities.

During World War II, the FBI received a profoundly expanded authority to engage in wiretapping and investigate national security threats. The FBI seized upon fears of Communism during the 1950s to increase its ability to engage in electronic surveillance.[129] Hoover greatly abused his powers as head of the FBI. He wiretapped his critics and people whose views he disliked, and he maintained an elaborate system of files about the personal lives of hundreds of prominent individuals, politicians, professors, and others. Hoover despised Martin Luther King, Jr., and he engaged in a systematic surveillance of him, including wiretapping and bugging his conversations.[130] When the FBI learned of King's extramarital affairs, a high level official sent King a letter suggesting that King commit suicide or else the recordings of his conversations would be "bared to the nation."[131]

Hoover's abuses came to light a few years after his death, when in 1975, Congress's Church Committee conducted an extensive inquiry into Hoover's activities.[132]

---

125. *See* WAYNE R. LAFAVE, JEROLD H. ISRAEL, & NANCY J. KING, CRIMINAL PROCEDURE 260 (3d ed. 2000).
126. *See* Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1128–33 (2002).
127. CURT GENTRY, J. EDGAR HOOVER: THE MAN AND THE SECRETS 112 (1991).
128. *See id.* at 113.
129. *See* WHITFIELD DIFFIE & SUSAN LANDAU, PRIVACY ON THE LINE: THE POLITICS OF WIRETAPPING AND ENCRYPTION 161–62 (1998).
130. *See id.* at 140–42.
131. *Id.* at 126.
132. *See id.* at 178.

[F] Freedom of Association and the McCarthy Era

The Civil Rights era led to attempts by some Southern states to expose the names of those involved in the civil rights movement, subjecting people to community sanctions. In *NAACP v. Alabama*,[133] the Court held that the NAACP could not be compelled to disclose the names and addresses of its members. According to the Court, there is a "vital relationship between freedom to associate and privacy in one's associations."[134] This was because revelation of membership in the NAACP exposed members "to economic reprisal, loss of employment, threat of physical coercion, and other manifestations of public hostility."[135]

The First Amendment right to freedom of association, as well as the Fifth Amendment, did not afford similar protections to the extensive investigation of Communists in the 1950s.[136] The hunt for Communists was led by Senator Joseph R. McCarthy, and aided with substantial help from Hoover.[137] The House Un-American Activities Committee (HUAC)[138] forced individuals to testify publicly about their Communist Party ties and to disclose names of others involved with the Party. The public disclosure of people's ties to the Communist Party often resulted in ostracism and blacklisting.[139] Many journalists, professors and entertainers were fired and blacklisted from future employment.[140]

---

133. NAACP v. Alabama, 357 U.S. 449 (1958).
134. *Id.* at 462.
135. *Id. See also* Shelton v. Tucker, 364 U.S. 479 (1960) (striking down a law requiring public teachers to list all organizations to which they belong or contribute); Baird v. State Bar of Ariz., 401 U.S. 1 (1971) (holding that a state may not ask questions solely to gain information about a person's political views or associations).
136. *See* ELLEN SCHRECKER, THE AGE OF MCCARTHYISM: A BRIEF HISTORY WITH DOCUMENTS 92–94 (1994).
137. GENTRY, *supra* note 127, at 378–80.
138. *See* SCHRECKER, *supra* note 136, at 76–84. For more background, see generally ALBERT FRIED, MCCARTHYISM: THE GREAT AMERICAN RED SCARE: A DOCUMENTARY HISTORY (1997); and RICHARD M. FRIED, NIGHTMARE IN RED: THE MCCARTHY ERA IN PERSPECTIVE (1990).
139. *See* Seth I. Kreimer, *Sunlight, Secrets, and Scarlet Letters: The Tension Between Privacy and Disclosure in Constitutional Law*, 140 U. PA. L. REV. 1, 13–71 (1991).
140. SCHRECKER, *supra* note 136, at 76–84.

In *Barenblatt v. United States*,[141] a person refused to answer the HUAC's questions and was jailed for contempt. The Court held that the First Amendment was not violated by the questioning. In *Wilkinson v. United States*,[142] a witness who criticized the HUAC was interrogated about Communist ties. The Court upheld the questioning because there was a "reasonable ground to suppose that the petitioner was an active Communist Party member."[143] Justice Black dissented, arguing that "this case involves nothing more nor less than an attempt by the Un-American Activities Committee to use the contempt power of the House of Representatives as a weapon against those who dare to criticize it."[144]

Ultimately, McCarthy experienced a downfall, the HUAC was disbanded, and many today view the Communist hysteria as a profound overreaction.

§ 1:4.2 The 1960s and 1970s

[A] New Limits on Government Surveillance

[A][1] *Fourth Amendment Resurgence:* Katz v. United States

The Fourth Amendment underwent a revolution in the 1960s. In 1961, in *Mapp v. Ohio*,[145] the Court held that in all criminal proceedings, evidence obtained in violation of the Fourth Amendment is excluded from evidence in criminal trials.[146] And in 1967, the Court in *Katz v. United States*[147] overruled *Olmstead*. *Katz* involved the wiretapping of a telephone conversation made by the defendant while in a phone booth. The Court declared: "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[148] From *Katz*, the Court's current approach to determining the Fourth Amendment's applicability emerged—the reasonable expectation of privacy test. The test, articulated in Justice Harlan's concurrence, asks whether (1) a person exhibits an "actual or subjective expectation of privacy" and (2) "the expectation [is] one that society is prepared to recognize as 'reasonable.'"[149]

141. Barenblatt v. United States, 360 U.S. 109 (1959).
142. Wilkinson v. United States, 365 U.S. 399 (1961).
143. *Id.* at 414.
144. *Id.* at 417.
145. Mapp v. Ohio, 367 U.S. 643 (1961).
146. *Id.* at 655.
147. Katz v. United States, 389 U.S. 347 (1967).
148. *Id.* at 351–52.
149. *Id.* at 361 (Harlan, J., concurring).

[A][2] Title III of the Omnibus Crime and Control Act of 1968

One year after *Katz*, in 1968, Congress vastly expanded its statutory protections against electronic surveillance beyond the limited protection of section 605. Title III of the Omnibus Crime Control and Safe Streets Act[150] extended the reach of wiretap regulations to state officials as well as to private parties.[151] Despite its profound increase in the extent of protection, Title III had important limitations. It applied to the interception of "aural" communications; it did not apply to visual surveillance or other forms of electronic communication.

