CHAPTER 1

The Constitutional Right to Privacy, Privacy Legislation, and Government Access to Personal Information

by
Blaze D. Waleski*

Chapter Contents

---

* Blaze Waleski is Special Counsel in the New York office of Sullivan & Cromwell LLP. The author acknowledges the assistance of Lissa Bourjolly, an associate in the New York office of Fulbright & Jaworski L.L.P., in preparing this chapter.

§ 1.01 Introduction

Restraints on governmental powers are a cornerstone of American jurisprudence. The United States legal system has long recognized limitations on government intrusion upon the privacy of individuals. Although the United States Constitution does not expressly refer to a right of privacy, the Constitution, and particularly the Bill of Rights, has been interpreted by the United States Supreme Court to protect individual privacy in certain contexts.

It is well established that this constitutional right of privacy extends to certain fundamental zones of privacy deemed "implicit in the concept of ordered liberty."[1] Only the most intimate phases of personal life—such as those involving abortion, the use of contraceptives, or sexual orientation—have been held to be constitutionally protected.[2] It is also well established that the "Fourth Amendment

---

[1] Palko v. Connecticut, 302 U.S. 319, 325, 58 S.Ct. 149, 82 L.Ed. 288 (1937).

[2] See:

Supreme Court: Eisenstadt v. Baird, 405 U.S. 438, 453-454, 92 S.Ct. 1029, 31 L.Ed.2d 349 (1972); Stanley v. Georgia, 394 U.S. 557, 564-565, 89 S.Ct. 1243, 22 L.Ed.2d 542 (1969); Griswold v. Connecticut, 381 U.S. 479, 484-486, 85 S.Ct. 1678, 14 L.Ed.2d 510 (1965).

explicitly affirms the 'right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.'"[3] In varying contexts, the Court has found a constitutional right of privacy rooted in the First Amendment, the Third Amendment, the Fourth and Fifth Amendments, the Ninth Amendment, and the Fourteenth Amendment.

The constitutional right of privacy does not extend to protect from government intrusion the privacy of personal information, *per se*, although it does limit the government's access to such information in certain contexts, and it circumscribes the use of that information in criminal proceedings when the information was obtained in violation of the Fourth and Fifth Amendments. In addition to the constitutional right of privacy, there are various statutory proscriptions on the access to and use of personal information, some of which govern access and use by the government, and others that extend to the private sector. This chapter will outline the constitutional right of privacy, and will also discuss relevant statutes that impact access to and use of personal information by both the government and private individuals.

Eighth Circuit: McNally v. The Pulitzer Publishing Co., 532 F.2d 69, 76 (8th Cir. 1976), citing Roe v. Wade, 410 U.S. 113, 152-154, 93 S.Ct. 705, 35 L.Ed.2d 147 (1973).

[3] Griswold v. Connecticut, 381 U.S. 479, 484, 85 S.Ct. 1678, 14 L.Ed.2d 510 (1965).

§ 1.02 Constitutional Considerations

The first ten amendments to the United States Constitution—or the Bill of Rights—were added shortly after the Constitution was ratified. Prompted by concerns about governmental tyranny and abuse, the Bill of Rights acknowledges certain fundamental or natural rights vis-à-vis the federal government, and affords protection against various government intrusions upon the individual. The First, Third, Fourth, Fifth, Ninth and Fourteenth Amendments have in some degree been interpreted to proscribe indiscriminate governmental invasions of privacy.[1] These restraints on the federal government extend to the state governments via the Fourteenth Amendment.[2]

[1]—The Amendments

The following table identifies the amendments to the United States Constitution that support a constitutional right of privacy.

Amendment	Relevant Language	Comments
First Amendment	"Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances."	The First Amendment protects free speech and freedom of association. It guarantees the right to free speech, to speak anonymously, to associate and to preserve the confidentiality of associations. Stanley v. Georgia, 394 U.S. 557, 564, 89 S.Ct. 1243, 22 L.Ed.2d 542 (1969) (state statute making illegal the mere possession of obscene material violated First and Fourteenth Amendments).
Third Amendment	"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."	The Third Amendment guarantees against military appropriation of private homes for peacetime quartering of troops.

---

[1] "The constitutional protection of the right to privacy is a relatively new development in our law, but with historical precedent. The right to privacy has been found under the First, Fourth, Fifth, Ninth, and Fourteenth Amendments, and the 'penumbra of the Bill of Rights'. It is clear that, whatever the source of the right, the protection is only as against government intrusions into a person's privacy."

Simmons v. Southwestern Bell Telephone Co., 452 F. Supp. 392, 394, 1978 U.S. Dist. LEXIS 17655 *3 (1978). (Internal citations omitted.)

[2] Meyer v. Nebraska, 262 U.S. 390, 399, 43 S.Ct. 625, 67 L.Ed. 1042 (1923).

Amendment	Relevant Language	Comments
Fourth Amendment	"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."	The Fourth Amendment guarantees against unreasonable searches and seizures of persons and property. Kyllo v. United States, 533 U.S. 27, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001) (government's use of a thermal imaging device to determine if the amount of heat coming from a house was consistent with the high intensity lamps typically used to grow marijuana indoors is a Fourth Amendment search and is presumptively invalid without a warrant); United States v. Place, 462 U.S. 696, 103 S.Ct. 2637, 77 L.Ed.2d 110 (1983) (government's use of a dog to sniff luggage for cocaine did not constitute a search because the dog sniffed particles outside the package). See also, Terry v. Ohio, 392 U.S. 1, 8-9, 88 S.Ct. 1868, 20 L.Ed.2d 889 (1968); Katz v. United States, 389 U.S. 347, 350, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967); Olmstead v. United States, 277 U.S. 438, 478, 48 S.Ct. 564, 72 L.Ed. 944 (1928) (Brandeis, J., dissenting).
Fifth Amendment	"No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a grand jury, except in cases arising in the land or naval forces, or in the militia, when in actual service in time of war or public danger; nor shall any person be subject for the same offense to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation."	The Fifth Amendment guarantees against compelled self-incrimination.

Amendment	Relevant Language	Comments
Ninth Amendment	"The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people."	The Ninth Amendment reserves traditional rights to the people, including the right of bodily integrity, possession, and independent decision-making associated with privacy. Griswold v. Connecticut, 381 U.S. 478, 486, 85 S.Ct. 1678, 14 L.Ed.2d 510 (1965) (Goldberg, J.,

(Text continued on page 1-7)

Amendment	Relevant Language	Comments
		concurring) ("The language and history of the Ninth Amendment reveal that the Framers of the Constitution believed that there are additional fundamental rights, protected from government infringement, which exist alongside those fundamental rights specifically mentioned in the first eight constitutional amendments."). Simmons v. Southwestern Bell Telephone Co., 452 F. Supp. 392, 395, 1978 U.S. Dist. LEXIS 17655 at *7 (1978) ("There is some authority that the Ninth Amendment is the constitutional basis for the protection of privacy, not found specifically in other Amendments. [citing Griswold v. Connecticut] Whatever the source of the right (which source seems to be an argument more of semantics than of substance), the right may be asserted, at least in a constitutional context, only against a governmental intrusion, and only where there exists a reasonable expectation of privacy . . .").
Fourteenth Amendment	"Section 1. All persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the state wherein they reside. No state shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any state deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws."	The Fourteenth Amendment guarantees liberty in providing that no state shall deprive a person of life, liberty or property without due process of law. The Fourteenth Amendment requires the states to honor and protect the constitutional rights of all United States citizens. Meyer v. Nebraska, 262 U.S. 390, 399, 43 S.Ct. 625, 67 L.Ed. 1042 (1923).