[B] The Constitutional Right to Privacy

[B][1] *Decisional Privacy:* Griswold v. Connecticut

In the 1960s and 1970s, the Court held in a series of cases that the Constitution protected a "zone of privacy" that safeguarded individual autonomy in making certain decisions involving their bodies and families. In 1965, in *Griswold v. Connecticut*,[152] the Court held that the government could not ban contraceptives. Although the Constitution does not explicitly protect a right to privacy, the Court reasoned that such a right is found in the "penumbras" of many of the ten amendments of the Bill of Rights.[153] Following *Griswold*, the Court held in *Roe v. Wade*[154] that the right to privacy "encompass[es] a woman's decision whether or not to terminate her pregnancy."[155]

[B][2] *Information Privacy:* Whalen v. Roe

Four years after *Roe v. Wade*, in 1977, the Court held in *Whalen v. Roe*[156] that the constitutionally protected "zone of privacy" extends to two distinct types of interests: (1) "independence in making certain kinds of important decisions"; and (2) the "individual interest in avoiding disclosure of personal matters."[157] The former interest describes *Griswold* and *Roe*; the latter interest was one that the Court had not yet defined. This latter interest has been called

---

150. Omnibus Crime and Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510–22.
151. *See* REGAN, *supra* note 114, at 122–25.
152. Griswold v. Connecticut, 381 U.S. 479 (1965).
153. *Id.* at 484.
154. Roe v. Wade, 410 U.S. 113 (1973).
155. *Id.* at 153.
156. Whalen v. Roe, 433 U.S. 425 (1977).
157. *Id.* at 599–600.

the "constitutional right to information privacy." The Court also articulated this interest in *Nixon v. Administrator of General Services*,[158] decided that same year.

Following *Whalen* and *Nixon*, the Court did not develop the right of information privacy. Nevertheless, a majority of circuit courts have recognized this right, which has been involved in a substantial number of cases.[159]

[C] Responses to the Rise of the Computer

[C][1] Burgeoning Interest in Privacy

The development of the computer in 1946 revolutionized information collection. Throughout the second half of the twentieth century, the computer revolutionized the way records and data were collected, disseminated, and used. The increasing use of computers in the 1960s raised a considerable public concern about privacy.[160] Commentators devoted significant attention to the issue.[161] Privacy also became an important topic on Congress's agenda.[162]

[C][2] Freedom of Information Act of 1966

The growing number of government agencies and the expanding regulatory scope of the administrative state led to a strong sentiment that government records should be open to the public. In 1966, Congress passed the Freedom of Information Act (FOIA), dramatically reforming public access to government records. Under FOIA, "any person" may request "records" maintained by an executive agency.[163] People or entities requesting records need not state a reason for requesting records.[164] Today, all fifty states have freedom of information laws, many of which are based upon the FOIA.

---

158. Nixon v. Adm'r of Gen. Servs., 433 U.S. 425 (1977).
159. *See* SOLOVE ET AL., *supra* note 61, at 401.
160. REGAN, *supra* note 114, at 82.
161. *See, e.g.*, VANCE PACKARD, THE NAKED SOCIETY (1964); MYRON BRENTON, THE PRIVACY INVADERS (1964); ALAN WESTIN, PRIVACY AND FREEDOM (1967); ARTHUR MILLER, THE ATTACK ON PRIVACY (1971); NOMOS XII: PRIVACY (J. Ronald Pennock & J.W. Chapman eds. 1971); ALAN WESTIN & MICHAEL A. BAKER, DATABANKS IN A FREE SOCIETY: COMPUTERS, RECORD-KEEPING AND PRIVACY (1972); Kenneth L. Karst, *"The Files": Legal Controls Over the Accuracy and Accessibility of Stored Personal Data*, 31 L. & CONTEMP. PROBS. 342 (1966); Symposium, *Computers, Data Banks, and Individual Privacy*, 53 MINN. L. REV. 211–45 (1968); Symposium, *Privacy*, 31 L. & CONTEMP. PROBS. 251–435 (1966).
162. *See* REGAN, *supra* note 114, at 82.
163. 5 U.S.C. § 552(a)(3)(A).
164. *See, e.g.*, United States Dep't of Justice v. Reporters Comm. for Freedom of Press, 489 U.S. 749, 771 (1989).

Among nine exceptions to disclosure, the federal FOIA contains two exceptions that safeguard privacy. Exception 6 exempts "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy."[165] Exemption (7)(C) exempts "records or information compiled for law enforcement purposes . . . which could reasonably be expected to constitute an unwarranted invasion of personal privacy."[166] When possible, records with redacted private data are disclosed to requesters.[167]

[C][3] Fair Information Practices

The increasing computerization of information and the burgeoning repositories of personal data in federal agencies continued to be a topic of importance. In 1973, the United States Department of Health Education and Welfare (HEW) issued a report, "Records, Computers, and the Rights of Citizens," which analyzed these problems in depth. The report observed:

> [A]n individual must increasingly give information about himself to large and relatively faceless institutions, for handling and use by strangers—unknown, unseen, and, all too frequently, unresponsive. Sometimes the individual does not even know that an organization maintains a record about him. Often he may not see it, much less contest its accuracy, control its dissemination, or challenge its use by others.[168]

The report recommended the passage of a code of Fair Information Practices:

- There must be no personal data record-keeping systems whose very existence is secret.
- There must be a way for an individual to find out what information about him is in a record and how it is used.
- There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.

---

165. 5 U.S.C. § 552(b)(6).
166. 5 U.S.C. § 552(b)(7)(C).
167. 5 U.S.C. § 552(b).
168. U.S. Department of Health, Education, and Welfare, Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Comm. on Automated Personal Data Systems 29 (1973).

- There must be a way for an individual to correct or amend a record of identifiable information about him.
- 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 reasonable precautions to prevent misuse of the data.[169]

As Marc Rotenberg observes, the Fair Information Practices "played a significant role in framing privacy laws in the United States,"[170] and influenced privacy law around the world.

[C][4] Privacy Act of 1974

A year after the HEW report, Congress passed the Privacy Act of 1974.[171] The Act responded to many of the concerns raised by HEW. It regulates the collection and use of records by federal agencies, and affords individuals right to access and correct their personal information.[172] Although the Act made important strides in bringing government information systems under control, the Act has a number of shortcomings. The Privacy Act does not apply to the private sector. Nor does it apply to state or local agencies.

Another limitation in the Privacy Act is the "routine use" exception where information may be disclosed for any "routine use" if disclosure is "compatible" with the purpose for which the agency collected the information.[173] Numerous commentators have criticized the "routine use" exception as an enormous loophole.[174]

The Privacy Act also attempted to restrict the use of SSNs. The HEW report had noted that there was "an increasing tendency" for the SSN to be used as a "standard universal identifier."[175] The Privacy Act aimed to "curtail the expanding use of social security numbers by federal and local agencies and, by so doing, to eliminate the threat to individual privacy and confidentiality of information posed by common numerical identifiers."[176]

169. *Id.* at 41–42.
170. *See* Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1, 44.
171. Pub. L. No. 93-579, 88 Stat. 1896 (2000) (codified at 5 U.S.C. § 552a).
172. 5 U.S.C. § 552a(d).
173. 5 U.S.C. § 552a(b)(3).
174. *See, e.g.*, Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 585–86 (1995); ROBERT GELLMAN, *Does Privacy Law Work?, in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 198 (Philip E. Agre & Marc Rotenberg eds. 1997).
175. U.S. Dep't of Health, Education, and Welfare, Report of the Secretary's Advisory Committee on Automated Personal Data Systems: Records, Computers, and the Rights of Citizens, at xxxii (1973).
176. Doyle v. Wilson, 529 F. Supp. 1343, 1348 (D. Del. 1982).