[2]—The Constitutional Right of Privacy

A right of privacy is implied in the United States Constitution, and particularly in the Bill of Rights. The word "privacy" does not appear in the Constitution, but the United States Supreme Court has held that there is a constitutional right of privacy.[3] This constitutional right of

[3] See Roe v. Wade, 410 U.S. 113, 152 93 S.Ct. 705, 35 L.Ed.2d 147 (1973) ("The Constitution does not explicitly mention any right of privacy."). See also, Griswold

privacy has not been extended to protect the privacy of personal information, *per se,* although it does, in certain circumstances, restrict the government from acquiring and using certain information.

The first publication of note advocating a right of privacy was the 1890 Harvard Law Review article written by Samuel D. Warren and his law partner, Louis D. Brandeis, entitled "The Right to Privacy."[4]

The implied constitutional right of privacy was initially discussed by the United States Supreme Court as "the right to be let alone" and appeared in a dissenting opinion by Justice Brandeis in the 1928 case, *Olmstead v. United States*, the first wiretapping case heard by the Court:

> "[T]he right to be let alone—the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment."[5]

In a footnote of the decision *Oklahoma Press Publishing Co. v. Walling*, a 1946 case addressing a newspaper's refusal to comply with a subpoena, the Court acknowledged Justice Brandeis's dissent in *Olmstead* as making "the case for protected privacy."[6] Without citing any precedent for the "right . . . to be let alone," the Court, in its 1966 decision in *Tehan v. United States*, stated that the Fourth and Fifth Amendments serve "as a protection of quite different constitutional values reflecting the concern of our society for the right of each individual to be let alone."[7] Over time, the Court applied this concept of the right to be let alone—or right of privacy—in varying but limited contexts.

[a]—Searches and Seizures

The "Fourth Amendment guarantees the 'right of the people to be secure in their persons, houses, papers, and effects, against

---

v. Connecticut, 381 U.S. 479, 482-483, 85 S.Ct. 1678, 14 L.Ed.2d 510 (1965) (discussing that various constitutional rights are not specifically mentioned in the Constitution, and holding that state government may not interfere with a married couple's right to use contraceptives).

[4] Warren and Brandeis, "The Right to Privacy," 4 Harv. L. Rev. 193 (1890).

[5] Olmstead v. U.S., 277 U.S. 438, 478, 48 S.Ct. 564, 72 L.Ed. 944 (1928) (Brandeis, J., dissenting). Three other judges, Justices Holmes, Butler and Stone, also dissented. As early as 1834, the U.S. Supreme Court noted that a "defendant asks nothing—wants nothing, but to be let alone until it can be shown that he has violated the rights of another." Wheaton v. Peters, 33 U.S. 591, 634, 8 L.Ed. 1055 (1834).

[6] Oklahoma Press Publishing Co. v. Walling, 327 U.S. 186, 204, n.30, 66 S.Ct. 494, 90 L.Ed. 614 (1946).

[7] Tehan v. United States, 382 U.S. 406, 416, 86 S.Ct. 459, 15L.Ed.2d 453 (1966).

unreasonable searches and seizures.'"[8] In the 1967 case, *Katz v. United States*, the Court effectively overturned its earlier decision in *Olmstead*, quoting the "right to be let alone" from the 1890 Warren and Brandeis law review article.[9] *Katz* held that recording by police of a conversation in a public telephone booth was a violation of the Fourth Amendment because the speaker had a reasonable expectation of privacy inside the booth. The Court made clear that the Fourth Amendment offers not a general right to privacy, but instead protects against certain kinds of governmental intrusion:

> "[T]he Fourth Amendment cannot be translated into a general constitutional 'right to privacy.' That Amendment protects individual privacy against certain kinds of governmental intrusion, but its protections go further, and often have nothing to do with privacy at all. Other provisions of the Constitution protect personal privacy from other forms of governmental invasion. But the protection of a person's *general* right to privacy—his right to be let alone by other people—is, like the protection of his property and of his very life, left largely to the law of the individual States."[10]

Subsequent cases reinforce the Fourth Amendment's warrant clause and its protection against unwarranted searches and seizures by the government.[11]

[i]—Fourth Amendment Protection for Information

Although the Fourth Amendment protects persons, places and things from unreasonable searches and seizures, it generally has not

---

[8] Griswold v. Connecticut, 381 U.S. 479, 484, 85 S.Ct. 1678, 14 L.Ed.2d 510 (1965).

[9] Katz v. United States, 389 U.S. 347, 350, n.6, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967). The Court cited to the 1890 Warren and Brandeis law review article rather than to Justice Brandeis's dissent in the 1928 *Olmstead* decision.

[10] Katz v. United States, 389 U.S. 347, 350-351, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967). (Emphasis in original; internal citations omitted.)

[11] See, e.g., United States v. United States District Court for the Eastern District of Michigan, 407 U.S. 297, 316, 92 S.Ct. 2125, 32 L.Ed.2d 752 (1972) ("The warrant clause of the Fourth Amendment is not dead language. Rather, it has been 'a valued part of our constitutional law for decades, and it has determined the result in scores and scores of cases in courts all over this country. It is not an inconvenience to be somehow "weighed" against the claims of police efficiency. It is, or should be, an important working part of our machinery of government, operating as a matter of course to check the "well-intentioned but mistakenly overzealous executive officers" who are a part of any system of law enforcement.' Coolidge v. New Hampshire [403 U.S. 443, 481 (1971)]").

been held to protect information, *per se*.[12] For example, it has been held under federal case law interpreting the Fourth Amendment that there is no expectation of privacy in Internet subscriber information.[13] It is well settled under federal law that a person has no reasonable expectation of privacy in information exposed to third parties, such as a bank or a telephone company.[14] Accordingly, an individual has no expectation of privacy in information disclosed to an Internet Service Provider (ISP).[15]

In a decision the court later vacated,[16] the Sixth Circuit Court of Appeals upheld the district court's preliminary injunction declaring unconstitutional that portion of the Stored Communications Act (SCA)[17] that allows law enforcement to compel an ISP to disclose the contents of e-mail stored more than 180 days, by court order upon a showing of "specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation"[18]

The "specific and articulable facts" standard is a standard lower than probable cause required for a warrant under the Fourth Amendment,

---

[12] See, e.g., United States v. Miller, 425 U.S. 435, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976) (Court held that bank records could be properly subpoenaed without a warrant, and that customer had abandoned any expectation of privacy in his banking information by disclosing it to the bank, since he had no Fourth Amendment right to privacy in the bank, itself).