Unfortunately, the Act did not restrict the use of SSNs by the private sector. As a result, the use of SSNs continued its upward trend.[177] Today, SSNs are used as a form of password to access one's accounts and records at banks, investment firms, schools, and hospitals.[178]

[C][5] Family Educational Rights and Privacy Act of 1974

The Family Educational Rights and Privacy Act of 1974 (FERPA),[179] otherwise known as the "Buckley Amendment," regulates the accessibility of student records. FERPA does not apply to records maintained by school law enforcement officials[180] or health and psychological records.[181]

[C][6] Foreign Intelligence Surveillance Act of 1978

The Foreign Intelligence Surveillance Act (FISA) of 1978,[182] created a distinct regime for electronic surveillance to gather foreign intelligence. Whereas Title III regulated electronic surveillance for domestic law enforcement purposes, FISA applied when foreign intelligence gathering was "the purpose" of the investigation.[183] FISA permits electronic surveillance and covert searches pursuant to court orders, which are reviewed ex parte by a special court of seven federal judges. Information obtained through FISA orders can be used in criminal trials.[184] The protections against surveillance are much looser than those of Title III. Under Title III and the Fourth Amendment, surveillance is only authorized if there is a showing of probable cause that the surveillance will uncover evidence of criminal activity. Under FISA, orders are granted if there is probable cause to believe that the monitored party is a "foreign power" or "an agent of a foreign power."[185]

---

177. *See* United States General Accounting Office, Report to the Chairman, Subcomm. on Social Security, Comm. on Ways and Means, House of Representatives: Social Security: Government and Commercial Use of the Social Security Number Is Widespread (Feb. 1999).
178. *See* Lynn M. LoPucki, *Human Identification Theory and the Identity Theft Problem*, 80 TEX. L. REV. 89, 108–14 (2001).
179. Pub. L. No. 93-380, 88 Stat. 484, (codified at 20 U.S.C. § 1232g).
180. 20 U.S.C. § 1232g(a)(4)(B)(ii).
181. 20 U.S.C. § 1232g(a)(4)(B)(iv).
182. Pub. L. No. 95-511, codified at 50 U.S.C. §§ 1801–11.
183. *See* former 50 U.S.C. § 1804(a)(7)(B) prior to USA PATRIOT Act amendment in 2001.
184. *See* SOLOVE ET AL., *supra* note 61, at 294.
185. 50 U.S.C. § 1801.

[D] Financial Privacy

Several important legal developments regarding financial privacy occurred throughout the 1970s. Many of these developments involved the lessening of financial privacy.

[D][1] Fair Credit Reporting Act of 1970

In earlier times, in small towns, people could readily learn about each others' financial condition and trustworthiness. Creditors had first-hand information about other people or could learn about them through community gossip. In the twentieth century, with the bulging population and increasing mobility of people, creditors no longer had these easy methods to obtain data about people.[186] Creditors began to rely on records and documents to assess reputation.[187] These developments spawned credit reporting agencies, companies that obtain and report information about a person's credit history. Credit reports contain a detailed financial history, financial account information, outstanding debts, bankruptcy filings, judgments, liens, and mortgage foreclosures. Today, the three major credit reporting agencies (Equifax, Experian, and Trans Union) have compiled extensive data about virtually every adult citizen.

Due to a series of complaints about erroneous credit reports and non-responsiveness by credit reporting agencies,[188] Congress passed the Fair Credit Reporting Act (FCRA) in 1970.[189] The FCRA provides limited protections for individuals. It enables people to access their records, and restricts the manner in which records are disclosed. Individuals can challenge inaccuracies on their reports[190] and can sue to collect damages for violations of the Act.[191]

However, FCRA immunizes creditors and credit reporting agencies from lawsuits for "defamation, invasion of privacy, or negligence" except when the information is "furnished with malice or willful intent to injure such consumer."[192] Although the FCRA allows people to sue for negligent violations of the Act,[193] there is a two-year statute of limitations "from the date on which the liability arises."[194] In *TRW, Inc. v. Andrews*,[195] the Supreme Court held this

186. STEVEN L. NOCK, THE COSTS OF PRIVACY: SURVEILLANCE AND REPUTATION IN AMERICA 3, 73 (1993).
187. SMITH, *supra* note 113, at 314.
188. *See id.* at 23.
189. 15 U.S.C. § 1681.
190. *See* 15 U.S.C. § 1681i.
191. 15 U.S.C. § 1681n.
192. 15 U.S.C. § 1681h(e).
193. 15 U.S.C. § 1681o.
194. 15 U.S.C. § 1681p.
195. TRW, Inc. v. Andrews, 534 U.S. 19 (2001).

period begins to run when the violations occurred, not when the individual discovers them. Many inaccuracies in credit reports, however, are not discovered for a significant period of time.

[D][2] Bank Secrecy Act of 1970

The Bank Secrecy Act, enacted in 1970,[196] requires banks to retain records and create reports to help law enforcement investigations. The Act was passed due to concerns that the computerization of records would make white collar crime more difficult to detect.[197] Federally insured banks must record the identities of account holders and maintain copies of each financial instrument. International transactions exceeding $5,000 are subject to reporting,[198] as well as domestic transactions exceeding $10,000.[199]

In *California Bankers Ass'n v. Shultz*,[200] the Supreme Court upheld the Act against a Fourth Amendment challenge by a group of bankers and account holders. The Court concluded that the bankers lacked Fourth Amendment rights in the data because "corporations can claim no equality with individuals in the enjoyment of a right to privacy."[201] The account holders failed to allege that they engaged in transactions exceeding $10,000, and as a result, lacked standing.[202]

[D][3] United States v. Miller

In 1976, in *United States v. Miller*,[203] the Court held that financial records possessed by third parties are not subject to Fourth Amendment protection.[204] Federal agents issued subpoenas to banks for the financial records of the defendant. The defendant argued that the government needed a warrant in order to obtain the information. The Court concluded that the defendant lacked a reasonable expectation of privacy in the records because "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities."[205] As the Court reasoned:

---

196. Pub. L. No. 91-508.
197. H. JEFF SMITH, MANAGING PRIVACY 24 (1994).
198. *See* 31 C.F.R. §§ 103.23, 103.25.
199. *See* 31 C.F.R. § 103.22.
200. Cal. Bankers Ass'n v. Shultz, 416 U.S. 21 (1974).
201. *Id.* at 65.
202. *Id.* at 67–68.
203. United States v. Miller, 425 U.S. 435, 435 (1976).
204. *Id.* at 442–43.
205. *Id*. at 443.

> The checks are not confidential communications but negotiable instruments to be used in commercial transactions. All of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business.[206]

[D][4] Right to Financial Privacy Act of 1978

In 1978, two years after *Miller*, Congress passed the Right to Financial Privacy Act (RFPA),[207] which provided limited protection of financial records to fill the gap left by *Miller*. Pursuant to the RFPA, government officials must use a warrant or subpoena to obtain financial information.[208] There must be "reason to believe that the records sought are relevant to a legitimate law enforcement inquiry."[209] Subject to certain exceptions, the customer must receive prior notice of the subpoena.[210]

[E] The Retreat from *Boyd*

The 1886 case, *Boyd v. United States*, established that the Fourth and Fifth Amendments prevented the government from issuing a subpoena to obtain a person's private papers.[211] Later on, in *Gouled v. United States*,[212] the Court concluded that the police could not search one's "house or office or papers" to obtain evidence to use against that person in a criminal proceeding.[213] These two cases established what became known as the "mere evidence rule," which barred the seizure of papers unless they were instrumentalities of a crime or illegal contraband. Although the mere evidence rule was chipped away in subsequent decisions, it was officially eliminated in 1967 in *Warden v. Hayden*.[214] In *Couch v. United States*,[215] the Court concluded that personal records maintained by third parties were not protected by the Fifth Amendment. The

---

206. *Id.* at 442.
207. Pub. L. No. 95-630.
208. *See* 29 U.S.C. §§ 3401–22. For more information on the RFPA, see George B. Trubow & Dennis L. Hudson, *The Right to Financial Privacy Act of 1978: New Protection from Federal Intrusion, 12* J. MARSHALL J. PRAC. & PROC. 487 (1979).
209. 29 U.S.C. § 3407.
210. *Id.* § 3409.
211. *See supra* section 1:3.2.
212. Gouled v. United States, 255 U.S. 298 (1921).
213. *Id.* at 309.
214. Warden v. Hayden, 387 U.S. 294 (1967).
215. Couch v. United States, 409 U.S. 322 (1973).

Court noted that "the Fifth Amendment privilege is a *personal* privilege: it adheres basically to the person, not to information that may incriminate him."[216] Since the subpoena was issued on a third party, "[i]nquisitorial pressure or coercion against a potentially accused person, compelling her, against her will, to utter self condemning words or produce incriminating documents is absent."[217] Similarly, in *Fisher v. United States*,[218] the Court concluded that the Fifth Amendment privilege did not apply to subpoenas for documents maintained by a person's attorney.[219] The Fifth Amendment, concluded the court, was limited to protecting against only the "compulsion to testify against oneself."[220]

[F] The Narrowing of the Fourth Amendment

In the late 1970s, the Supreme Court issued several decisions constraining the scope of Fourth Amendment protection. In 1979, the Court concluded in *Smith v. Maryland*[221] that the Fourth Amendment did not apply to a list of the telephone numbers a person dials that were recorded by a pen register.[222] Since people "know that they must convey numerical information to the phone company" and that the phone company records this information for billing purposes, people cannot "harbor any general expectation that the numbers they dial will remain secret."[223] Just three years earlier, the Court in *Miller* had employed a similar rationale with regard to bank records.[224]

In 1978, the Court held in *Zurcher v. Stanford Daily*,[225] that the Fourth Amendment did not prohibit state authorities from searching the premises of third parties if the authorities had probable cause to believe that evidence of a crime would be located at the property.[226] *Zurcher* involved a search of the offices of a newspaper that had taken photographs of a violent demonstration. The newspaper had no involvement in the demonstration and nobody at the newspaper was suspected of criminal activity. The newspaper argued that searches of their offices "will seriously threaten the ability of the press to gather, analyze, and disseminate news."[227] The

---

216. *Id*. at 328.
217. *Id.* at 329.
218. Fisher v. United States, 425 U.S. 391 (1976).
219. *See id.* at 414.
220. *Id.*
221. Smith v. Maryland, 442 U.S. 735 (1979).
222. *Id.* at 743.
223. *Id.*
224. *See supra* section 1:4.2[D][3].
225. Zurcher v. Stanford Daily, 436 U.S. 547 (1978).
226. *Id.* at 554.
227. *Id*. at 563.

Court, however, concluded that the requirements of a warrant "should afford sufficient protection" against these harms.[228]

§ 1:4.3 The 1980s

[A] Receding Fourth Amendment Protection

Throughout the 1980s, the Supreme Court issued a series of decisions adopting a narrow view of what constitutes a reasonable expectation of privacy. For example, in *Florida v. Riley*,[229] the Court concluded that there was no reasonable expectation of privacy in a greenhouse when the police flew over it with a helicopter.[230] In *California v. Greenwood*,[231] the Court held that there was no reasonable expectation of privacy in garbage left in bags on the curb because "[i]t is common knowledge that plastic bags left on or at the side of a public street are readily accessible to animals, children, scavengers, snoops, and other members of the public."[232] The Court also reasoned that the trash was left at the curb "for the express purpose of conveying it to a third party, the trash collector, who might himself have sorted through [the] trash or permitted others, such as the police, to do so."[233]

In the schools and the workplace, the Court concluded that people only have limited expectations of privacy and that searches by school officials and government employers are not subject to regular Fourth Amendment requirements. In *New Jersey v. T.L.O.*,[234] the Court concluded that the Fourth Amendment's warrant requirement "is unsuited to the school's environment" and that probable cause "is not an irreducible requirement of a valid search."[235] Likewise, at the workplace, the Court held in *O'Connor v. Ortega*,[236] that searches by government employers do not require a warrant or probable cause; they only need to be "reasonable . . . under all circumstances."[237]

---

228. *Id.* at 565.
229. Florida v. Riley, 488 U.S. 445 (1989).
230. *See id.* at 451–52.
231. California v. Greenwood, 486 U.S. 35 (1988).
232. *Id.* at 40.
233. *Id.*
234. New Jersey v. T.L.O., 469 U.S. 325 (1984).
235. *Id.* at 340.
236. O'Connor v. Ortega, 480 U.S. 709 (1987).
237. *Id.* at 725–26.

[B] The Growth of Federal Privacy Statutory Protection

[B][1] Privacy Protection Act of 1980

Dissatisfaction over *Zurcher* led Congress to pass the Privacy Protection Act in 1980.[238] The Act restricts the search or seizure of "any work product materials possessed by a person reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication."[239] As a result of the Act, a subpoena is needed to obtain work product materials, which permits the party to challenge the request in court and to produce the documents without having law enforcement officials intrude on the premises.