[13] *Second Circuit:* Freedman v. America Online, Inc., 412 F. Supp.2d 174, 181 (D. Conn. 2005); United States v. Cox, 190 F. Supp. 2d 330, 332 (N.D.N.Y. 2002).

Fourth Circuit: United States v. Sherr, 400 F. Supp.2d 843, 848 (D. Md. 2005); United States v. Hambrick, 55 F. Supp. 2d 504, 508-509 (W.D. Va. 1999), *aff'd* 225 F.3d 656 (4th Cir. 2000), *cert. denied* 531 U.S. 1099 (2001).

Sixth Circuit: Guest v. Leis, 255 F.3d 325, 336 (6th Cir. 2001).

Tenth Circuit: United States v. Kennedy, 81 F. Supp.2d 1103, 1110 (D. Kan. 2000).

[14] See: Smith v. Maryland, 442 U.S. 735, 742, 99 S.Ct. 2577, 61 L.Ed.2d 220, (1979) (no privacy interest in telephone numbers dialed); United States v. Miller, 425 U.S. 435, 442, 96 S.Ct. 1619 48 L.Ed.2d 71 (1976) (no privacy interest in bank records).

[15] Guest v. Leis, 255 F.3d 325, 336 (6th Cir. 2001) ("As we have noted above, a person must have a reasonable expectation of privacy in the matter searched in order to challenge a search under the Fourth Amendment. Individuals generally lose a reasonable expectation of privacy in their information once they reveal it to third parties."). But see, State v. Reid, 194 N.J. 386, 945 A.2d 26 (2008), where the New Jersey Supreme Court held under the Constitution of the State of New Jersey that individuals do have an expectation of privacy in Internet subscriber information. See § 1.02[2][b][ii] *infra*.

[16] Warshak v. United States, 2007 U.S. App. LEXIS 23741 (6th Cir. Oct. 9, 2007), *vacating in part* Warshak v. United States, 490 F.3d 455 (6th Cir. 2007).

[17] 18 U.S.C. §§ 2703 *et al*.

[18] Warshak v. United States, 490 F.3d 455, 460 (6th Cir. 2007).

but higher than the general reasonableness standard needed for an administrative subpoena. When individuals have a reasonable expectation of privacy "in their persons, houses, papers, and effects," the Fourth Amendment requires that the government show "probable cause" to obtain a warrant to search or seize such things.[19]

- The SCA requires a *warrant* issued pursuant to the Federal Rules of Criminal Procedure or an equivalent state warrant (i.e., upon probable cause) to obtain the *contents* of e-mail stored 180 days or less.[20]
- The SCA requires a *court order* upon a showing of "specific and articulable facts" to obtain the *contents* of e-mail stored more than 180 days.[21]
- The SCA requires a *judicial subpoena* to obtain the *record* of e-mail, limited to the following information: (1) name; (2) address; (3) local and long-distance telephone connection records, or records of session times and durations; (4) length of service (including start date) and types of service used; (5) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and (6) means and source of payment for such service (including any credit card or bank account number).[22]

Noting that the appropriate standard depends upon the individual's reasonable expectation of privacy, the Sixth Circuit Court of Appeals held that an individual has a reasonable expectation of privacy in the *contents* of the e-mail kept in his e-mail account, regardless of how may days the e-mail had been in storage, and that the Fourth Amendment therefore requires probable cause before the government may seek, *ex parte* (i.e., using a warrant), the disclosure of the contents of stored e-mails.[23] The court's decision would suggest that that portion

---

[19] U.S. Const., 4th Amend.; Warshak v. United States, 490 F.3d 455, 468 (6th Cir. 2007).

[20] 18 U.S.C. § 2703(a).

[21] Such a court order is required if the government seeks to obtain the contents of the e-mail without giving notice to the subscriber or customer that his or her e-mail is to be obtained by the government. 18 U.S.C. § 2703(b). See 18 U.S.C. § 2703(d) for the "specific and articulable facts" requirement for the court order. The delayed notice option is set out at 18 U.S.C. § 2705(a). The government may still obtain the contents of the e-mail without notice to the subscriber if the government obtains a warrant. 18 U.S.C. § 2703(b)(1)(A). Alternatively, the government may use a judicial subpoena to obtain the contents of the e-mail, but must give prior written notice to the subscriber or customer. 18 U.S.C. § 2703(b)(1)(B)(i).

[22] 18 U.S.C. § 2703(c)(2).

[23] Warshak v. United States, 490 F.3d 455, 474 (6th Cir. 2007) ("But the reasonable expectation of privacy of an e-mail user goes to the *content* of the e-mail message."). (Emphasis supplied.)

of the SCA that allows the disclosure of e-mail in storage more than 180 days upon a showing of "specific and articulable facts" is unconstitutional.

The court's analysis in this case would appear to be a departure from the Supreme Court's holding[24] that a bank customer had no reasonable expectation of privacy in his financial documents because they were with a third party, a bank. Rather, the Sixth Circuit suggests that the contents of e-mail in storage are entitled to the same expectation of privacy as the contents of a telephone call,[25] even though the e-mail is with a third party e-mail provider.[26]

[ii]—State Constitutional Protection for Information

Deviating from United States federal law, some states have recognized a right to privacy in personal information under the state constitution.[27]

[b]—Zones of Privacy

The United States Supreme "Court has recognized a guarantee of certain areas or zones of privacy . . . under the [United States] Constitution."[28] The constitutional right of privacy has been extended to

---

[24] United States v. Miller, 425 U.S. 435, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976).

[25] Katz v. United States, 389 U.S. 347, 350, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967).

[26] As new technologies evolve, the constitutional borders on privacy continue to be tested. For example, most state and federal appellate courts that have addressed the issue have held that GPS monitoring is not a "search" and is therefore not subject to the Fourth Amendment's probable cause and warrant requirements. These decisions tend to rely on United States v. Knotts, 460 U.S. 276, 103 S.Ct. 1081, 75 L.Ed.2d 55 (1983), wherein the U.S. Supreme Court held that police did not need a warrant to install a radio transmitter/beeper device on a vehicle to track its whereabouts (apparently for a matter of hours), on the basis that motorists cannot reasonably expect their travels on public roads to be private. In United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010), however, the U.S. Court of Appeals for the District of Columbia Circuit held inadmissible, as a violation of the defendant's Fourth Amendment rights, GPS surveillance obtained without a warrant that tracked his vehicle's movement twenty-four hours a day for twenty-eight days. The court reasoned that "First, unlike one's movements during a single journey, the whole of one's movements over the course of a month is not *actually* exposed to the public because the likelihood anyone will observe all those movements is effectively nil. Second, the whole of one's movements is not exposed *constructively* even though each individual movement is exposed, because that whole reveals more—sometimes a great deal more—than does the sum of its parts." *Id*., 615 F.3d at 558.