[B][2] Cable Communications Policy Act of 1984

The Cable Communications Policy Act (CCPA) of 1984[240] protects the privacy of cable records. Cable companies must notify subscribers about the collection and use of personal information.[241] Companies cannot disclose a subscriber's viewing habits.[242] The Act is enforced with a private right of action.

[B][3] Computer Matching and Privacy Protection Act of 1988

As discussed earlier, a major loophole in the Privacy Act of 1974 has been the "routine use" exception.[243] Under this exception, to detect fraud, the federal government in 1977 began running computer comparisons of employee records with the records of people receiving benefits.[244] In 1988, Congress addressed this practice, known as "computer matching" by passing the Computer Matching and Privacy Protection Act.[245] The law established procedures for computer matchings, but did not halt the practice.[246]

---

238. Pub. L. No. 96-440, 94 Stat. 1879, codified at 42 U.S.C. § 2000aa.
239. 42 U.S.C. § 2000aa(a).
240. 42 U.S.C. § 551.
241. *See* 42 U.S.C. § 551(a)(1).
242. *See* 42 U.S.C. § 551(c)(2)(C)(ii).
243. *See supra* section 1:4.2[C][4].
244. *See* REGAN, *supra* note 114, at 86; GELLMAN, *supra* note 174, at 198–99.
245. *See* Computer Matching and Privacy Protection Act (CMPPA) of 1988, Pub. L. No. 100-503, 102 Stat. 2507 (codified as amended at 5 U.S.C. § 552a(a)(8)–(13), (e)(12), (o)–(r), (u)).
246. *See* U.S. Gen. Accounting Office, Computer Matching: Quality of Decisions and Supporting Analyses Little Affected by 1988 Act 3 (1993); PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW 101 (1996).

[B][4] Employee Polygraph Protection Act of 1988

In 1988, Congress passed the Employee Polygraph Protection Act (EPPA).[247] The EPPA prohibits private sector employers from using polygraph examinations on employees and prospective employees. The Act does not apply to public sector employers.[248] Employers can, however, use polygraphs "in connection with an ongoing investigation involving economic loss or injury to the employer's business, such as theft, embezzlement, misappropriation, or an act of unlawful industrial espionage or sabotage" when "the employer has a reasonable suspicion that the employee was involved in the incident or activity under investigation."[249] Private sector employers who provide security services are exempt.[250]

[B][5] Video Privacy Protection Act of 1988

The confirmation hearings of Supreme Court Justice nominee Robert Bork sparked a law to protect videocassette rental data. Reporters attempted to obtain a list of the videos Bork had rented from his video store. Incensed at this practice, Congress passed the Video Privacy Protection Act (VPPA) of 1988.[251] The VPPA forbids videotape service providers from disclosing customer video rental or purchase information.[252]

[C] Electronic Communications Privacy Act of 1986

In 1986, Congress revisited its wiretapping law by substantially reworking Title III of 1968. The Electronic Communications Privacy Act (ECPA)[253] expanded Title III to new forms of communications, with a particular focus on computers. The ECPA restricts the interception of transmitted communications[254] and the searching of stored communications.[255] Title I of the ECPA, known as the "Wiretap Act," regulates the interception of communications.[256] Title II, referred to as the "Stored Communications Act," governs access to

247. Pub. L. No. 100-618, codified at 29 U.S.C. § 2001–09.
248. 29 U.S.C. § 2006(a).
249. 29 U.S.C. § 2006(d).
250. 29 U.S.C. § 2006(e).
251. Pub. L. No. 100-618, 102 Stat. 3195, (codified at 18 U.S.C. §§ 2710–11).
252. 18 U.S.C. § 2710(b).
253. 18 U.S.C §§ 2510–22, 2701–11, 3121–27.
254. 18 U.S.C. §§ 2510–22.
255. 18 U.S.C. §§ 2701–11.
256. 18 U.S.C. §§ 2510–22.

stored communications and records held by communications service providers (such as ISPs).[257] Title III, called the "Pen Register Act," provides limited regulation of pen registers and trap and trace devices.[258]

[D] OECD Guidelines and International Privacy

Internationally, there was substantial growth in information privacy law. The most significant development was the creation of guidelines for the protection of information privacy by the Organization of Economic Cooperation and Development (OECD) in 1980.[259] The OECD Privacy Guidelines built upon the Fair Information Practices articulated by HEW in 1973. The OECD Guidelines contain eight principles:

(1) collection limitation—data should be collected lawfully with the individual's consent;

(2) data quality—data should be relevant to a particular purpose and be accurate;

(3) purpose specification—the purpose for data collection should be stated at the time of the data collection and the use of the data should be limited to this purpose;

(4) use limitation—data should not be disclosed for different purposes without the consent of the individual;

(5) security safeguards—data should be protected by reasonable safeguards;

(6) openness principle—individuals should be informed about the practices and polices of those handling their personal information;

(7) individual participation—people should be able to learn about the data that an entity possesses about them and to rectify errors or problems in that data;

(8) accountability—the entities that control personal information should be held accountable for carrying out these principles.

---

257. 18 U.S.C. §§ 2701–11.

258. 18 U.S.C. §§ 3121–27.

259. GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA, *available in* MARC ROTENBERG, PRIVACY LAW SOURCEBOOK (2002). For a comparison of U.S. privacy law to the OECD guidelines, see Joel R. Reidenberg, *Restoring Americans' Privacy in Electronic Commerce*, 14 BERKELEY J. L. & TECH. 771 (1999).

§ 1:4.4 The 1990s

[A] The Internet, Computer Databases, and Privacy

The last decade of the twentieth century presented profound new challenges for the protection of information privacy, such as rise of the Internet and the increasing use of email in the mid 1990s. The Internet presented new methods of gathering information. When a person visits a website, the website can record information about the person and how the person navigates the website. This information is referred to as "clickstream data." To identify users, companies use an identifying tag known as a "cookie," a text file that is stored on the user's computer. When the user returns to the website, the site searches for its cookie, which identifies the user and allows the website to access the data it collected about the user from her previous web surfing activity. Another information collection device, known as a "web bug," secretly uses pixel tags to gather data about the user.[260]

Throughout the 1990s, the collection and use of personal information in computer databases rapidly accelerated. The decade saw the rise of an entire industry devoted to aggregating personal information for use by marketers—the database industry. Hundreds of companies gather personal data and create massive databases, which they then rent to marketers. The industry generates billions of dollars each year.[261]

[B] The Continued Growth of Federal Statutory Protection

As in the 1980s, Congress continued to pass a number of major statutes to address emerging privacy problems.