[27] § 1.02[4][a] *infra* addresses this topic.

[28] Roe v. Wade, 410 U.S. 113, 152, 93 S.Ct. 705, 35 L.Ed.2d 147 (1973).

activities relating to marriage,[29] procreation,[30] contraception,[31] family relationships,[32] child rearing and education.[33] In certain contexts, these intimate phases of personal life are entitled to the constitutional right of privacy.

For example, in 1965, holding that a state law banning the use of contraceptives was unconstitutional, the Court recognized that the Fourth and Fifth Amendments protect against government invasions of the sanctity of a man's home and the privacies of life. The Court found that marriage is a constitutionally protected zone of privacy.[34]

Subsequent cases extended this constitutional right to privacy with respect to intimate personal matters. In 1969, the Court held that possession of obscene material in a home was not a crime.[35] In 1972, the Court struck as unconstitutional a state statute that prohibited the distribution of contraceptives to unmarried persons.[36] In 1973, the Court held that a woman has a right to privacy in her decision whether or not to terminate a pregnancy, noting, however, that that right is not absolute.[37]

Relying on these cases, later cases established constitutional protection for intimately personal matters such as sexual relations, child rearing and marriage, referring to them as "zones of privacy."[38] Indirectly, these constitutional "zones of privacy" may afford protection of certain information relative to the zone, but they do not necessarily protect the privacy of personal information.

For example, in 2003, the Court held that a state statute prohibiting homosexual relationships violated the right of "adults to engage in the private conduct in the exercise of their liberty under the Due

---

[29] Loving v. Virginia, 388 U.S. 1, 12, 87 S.Ct. 1817, 18 L.Ed.2d 1010 (1967).

[30] Skinner v. Oklahoma, 316 U.S. 535, 541-542, 62 S.Ct. 1110, 86 L.Ed. 1655 (1942).

[31] Eisenstadt v. Baird, 405 U.S. 438, 453-454, 92 S.Ct. 1029, 31 L.Ed.2d 349 (1972).

[32] Prince v. Massachusetts, 321 U.S. 158, 166, 64 S.Ct. 438, 88 L.Ed. 645 (1944).

[33] Pierce v. Society of Sisters, 268 U.S. 510, 535, 45 S.Ct. 571, 69 L.Ed. 1070 (1925); Meyer v. Nebraska, 262 U.S. 390, 399, 43 S.Ct. 625, 67 L.Ed. 1042 (1923).

[34] Griswold v. Connecticut, 381 U.S. 479, 486, 85 S.Ct. 1678, 14 L.Ed.2d 510 (1965).

[35] Stanley v. Georgia, 394 U.S. 557, 564, 89 S.Ct. 1243, 22 L.Ed.2d 542 (1969).

[36] Eisenstadt v. Baird, 405 U.S. 438, 454, 92 S.Ct. 1029, 31 L.Ed.2d 349 (1972).

[37] Roe v. Wade, 410 U.S. 113, 154, 93 S.Ct. 705, 35 L.Ed.2d 147 (1973).

[38] See: Wisconsin v. Yoder, 406 U.S. 205, 92 S.Ct. 1526, 32 L.Ed.2d 15 (1972) (holding Amish parents had right to withhold their children from school, despite law requiring attendance); Loving v. Virginia, 388 U.S. 1, 87 S.Ct. 1817, 18 L.Ed.2d 1010 (1967) (holding unconstitutional state law barring white person from marrying non-white person); Winston v. Lee, 470 U.S. 753, 758, 105 S.Ct. 1611, 84 L.Ed.2d 662 (1985) (holding recovery of evidence by surgery was unreasonable).

Process Clause of the Fourteenth Amendment."[39] Recognizing that the private lives of individuals in this regard entitles them to a constitutionally protected right of privacy, the Court stated:

> "The petitioners are entitled to respect for their private lives. The State cannot demean their existence or control their destiny by making their private sexual conduct a crime. Their right to liberty under the Due Process Clause gives them the full right to engage in their conduct without intervention of the government. 'It is a promise of the Constitution that there is a realm of personal liberty which the government may not enter.'"[40]

Holding that the government may not forbid homosexual relationships by statute, this decision protects from government intrusion the privacy of an individual's sexual orientation.

[3]—Key Federal Court Cases Addressing the Constitutional Right of Privacy

The following table identifies key United States Supreme Court decisions discussing the constitutional right of privacy.

Case	Citation	Significance to privacy rights under the Constitution
Wheaton v. Peters	33 U.S. 591, 8 L.Ed. 1055 (1834)	A "defendant asks nothing—wants nothing, but to be let alone until it can be shown that he has violated the rights of another."
Olmstead v. United States	277 U.S. 438, 48 S.Ct. 564, 72 L.Ed. 944 (1928)	Wiretapping without a warrant was constitutional because there was no physical or tangible intrusion. "One who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside, and that the wires beyond his house, and messages while passing over them, are not within the protection of the Fourth Amendment."
Oklahoma Press Publishing Company v. Walling	327 U.S. 186, 66 S.Ct. 494, 90 L.Ed. 614 (1946)	The Court acknowledged Brandeis's dissent in Olmstead and his ar-gument for the existence and recognition of constitutionally protected privacy rights.

---

[39] Lawrence v. Texas, 539 U.S. 558, 564, 123 S.Ct. 2472, 156 L.Ed.2d 508 (2003).

[40] *Id*., 539 U.S. at 578, quoting Planned Parenthood of Southeastern Pennsylvania v. Casey, 505 U.S. 833, 847, 112 S.Ct. 2791, 120 L.Ed.2d 674 (1992).

Case	Citation	Significance to privacy rights under the Constitution
Silverman v. United States	365 U.S. 505, 81 S.Ct. 679, 5 L.Ed.2d 734 (1961)	Eavesdropping by attaching a listening device to a heat duct of a private home was accomplished by means of an unauthorized physical penetration into the premises occupied by petitioners, which violated their rights under the Fourth Amendment. The Court recognized the right of a man to retreat into his own home and there be free from un-reasonable governmental intrusion. Because the Court held there was a physical intrusion violating the Fourth Amendment, it concluded, "[w]e need not here contemplate the Fourth Amendment implications of . . . other frightening paraphernalia which the vaunted marvels of an electronic age may visit upon human society."
Griswold v. Connecticut	381 U.S. 479, 85 S.Ct. 1678, 14 L.Ed.2d 510 (1965)	Recognizing that the Fourth and Fifth Amendments protect against government invasions of the sanctity of a man's home and privacies of life, the Court held that marriage is a constitutionally protected zone of privacy. Therefore, a state law that banned the use of contraceptives was unconstitutional as violating marital privacy.
Tehan v. Shott	382 U.S. 406, 86 S.Ct. 459, 15 L.Ed.2d 453 (1966)	The Court noted that the federal privilege against self-incrimination reflects the Constitution's concern for the essential values represented by "our respect for the inviolability of the human personality and of the right of each individual 'to a private enclave where he may lead a private life.'"
Stanley v. Georgia	394 U.S. 557, 89 S.Ct. 1243, 22 L.Ed.2d 542 (1969)	In holding a state law criminalizing mere possession of obscene material unconstitutional, the Court stated: "It is now well established that the Constitution protects the right to receive information and ideas . . . regardless of their social worth, and to be generally free from governmental intrusions into one's privacy and control of one's thoughts."
Katz v. United States	389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967)	Attaching a listening and recording device to the outside of a phone booth without a warrant was an unconstitutional invasion of privacy. Overturning Olmstead, the Court held that the Fourth Amendment governs not only the seizure of tangible items but extends as well to the recording of oral statements. A physical intrusion is not required for finding a violation of a legitimate expectation of privacy. The petitioner had manifested a reasonable expectation of privacy in his conversation in a phone booth. Katz established a two-part inquiry for Fourth Amendment analysis: (1) has the indi-vidual manifested a subjective expectation of privacy in the object of the challenged search, and (2) is society willing to recognize that expectation as reasonable?

Case	Citation	Significance to privacy rights under the Constitution
United States v. United States District Court	407 U.S. 297, 92 S.Ct. 2125, 32 L.Ed.2d 752 (1972)	The President's authorization of electronic surveillance in the domestic security arena without judicial approval was held unconstitutional. Balancing government's duty to protect domestic security with the citizen's right to be secure in his privacy against unreasonable government intrusion, the Court emphasized that "broad and unsuspected governmental incursions into conversational privacy which electronic surveillance entails necessitate the application" of constitutional safeguards. In holding that a warrant was required, the Court stated, "by no means of least importance will be the reassurance of the public generally that indiscriminate wiretapping and bugging of law-abiding citizens cannot occur."
Eisenstadt v. Baird	405 U.S. 438, 92 S.Ct. 1029, 31 L.Ed.2d 349 (1972)	State law banning distribution of contraceptives was held unconstitutional. The Court acknowledged the "right of the individual, married or single, to be free from unwarranted government intrusion into matters so fundamentally affecting a person as the decision to bear or beget a child."
Roe v. Wade	410 U.S. 113, 93 S.Ct. 705, 35 L.Ed.2d 147 (1973)	The Court reviewed prior case law concerning constitutionally protected "zones of privacy" involving marriage, child rearing and procreation, and held that a woman has a right to privacy in her decision whether or not to terminate a pregnancy, although that right is not absolute.
United States v. Miller	425 U.S. 435, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976)	A bank depositor had no expectation of privacy in financial information voluntarily conveyed to banks and exposed to their employees in the ordinary course of business.[41]
United States v. New York Telephone Company	434 U.S. 159, 98 S.Ct. 364, 54 L.Ed.2d 376 (1977)	Law enforcement may require a telephone company to transmit pen register information to a remote location. The Court emphasized that pen registers disclosed "neither the purport of the communication, the identities of the parties communicating, nor whether the communication was even completed." Therefore, there was no legitimate expectation of privacy in the information sought.

[41] In response to this decision, Congress passed the Right to Financial Privacy Act of 1978, 18 U.S.C. §§ 3401-3422, providing privacy for financial records of bank customers.

Case	Citation	Significance to privacy rights under the Constitution
Smith v. Maryland	442 U.S. 735, 99 S.Ct. 2577, 61 L.Ed2d 220 (1979)	Following United States v. New York Telephone Company, the Court held there was no constitutionally protected privacy interest in the numbers one dials to initiate a telephone call. Therefore, the installation and use of pen registers to record numbers dialed on a phone was constitutional because, unlike "the listening device employed in Katz . . . pen registers do not acquire the contents of communications." The Court noted that an individual "voluntarily conveys those numbers to the telephone company when he uses the telephone . . . [A] person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."
United States v. Knotts	460 U.S. 276, 103 S.Ct. 1081, 75 L.Ed.2d 55 (1983)	Police use of a radio transmitter/beeper device on a vehicle to track its whereabouts (apparently for a matter of hours) without a warrant was not a violation of the Fourth Amendment because motorists cannot reasonably expect their travels on public roads to be private.
United States v. Karo	468 U.S. 705, 104 S.Ct. 3296, 82 L.Ed.2d 530 (1984)	Police monitoring of a beeper attached to an object brought into a private residence to obtain information that could not have been obtained by observation from outside violates the Fourth Amendment rights of those who have a justifiable interest in the privacy of the residence.
California v. Ciraola	476 U.S. 207, 106 S.Ct. 1809, 90 L.Ed.2d 210 (1986)	The Court held there was no legitimate expectation of privacy of a garden around a home where it was viewable from above. Because the petitioner knowingly exposed his garden to aerial view from the public, police observation of the garden from an aircraft overhead was constitutional.
Dow Chemical v. United States	476 U.S. 227, 106 S.Ct. 1819, 90 L.Ed.2d 226 (1986)	The taking of aerial photographs of an industrial plant complex from navigable airspace is not a search prohibited by the Fourth Amendment. "The government was not employing some unique sensory device not available to the public, but rather was employing a conventional, albeit precise, commercial camera commonly used in mapmaking . . . . The mere fact that human vision is enhanced somewhat, at least to the degree here, does not give rise to constitutional problems."
California v. Greenwood	486 U.S. 35, 108 S.Ct. 1625, 100 L.Ed.2d 30 (1988)	There was no reasonable expectation of privacy in garbage left for collection in a manner accessible to the public outside one's home. Hence, "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of 4th Amendment protection."

Case	Citation	Significance to privacy rights under the Constitution
Kyllo v. United States	533 U.S. 27, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001)	Police use of a thermal imaging device aimed at private house from a public street to sense heat emanating from the house was unconstitutional. "Where the Government uses a device that is not in general public use, to explore details of a private home that would previously have been unknowable without physical intrusion, the surveillance is an unconstitutional invasion of privacy without a warrant . . . . To withdraw protection of this minimum expectation [of privacy] would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment."

The following table identifies key circuit court decisions discussing the constitutional right of privacy.

Case	Citation	Significance to privacy rights under the Constitution
United States v. Arnold	486 F.3d 177 (6th Cir. 2007)	The border search doctrine extends to searches of international passengers at U.S. airports because they are "functional equivalent[s] of a border"; the First Amendment does not require reasonable suspicion to search data, including photographs, residing on a laptop.
United States v. Maynard	615 F.3d 544 (D.C. Cir. 2010)	Police use of GPS surveillance that tracked a vehicle's movement 24 hours a day for 28 days without a warrant violated the Fourth Amendment because the likelihood anyone will observe all those movements is effectively nil, and the whole of one's movements is not exposed constructively even though each individual movement is exposed, because that whole reveals more–sometimes a great deal more–than does the sum of its parts.