[B][1] Telephone Consumer Protection Act of 1991

In 1991, Congress enacted the Telephone Consumer Protection Act (TCPA),[262] which permits people to request that telemarketers not call them again. If the telemarketer continues to call, people can sue for damages of up to five hundred dollars for each call.[263]

---

260. *See* Robert O'Harrow, Jr., *Fearing a Plague of 'Web Bugs'; Invisible Fact-Gathering Code Raises Privacy Concerns*, WASH. POST, Nov. 13, 1999, at E1; Leslie Walker, *Bugs That Go Through Computer Screens*, WASH. POST, Mar. 15, 2001, at E1.
261. *See* Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1407–09 (2001).
262. Pub. L. No. 102-243, 105 Stat. 2394 (codified at 47 U.S.C. § 227).
263. 47 U.S.C. § 227(c)(5).

[B][2] Driver's Privacy Protection Act of 1994

For many years, states had been selling their motor vehicle records to marketers.[264] The sale of this information generated millions of dollars to states, and individuals had no way to block the dissemination of their personal data.[265] In 1994, Congress passed the Driver's Privacy Protection Act (DPPA),[266] which requires that states first obtain a person's consent before disclosing her motor vehicle record information to marketers.[267] The law was challenged on federalism grounds, but in *Reno v. Condon*,[268] the Supreme Court held that DPPA fell within Congress's authority to regulate interstate commerce:

> The motor vehicle information which the States have historically sold is used by insurers, manufacturers, direct marketers, and others engaged in interstate commerce to contact drivers with customized solicitations. The information is also used in the stream of interstate commerce by various public and private entities for matters related to interstate motoring.[269]

This decision has important implications for many federal privacy statutes. Even in the face of the Court's trend to limit Congress's power under the Commerce Clause, the Court recognized that the dissemination of personal information is an issue of interstate commerce.

[B][3] Health Insurance Portability and Accountability Act of 1996

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 is the first federal statute to directly address health privacy.[270] HIPPA required the Department of Health and Human Services (HHS) to draft regulations to protect the privacy of medical records.[271] HHS's regulations, among other things, require that people authorize all uses and disclosures of their health information that are not for treatment, payment, or health care operation (such as for marketing purposes).[272]

---

264. *See* Rajiv Chandrasekaran, *Governments Find Information Pays*, WASH. POST, Mar. 9, 1998, at A1.
265. *See id.*
266. 18 U.S.C. §§ 2721–25.
267. *See* 18 U.S.C. § 2721(b)(12).
268. Reno v. Condon, 528 U.S. 141, 144–45 (2000).
269. *Id.* at 148.
270. Pub. L. No. 104-191, 110 Stat. 1936.
271. 110 Stat. at 2033–34.
272. 45 C.F.R. § 164.508(a).

HIPAA does have some important limitations. First, not all medical records are covered—only records maintained by certain types of record-holders: health plans, health care clearinghouses, and health care providers.[273] Although physicians, hospitals, pharmacists, and health insurers are covered, other parties that have medical information are not.[274] For example, many websites gather health information when conducting medical assessments, but these websites are not covered by HIPAA.[275]

Second, the regulations contain a broad provision for law enforcement access. They permit law enforcement officials to obtain medical records with only a subpoena rather than a warrant.[276] Additionally, law enforcement officials can obtain health data if they request it "for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person."[277]

[B][4] Children's Online Privacy Protection Act of 1998

The Children's Online Privacy Protection Act (COPPA) of 1998[278] governs the collection of children's personal information on the Internet.[279] The law only applies to children under the age of thirteen.[280] Children's websites must post privacy policies and obtain "parental consent for the collection, use, or disclosure of personal information from children."[281] COPPA applies only to websites "directed to children" or where the operator of the website "has actual knowledge that it is collecting personal information from a child."[282]

---

273. *Id.* § 160.102.
274. PEW INTERNET & AMERICAN LIFE PROJECT, INSTITUTE FOR HEALTHCARE RESEARCH AND POLICY, GEORGETOWN UNIVERSITY, EXPOSED ONLINE: WHY THE NEW FEDERAL HEALTH PRIVACY REGULATION DOESN'T OFFER MUCH PROTECTION TO INTERNET USERS 6–8 (Nov. 2001).
275. *See id.* at 7.
276. 45 C.F.R. § 164.512(f)(1)(ii).
277. *Id.* § 164.512(f)(2).
278. 15 U.S.C. §§ 6501–06.
279. 15 U.S.C. § 6502(a)(1).
280. 15 U.S.C. § 6501(1).
281. 15 U.S.C. § 6502(b)(1)(A)(ii).
282. 15 U.S.C. § 6502(b)(1)(A).

[B][5] The Gramm-Leach-Bliley Act of 1999

In 1999, Congress passed the Gramm-Leach-Bliley (GLB) Act,[283] which allows financial institutions with different branches or affiliates engaging in different services to share the "nonpublic personal information" among each branch of the company. Affiliates must inform customers of the information sharing, but people have no right to stop the companies from sharing it. However, when financial institutions desire to share customer data with third parties, people have a right to opt-out.[284]

The GLB Act resulted in a mass mailing of privacy policies to customers, informing them that data might be shared with other companies and giving people a number to call or a form to fill out if they wanted to block this data sharing. The opt-out provisions of the Act were strongly criticized. For example, as Ted Janger and Paul Schwartz noted, very few customers have opted-out.[285] The reasons, they stated, are that privacy policies are hard to understand and are sometimes misleading; and opt-out rights are difficult and cumbersome to exercise.[286]

[C] The FTC and Privacy Policies

Since 1998, the Federal Trade Commission (FTC) has been bringing actions against companies that violate their own privacy policies. The FTC has interpreted the FTC Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce,"[287] to be infringed when a company breaks a promise it made in its privacy policy. The FTC can bring civil actions and seek injunctive remedies. Since it began enforcing the Act in this manner, the FTC has brought several high-profile cases, almost all of which have resulted in settlements.[288]

[D] The EU Data Protection Directive

In 1996, the European Union promulgated the Data Protection Directive,[289] which establishes basic principles for privacy legislation for European Union member countries. As Joel Reidenberg explains:

---

283. Pub. L. No. 106-102, 113 Stat. 1338, (codified at 15 U.S.C. §§ 6801-–09).
284. 15 U.S.C. § 6802(a), (b).
285. Ted Janger & Paul M. Schwartz, *The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules*, 86 MINN. L. REV. 1219, 1230 (2002).
286. *See id.* at 1230–41.
287. 15 U.S.C. § 45.
288. *See* SOLOVE ET AL., *supra* note 61, at 750–59.
289. Council Directive 95/46, 1995 O.J. (L 281) 31–50 (EC), hereinafter "EU Data Protection Directive."