[4]—State Constitutions

A number of state constitutions expressly recognize a right to privacy, some worded similarly to the Fourth Amendment to the United States Constitution's right against unreasonable searches and seizures, but others more broadly stated. The following table identifies state constitutional privacy rights:

State	Cite	State Constitutional Right
Alaska	Article I, § 22	Right of Privacy. The right of the people to privacy is recognized and shall not be infringed. The legislature shall implement this section.
Arizona	Article II, § 8	Right to Privacy. No person shall be disturbed in his private affairs, or his home invaded, without authority of law.
California	Article I, § 1	All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty; acquiring, possessing, and protecting property; and pursuing and obtaining safety, happiness, and privacy.
Florida	Article I, § 12	Searches and seizures. The right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures, and against the unreasonable interception of private communications by any means, shall not be violated. No warrant shall be issued except upon probable cause, supported by affidavit, particularly describing the place or places to be searched, the person or persons, thing or things to be seized, the communication to be intercepted, and the nature of evidence to be obtained. This right shall be construed in conformity with the 4th Amendment to the United States Constitution, as interpreted by the United States Supreme Court. Articles or information obtained in violation of this right shall not be admissible in evidence if such articles or information would be inadmissible under decisions of the United States Supreme Court construing the 4th Amendment to the United States Constitution.
	Article I, § 23	Right to Privacy. Every natural person has the right to be let alone and free from governmental intrusion into the person's private life except as otherwise provided herein. This section shall not be construed to limit the public's right of access to public records and meetings as provided by law.

State	Cite	State Constitutional Right
Hawaii	Article I, § 6 Article I, § 7	Right to Privacy. The right of the people to privacy is recognized and shall not be infringed without the showing of a compelling state interest. The legislature shall take affirmative steps to implement this right. Searches, Seizures and Invasion of Privacy. The right of the people to be secure in their persons, houses, papers and effects against unreasonable searches, seizures and invasions of privacy 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 or the communications sought to be intercepted.
Illinois	Article I, § 6 Article I, §§ 6 & 12	Searches, Seizures, Privacy and Interceptions. The people shall have the right to be secure in their persons, houses, papers and other possessions against unreasonable searches, seizures, invasions of privacy or interceptions of communications by eavesdropping devices or other means. No warrant shall issue without probable cause, supported by affidavit particularly describing the place to be searched and the persons or things to be seized. Right To Remedy and Justice. Every person shall find a certain remedy in the laws for all injuries and wrongs which he receives to his person, privacy, property or reputation. He shall obtain justice by law, freely, completely, and promptly.
Louisiana	Article I, § 5	Right to Privacy. Every person shall be secure in his person, property, communications, houses, papers, and effects against unreasonable searches, seizures, or invasions of privacy. No warrant shall issue without probable cause supported by oath or affirmation, and particularly describing the place to be searched, the persons or things to be seized, and the lawful pur-pose or reason for the search. Any person adversely affected by a search or seizure conducted in violation of this Section shall have standing to raise its illegality in the appropriate court.
Montana	Article II, § 10	Right of Privacy. The right of individual privacy is essential to the well-being of a free society and shall not be infringed without the showing of a compelling state interest.

State	Cite	State Constitutional Right
New Jersey	Article 1, ¶ 7	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 warrant shall issue except upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched and the papers and things to be seized.
South Carolina	Article I, § 10	Searches and seizures; invasions of privacy. The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures and unreasonable invasions of privacy 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, the person or thing to be seized, and the information to be obtained.
Washington	Article I, § 7	Invasion of Private Affairs or Home Prohibited. No person shall be disturbed in his private affairs, or his home invaded, without authority of law.

[a]—State Constitutional Protection of Information

It has been held that under the Constitution of the state of New Jersey, individuals have a reasonable expectation of privacy in their Internet service subscriber information.[42] In one case, the New Jersey Supreme Court acknowledged a right to "informational privacy" under the state constitution, but limited it to "subscriber information held by an ISP."[43]

Noting that "[b]oth the Fourth Amendment to the United States Constitution and Article I, Paragraph 7, of the New Jersey Constitution protect, in nearly identical language, 'the right of the people to be secure . . . against unreasonable searches and seizures,'" the court acknowledged that "despite the congruity of the language," the search and seizure protections in the federal and New Jersey State Constitutions "are not always coterminous."[44] For example, whereas the United States Supreme Court refused to suppress bank records obtained

---

[42] State v. Reid, 194 N.J. 386, 945 A.2d 26 (2008).

[43] *Id*., 194 N.J. at 399. The New Jersey Appellate Division had recognized a broader "informational privacy" right under New Jersey's constitution, not necessarily limited to subscriber information held by an ISP, but the New Jersey Supreme Court expressly declined to adopt this broader standard. *Id*. at n.3.

[44] *Id*., 194 N.J. at 396.

via grand jury subpoenas as opposed to a warrant, holding that a customer did not have a Fourth Amendment reasonable expectation of privacy in his bank account records, including his checks, because they were given to a third party, the bank,[45] the New Jersey Supreme Court noted that under New Jersey case law, "although bank customers voluntarily provide information to banks, 'they do so with the understanding that it will remain confidential.'"[46]

The Appellate Court of Illinois has held that the Illinois State Constitution affords individuals a right to privacy in their bank records.[47] A defendant was charged with theft of $40,000 from an Illinois bank where she was an employee and customer. Law enforcement obtained her bank account records without a warrant in connection with the state's investigation. The defendant moved to suppress, arguing that the Illinois Constitution protects an individual's expectation of privacy in her bank records.

The state contended that there is no right to privacy in bank records, arguing that the Illinois Supreme Court applies the search and seizure provisions of the Illinois Constitution consistent with the Fourth Amendment of the United States Constitution, and cited *United States v. Miller*, wherein the United States Supreme Court held that there is no legitimate expectation of privacy in information that a customer has voluntarily conveyed to a bank.[48]

The court found that the Illinois Constitution offers greater privacy protection than the U.S. Constitution, and held that the state's request for a customer's bank records without a warrant or subpoena was an unreasonable intrusion upon the defendant's right to privacy and therefore unconstitutional under the Illinois State Constitution.

---

[45] United States v. Miller, 425 U.S. 435, 443, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976) ("This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.").

[46] State v. Reid, 194 N.J. 386, 398, 945 A.2d 26, 32 (2008), quoting State v. McAllister, 184 N.J. 17, 31, 875 A.2d 866 (2005). "It is well-settled under New Jersey law that disclosure to a third-party provider, as an essential step to obtaining service altogether, does not upend the privacy interest at stake." State v. Reid, 194 N.J. at 399.

[47] People v. Nesbitt, No. 2-09-0976 (Ill. App. Nov. 8, 2010) (holding that "it is clear that the privacy clause of the Illinois Constitution protects an individual's bank records").

[48] See § 1.02[2][a][i] *supra*, for a discussion of *United States v. Miller*.