> The background and underlying philosophy of the European Union Directive differs in important ways from that of the United States. . . . [T]he United States has, in recent years, left the protection of privacy to markets rather than law. In contrast, Europe treats privacy as a political imperative anchored in fundamental human rights.[290]

The EU Data Protection Directive provides for a comprehensive protection of personal information maintained by a broad range of entities. This omnibus approach exists in stark contrast to the United States' approach, which regulates privacy "sectorally" in various narrow contexts.[291]

The EU Data Protection Directive also contains restrictions on the flow of personal data outside the borders of EU nations to other countries not governed by the Directive. Data can be transferred to a third country if the country "ensures an adequate level of protection."[292] As Peter Swire and Robert Litan observed, the vastly different approaches of the United States and EU presented significant problems, since the United States may not be found to have an "adequate level of protection" and this would have severe commercial implications.[293] In 1998, the U.S. Department of Commerce began negotiating with the EU so that the United States would satisfy the Directive's requirement of having adequate protection. In 2000, an agreement was reached, known as the Safe Harbor Arrangement. Under the Arrangement, U.S. companies can voluntarily agree to follow principles (drawn from the Fair Information Practices). Compliance with the principles will be enforced by the FTC and Department of Transportation.[294]

---

290. Joel R. Reidenberg, *E-Commerce and Trans-Atlantic Privacy*, 38 HOUS. L. REV. 717, 730 (2001).
291. *See* Joel R. Reidenberg, *Setting Standards for Fair Information Practices in the U.S. Private Sector*, 80 IOWA L. REV. 497 (1995).
292. EU Data Protection Directive, Article 25(1).
293. *See generally* PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE (1998).
294. *See* SOLOVE ET AL., *supra* note 61, at 936–42.

§ 1:5 The Twenty-First Century

§ 1:5.1 After September 11: Privacy in a World of Terror

In the aftermath of the terrorist attacks on September 11, 2001, the nation awakened to the reality that there were dangerous terrorist cells within U.S. borders. Shortly after September 11, there was a strong political drive for new surveillance measures and new powers for law enforcement officials.

[A] The USA PATRIOT Act of 2001

In a very short time after September 11, Congress passed the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act" (USA PATRIOT Act) of 2001. The Act made several significant changes to the ECPA and FISA, among other statutes. In one amendment, the USA PATRIOT Act enlarged the definition of pen registers and trap and trace devices to apply to addressing information on emails and to "IP addresses."[295] The Act also provided for new justifications for delayed notice of search warrants, increasing the types of subscriber records that could be obtained from ISPs and communications providers, and allowing for a nationwide scope for pen register orders and search warrants for email.[296] The Act also provided for roving wiretaps under FISA as well as increased sharing of foreign intelligence information between law enforcement entities.[297]

Additionally, the Act expanded the application of the Foreign Intelligence Surveillance Act (FISA). Previously, the looser protections of FISA applied only when "the purpose" of the investigation was to gather foreign intelligence. The USA PATRIOT Act expanded FISA's application to instances when foreign intelligence gathering is "a significant purpose" of the investigation.[298]

[B] The FISA "Wall"

Following 9/11, a contentious debate emerged about the FISA "wall." Since FISA allows law enforcement to use the information gathered to prosecute crimes, there is a danger that FISA (a statute designed for foreign intelligence gathering) will be used as an end-around of the more stringent procedures in ECPA (a statute designed to regulate electronic surveillance for domestic criminal

---

295. *See* 18 U.S.C. § 3127(3) as amended by the USA PATRIOT Act § 216.
296. *See* SOLOVE ET AL., *supra* note 61, at 294–300.
297. *See id.* at 343.
298. 50 U.S.C. § 1804(a)(7)(B) as amended by USA PATRIOT Act § 204.

investigations). To protect against this, an "information screening wall" is established to prevent law enforcement officials from initiating or directing FISA surveillance. Relevant information is passed on to law enforcement, but the law enforcement officials are walled off from having control over the FISA surveillance.[299] Unfortunately, during the investigation of the 9/11 terrorists prior to 9/11, FBI officials were deeply confused about FISA and the "wall," and this stymied the investigation.[300]

In 2002, Attorney General John Ashcroft submitted to the FISA court new FISA investigation procedures that substantially diminished the "wall." The FISA court rejected the procedures, noting many errors in prior FISA applications and emphasizing the importance of the "wall."[301] The government appealed to the Foreign Intelligence Surveillance Court of Review, which in 2002, released its first and only published opinion, *In re Sealed Case*.[302] The court reversed the FISA court, and it concluded that the USA PATRIOT Act, "by using the word 'significant,' eliminated any justification for the FISA court to balance the relative weight the government places on criminal prosecution as compared to other counterintelligence responses."[303]

[C] The Homeland Security Act of 2002

In 2002, Congress passed the Homeland Security Act,[304] which created the Department of Homeland Security (DHS), consisting of twenty-two federal agencies. The Act created a Privacy Office for ensuring compliance with privacy laws.

[D] The Intelligence Reform and Terrorism Prevention Act of 2004

In 2004, Congress passed the Intelligence Reform and Terrorism Prevention Act to facilitate greater information sharing between federal agencies. The Act requires that intelligence be "provided in its most shareable form" and it aims to "promote a culture of information sharing."

---

299. For more information on the "wall," see Peter Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. 1306 (2004); Paul Rosenzweig, *Civil Liberty and the Response to Terrorism*, 42 DUQ. L. REV. 663 (2004); Jamie S. Gorelick, *The Truth About "the Wall,"* WASH. POST, Apr. 18, 2004, at B7.
300. The 9/11 Commission Report (2004).
301. *In re* All Matters Submitted to the Foreign Intelligence Surveillance Court (May 17, 2002).
302. *In re* Sealed Case, 310 F.3d 717 (U.S. Foreign Intelligence Surveillance Ct. Rev. 2002).
303. *Id.*
304. 6 U.S.C. § 222.

[E] The Real ID Act of 2005

Attached to a military spending bill, and passed without debate, the Real ID Act of 2005 mandated that state driver's licenses meet federal standards set forth by the DHS.[305] Critics claimed that it would establish a de facto national identification card and that it would be extremely costly for the states to implement.

[F] NSA Warrantless Surveillance

In December 2005, the *New York Times* reported that the Bush Administration had secretly authorized the National Security Administration (NSA) to engage in warrantless electronic surveillance of American citizens.[306] A debate has ensued about whether the President violated FISA in conducting the surveillance and, if so, whether the President has the constitutional power to conduct the surveillance notwithstanding the limits set forth in FISA.

§ 1:5.2 Consumer Privacy

[A] The Fair and Accurate Credit Transactions Act of 2003

In 2003, Congress passed the Fair and Accurate Credit Transactions Act (FACTA), which amended the Fair Credit Reporting Act and extended its preemption on certain state law provisions addressing identity theft and credit reporting. Among other things, the FACTA provided some limited protections against identity theft. For example, FACTA requires credit reporting agencies to provide people with a free credit report each year. It requires credit reporting agencies to disclose to a consumer her credit score, and it allows victims of fraud to alert just one credit reporting agency, which then must notify the others. These provisions and others were criticized by many as not going far enough to address the problem of identity theft.