§ 1.03 Privacy Laws That Impact Access to and Use of Personal Information by the Government

Various federal statutes impact the government's access to and use of personal information. The following table identifies a number of those statutes.[1]

Familiar Name of Statute	Cite
Federal Wiretap Statute	Title 18, Sections 2510-2522 of the United States Code; Title 47, Section 605 of the United States Code
Electronic Communications Privacy Act	Title 18, Sections 2701-2712 of the United States Code
Pen/Trap Statute	Title 18, Sections 3121-3127 of the United States Code
Right to Financial Privacy Act	Title 18, Sections 3401-3422 of the United States Code
Privacy Protection Act	Title 42, Section 2000aa of the United States Code
Foreign Intelligence Surveillance Act	Title 50, Sections 1801-1811 of the United States Code

[1]—Federal Wiretap Statute

[a]—Prohibitions Against the Interception, Use or Disclosure of Oral, Wire and Electronic Communications

Title III of the Omnibus Crime Control and Safe Streets Act of 1968,[1.1] or the Wiretap Statute, prohibits the intentional interception, use or disclosure (whether by the government or private persons) of wire, oral and electronic communications (e.g., eavesdropping) unless a statutory exception applies. "Wire communications" include transfers

(Text continued on page 1-17)

[1] Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (or the Wire Tap Statute) was designed to protect communications from government surveillance. The Electronic Communications Privacy Act of 1986, including the Pen/Trap Statute, amended the Wire Tap Statute and these statutes are discussed below. These laws also regulate private individuals and businesses, in addition to the government.

[1.1] 18 U.S.C. §§ 2510-2522; 47 U.S.C. § 605. The Wiretap Statute was amended and modernized in 1986 to address new methods of communication, such as e-mail, with the enactment of the Electronic Communications Privacy Act. See § 1.03[2] *infra*.

of the human voice by means of a wire, cable or other connection between the sender and recipient.[2] "Electronic communications" include electronic transfers of communications not carried by sound waves, such as e-mail, video teleconferences, and other data transfers, and both wire and wireless transfers.[3]

The statute applies to real-time ("live") electronic surveillance of the content of communications.[4] It is unlawful for any person to "intercept" any such communication[5] or to "use" or "disclose" information knowing that it came from an unlawfully intercepted communication.[6] "Interception" includes the use of "any electronic, mechanical, or other device" to make an "aural acquisition" of the "contents" of the communication.[7]

For example, the Wiretap Statute prohibits wiretapping telephones and installing electronic "sniffers" that read Internet traffic. The statute prohibits providers of electronic communications services from intentionally disclosing the contents of protected communications, such as electronic mail, radio communications, data transmissions, and telephone calls, "to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient," except as otherwise provided by the statute.[8]

[b]—Exceptions

There are various exceptions to Title III's prohibitions on wiretaps. The frequently invoked exceptions are the following:

[i]—18 U.S.C. Section 2518 Court Order or "Wiretap Order"[9]

A wiretap order (or Section 2518 order) is issued by a court.[10] A judge or magistrate must find probable cause, based on an affidavit

---

[2] 18 U.S.C. § 2510(4), (18).

[3] 18 U.S.C. § 2510(12).

[4] The Electronic Communications Privacy Act (ECPA), an extension of the Wiretap Statute, extends protection to electronic and stored communications. Although discussed herein as two separate acts, the provisions of the Wiretap Statute and the ECPA overlap and should be reviewed in concert.

[5] 18 U.S.C. § 2511(1)(a).

[6] 18 U.S.C. § 2511(1)(c) and (d).

[7] 18 U.S.C. § 2510(4).

[8] 18 U.S.C. § 2511(3)(a). See 18 U.S.C. § 2511(3)(b) and § 1.03[1][b] *infra* for exceptions to the foregoing prohibition applicable to providers of electronic communication services *to the public*.

[9] 18 U.S.C. § 2518.

[10] 18 U.S.C. § 2518.

submitted by the government, to believe that the interception will reveal evidence of a predicate felony offense listed in Title 18, Section 2516 of the United States Code.[11] There are a number of predicate offenses enumerated in Section 2516.[12] A Section 2518 order

---

[11] 18 U.S.C. § 2518.

[12] 18 U.S.C. § 2516 lists the predicate offenses for securing a wiretap order. They include, without limitation: any offense relating to the enforcement of the Atomic Energy Act of 1954; sabotage of nuclear facilities or fuel; espionage; kidnapping; protection of trade secrets; sabotage; treason; riots; malicious mischief; destruction of vessels; piracy; restrictions on payments and loans to labor organizations; murder; kidnapping; robbery; extortion; bribery of public officials and witnesses; bribery of bank officials; bribery in sporting contests; unlawful use of explosives; concealment of assets; transmission of wagering information; influencing or injuring an officer, juror or witness; obstruction of criminal investigations; obstruction of state or local law enforcement; sex trafficking of children by force, fraud or coercion; Presidential and Presidential staff assassination, kidnapping and assault; interference with commerce by threats or violence; interstate and foreign travel or transportation in aid of racketeering enterprises; use of interstate commerce facilities in the commission of murder for hire; violent crimes in aid of racketeering activity; offer, acceptance or solicitation to influence operations of employee benefit plan; prohibition of business enterprises of gambling, laundering of monetary instruments; engaging in monetary transactions in property derived from specified unlawful activity; theft from interstate shipment; embezzlement from pension and welfare funds; fraud by wire, radio or television; bank fraud; sexual exploitation of children; selling or buying of children; material constituting or containing child pornography; child obscenity; production of sexually explicit depictions of a minor for importation into the United States; transportation for illegal sexual activity and related crimes; interstate transportation of stolen property; trafficking in certain motor vehicles or motor vehicle parts; hostage taking; fraud and related activity in connection with access devices; witness relocation and assistance; destruction of aircraft or aircraft facilities; aircraft parts fraud; violations with respect to racketeer influenced and corrupt organizations; threatening or retaliating against a federal official; mail fraud; computer fraud and abuse; congressional, Cabinet or Supreme Court assassinations, kidnapping and assault; prohibited transactions involving nuclear materials; destruction of motor vehicles or motor vehicle facilities; biological weapons; wrecking trains; production of false identification documentation; procurement of citizenship or nationalization unlawfully; reproduction of naturalization or citizenship papers; sale of naturalization or citizenship papers; passport issuance without authority; false statements in passport applications; forgery or false use of passports; misuse of passports; fraud and misuse of visas, permits and other documents; counterfeiting; fraud connected with a case under Title 11 of the United States Code or the manufacture, importation, receiving, concealment, buying, selling or otherwise dealing in narcotic drugs, marihuana or other dangerous drugs; extortionate credit transactions; interception and disclosure of certain communications and use of certain intercepting devices; obscenity; destruction of a natural gas pipeline; aircraft piracy; any criminal violation of the Arms Export Control Act; a violation of the Immigration and Nationality Act relating to the smuggling of aliens; production of false identification documents; false statements in passport applications; fraud and misuse of visas, permits and other documents; any criminal violation relating to chemical weapons; terrorism; or conspiracy to commit any offense described above.