---

305. The "Real ID Act" was attached to the Emergency Supplemental Appropriation for Defense, the Global War on Terror, and Tsunami Relief, H.R. 1268, Pub. L. No. 109-13 (2005). The driver's license requirements are in § 202 of the Act.
306. James Risen & Eric Lichtblau, *Bush Secretly Lifted Some Limits on Spying in U.S. After 9/11, Officials Say*, N.Y. TIMES, Dec. 15, 2005.

[B] The National Do-Not-Call Registry

In an effort to address unwanted telemarketing calls, the Federal Trade Commission (FTC) and the Federal Communications Commission (FCC) created a do-not-call registry.[307] People can voluntarily register their telephone numbers, and commercial telemarketers are prohibited from calling the numbers. Telemarketers challenged the do-not-call registry as a violation of their First Amendment rights. In 2004, a federal circuit court concluded in *Mainstream Marketing Services, Inc. v. Federal Trade Commission*[308] that the do-not-call registry satisfied the Central Hudson balancing test for commercial speech and therefore did not run afoul of the First Amendment.

[C] The CAN-SPAM Act of 2003

In 2003, Congress enacted the Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM).[309] The Act restricts knowingly sending commercial messages to deceive or mislead recipients. It requires spammers to contain a return address to allow people to opt out and it creates civil and criminal penalties for violations.

[D] *Remsburg v. Docusearch*

The New Hampshire Supreme Court adopted a bold new theory upon which companies could be liable for the way they disseminate personal information. In *Remsburg v. Docusearch, Inc.*,[310] a man bought data about a woman from a database company. He used the information about her work address to confront her at her place of employment and kill her. The court held that the company could be liable if it did not act with "reasonable care in disclosing a third person's personal information to a client."[311]

[E] Privacy Policies and Contract Law

After 9/11, federal agencies contacted several airlines and requested that they turn over their passenger records, which contained personal information about passengers including names, flight numbers, credit card information, hotel information, and meal requests. Several airlines complied, but their compliance was

---

307. The FTC rule is at 16 C.F.R. § 310.4(b)(1)(iii)(B), and the F.C.C. rule is at 47 C.F.R. § 64.1200(c)(2).
308. Mainstream Mktg. Servs., Inc. v. FTC, 358 F.3d 1228 (10th Cir. 2004).
309. 15 U.S.C. § 7701 *et seq*.
310. Remsburg v. Docusearch, Inc., 816 A.2d 1001 (N.H. 2003).
311. *Id.*

in breach of their privacy policies. In several cases, groups of plaintiffs sued the airlines for breach of contract. However, courts concluded that general statements of policy were not contractual and that the plaintiffs had failed to establish damages.[312]

[F] Data Security Breaches

In February and March of 2005, several data brokers announced major security breaches in the personal data that they stored. ChoicePoint, one of the largest data brokers with files on nearly every American citizen, sold personal data on over 145,000 people (the figure was later revised to 162,000) to fraudulent companies established by a ring of identity thieves.[313] Other companies announced data leaks and break-ins, including LexisNexis.[314] These events gave renewed attention to the growing problem of identity theft, a crime that affects about 10 million Americans each year.[315]

The ChoicePoint breach came to light when ChoicePoint mailed letters to 30,000 California residents informing them of what had happened. This disclosure was done pursuant to California's security breach notice requirement, which provided:

> Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement. . . .[316]

---

312. *See* Dyer v. Nw. Airlines Corp., 334 F. Supp. 2d 1196 (D.N.D. 2004); *In re* Nw. Airlines Privacy Litig., 2004 WL 1278459 (D. Minn. 2004); *In re* Jetblue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299 (E.D.N.Y. 2005).
313. Joseph Menn, *Did the ChoicePoint End Run Backfire?*, L.A. TIMES, Mar. 13, 2005; Bob Sullivan, *Database Giant Gave Access to Fake Firms*, MSNBC, Feb. 14, 2005, at www.msnbc.msn.com/id/6969799/.
314. Ellen Simon, *U.S. Citizens' Data Possibly Compromised*, S.F. CHRONICLE, Mar. 9, 2005. For more background about consumer privacy and data brokers, as well as legislative proposals to address the problem, see Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection*, 2006 ILL. L. REV. 357 (2006).
315. Federal Trade Commission, Identity Theft Survey Report 4 (Sept. 2003). For an excellent discussion of identity theft, see BOB SULLIVAN, YOUR EVIL TWIN: BEHIND THE IDENTITY THEFT EPIDEMIC (2004).
316. S.B. 1386, codified at CAL. CIV. CODE § 1798.82(a)).

Soon thereafter, the attorney generals of other states began demanding that their residents be notified as well, and ChoicePoint announced that it would voluntarily notify all who had been affected.

By early 2006, nearly half of the states had passed security breach disclosure laws similar to California's, and about a dozen had passed security freeze laws that allow people to freeze access to their credit reports.[317] Bills are pending in many more states.

§ 1:6 Conclusion

Information privacy law has come a long way. Spurred by the development of new technologies, the law has responded in numerous ways to grapple with emerging privacy problems. Although the law has made great strides, much work remains to be done. Several scholars, including myself, have criticized the ability of information privacy laws thus far to grapple with the growing collection and use of personal information in computer databases.[318] Recent books, such as Robert O'Harrow's *No Place to Hide* and my own book, *The Digital Person: Technology and Privacy in the Information Age*, have aimed to bring greater attention to the effects of companies maintaining extensive dossiers of information about individuals and selling this data to government agencies for profiling and investigatory purposes.[319] As Paul Schwartz observes, "personal information in the private sector is often unaccompanied by the presence of basic legal protections. Yet, private enterprises now control more powerful resources of information technology than ever before."[320]

---

317. For a compilation of these laws, see State PIRG Summary of State Security Freeze and Security Breach Notification Laws, *available at* www.pirg.org/consumer/credit/statelaws.htm.

318. *See, e.g.*, Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393 (2001); Daniel J. Solove, *Access and Aggregation: Public Records, Privacy, and the Constitution*, 86 MINN. L. REV. 1137 (2002); Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083 (2002); Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373 (2000); Elbert Lin, *Prioritizing Privacy: A Constitutional Response to the Internet*, 17 BERKELEY TECH. L.J. 1085 (2002); Stan Karas, *Privacy, Identity, Databases*, 52 AM. U. L. REV. 393 (2002).

319. ROBERT O'HARROW, JR., NO PLACE TO HIDE (2005); DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE (2004).

320. Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1633 (1999).