may *only* be issued when one of the predicate felony offenses enumerated in Section 2516 is shown.[13]

Title 18, Section 2518 of the United States Code sets out specific grounds upon which a court order authorizing a wiretap may be granted. A judge may enter an *ex parte* order authorizing interception of wire, oral or electronic communications within the jurisdiction of the court in which the judge is sitting (and outside that jurisdiction but within the United States in the case of a mobile interception device authorized by a federal court[14]), if the judge determines, based on the facts submitted by the applicant, that:

(a) there is probable cause that an individual is committing, has committed or is about to commit one of the offenses enumerated in Title 18, Section 2516 of the United States Code;
(b) there is probable cause that particular communications concerning that offense will be obtained through such interception;
(c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous; and
(d) except as provided in Section 2518(11),[15] "there is probable cause that the facilities from which, or the place where, the wire, oral or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person."[16]

Each Section 2518 order shall specify:

"(a) the identity of the person, if known, whose communications are to be intercepted;
"(b) the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted;[17]

---

[13] The USA Patriot Act temporarily added terrorism and computer crimes to the predicate offense list. USA Patriot Act, Pub. L. No. 107-56, 115 Stat. 272, §§ 201, 202, 224 (2001).

[14] 18 U.S.C. § 2518(3).

[15] 18 U.S.C. § 2518(11) allows for a "roving" wiretap of wire or electronic communications in certain instances. See § 1.03[1][b][A] *infra*.

[16] 18 U.S.C. § 2518(3).

[17] The order need not specify the nature and location of the communications facility if the application for the Section 2518 order is made by a federal officer and is

"(c) a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates;

"(d) the identity of the agency authorized to intercept the communications, and of the person authorizing the application; and

"(e) the period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained."[18]

Under emergency circumstances that involve (1) immediate danger of death or serious physical injury to any person; (2) conspiratorial activities threatening the national security interest, or (3) conspiratorial activities characteristic of organized crime, any investigative or law enforcement officer may intercept a wire, oral or electronic communication if an application for a Section 2518 order is made within forty-eight (48) hours *after* the interception has occurred, or begins to occur.[19]

[A]—Roving Wiretap

A "roving" wiretap (also called a "multipoint" tap) refers to an order that may not name a specific telephone line or Internet account that is to be tapped. Instead of specifying the communications facility (e.g., the telephone provider or Internet Service Provider), the order will identify the suspect person and the communications that are to be intercepted.[20] A roving wiretap may be used to intercept communications of a suspect person who switches telecommunications providers or accounts in an effort to thwart law enforcement.

[B]—Modify or Quash Subpoena

A provider of wire or electronic communications services that has received a Section 2518 order as provided for in Section 2518 (11)(b)

---

approved by the Attorney General or a representative thereof, it is not practical to specify such nature and location, and the person committing the offense and the communications that are to be intercepted are identified. If the wiretap concerns a wire or electronic communication (as opposed to an oral communication), there must be "probable cause to believe that the [suspect] person's actions could have the effect of thwarting interception from a specified facility." 18 U.S.C. § 2518(11).

[18] 18 U.S.C. § 2518(4).

[19] 18 U.S.C. § 2518(7).

[20] 18 U.S.C. § 2518(11).

may seek to have the court "modify or quash the order on the ground that its assistance with respect to the interception cannot be performed in a timely or reasonable fashion."[21]

[C]—Emergency Situations[22]

An investigative or law enforcement officer may, without a court order, intercept a wire, oral or electronic communication if (1) an application for an order approving the interception is made within forty-eight hours after the interception has occurred; and (2) the officer reasonably believes that "an emergency situation exists that involves—

"(1) immediate danger of death or serious physical injury to any person,

"(2) conspiratorial activities threatening the national security interest, or

"(3) conspiratorial activities characteristic of organized crime" requiring interception of the communication before an order authorizing such interception can, with due diligence, be obtained, and there are grounds upon which an order could be entered.[23]

[ii]—Consent[24]

A person may intercept a wire, oral or electronic communication if that person is a party to the communication or one of the parties to the communication has given prior consent to such interception, "unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State."[25]

A provider of an electronic communication service to the public may divulge the contents of such communication "with the lawful consent of the originator or any addressee or intended recipient of such communication."[26]

[iii]—Inadvertently Obtained Criminal Evidence[27]

A person or entity providing electronic communication services *to the public* may disclose the contents of any such communications that

---

[21] 18 U.S.C. § 2518(12).
[22] 18 U.S.C. § 2518(7).
[23] 18 U.S.C. § 2518(7).
[24] 18 U.S.C. § 2511(2)(c)-(d).
[25] 18 U.S.C. § 2511(2)(c)-(d).
[26] 18 U.S.C. § 2511(3)(b)(ii).
[27] 18 U.S.C. § 2511(3)(b)(iv).

"were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency."[28]

[iv]—Subcontractor[29]

The provider of an electronic communication service to the public may disclose the contents of any such communication "to a person employed or authorized, or whose facilities are used, to forward such communication to its destination."[30] A company that maintains a Web site offering e-mail or other electronic message services may therefore pass on the contents of such message to its hosting provider or telecommunications provider for transmittal to the intended recipient of the message.

[v]—Service Provider[31]

The "service provider exception" was added by the Electronic Communications Privacy Act, which extended the Wiretap Statute to include the interception of electronic communications, including e-mail. Under the "service provider exception," an employee of a provider of wire or electronic communications services may intercept, disclose or use such communication "in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks."[32]

An employer may monitor its employees' communications if the "interception device" is used by the employer in the ordinary course of business. A common example is where an employer monitors its employees' telephone conversations to evaluate business-related matters such as efficiency, productivity and client service. In one case,[33] an employee alleged that his employer was improperly monitoring his private conversations. The district court acknowledged that the monitoring was done for quality control purposes. The court also noted

---

[28] 18 U.S.C. § 2511(3)(b)(iv).
[29] 18 U.S.C. § 2511(3)(b)(iii).
[30] 18 U.S.C. § 2511(3)(b)(iii).
[31] 18 U.S.C. § 2511(2)(a)(i).
[32] 18 U.S.C. § 2511(2)(a)(i). See also, 18 U.S.C. § 2511(3)(b)(i).
[33] Simmons v. Southwestern Bell Telephone Co., 452 F. Supp. 392 (W.D. Okla. 1978).

that the employer provided a separate non-monitored phone line for personal calls. The court concluded that the company's monitoring activities were reasonable and done in the ordinary course of business, and thus protected under Section 2511(2)(a)(i).[34]

The "service provider exemption" has been used to permit an employer to access its employees' e-mail files. One court rejected privacy claims under the Electronic Communications Privacy Act (ECPA) raised by two police officers.[35] In that case, the plaintiff police officer sent messages to other members of the police department through the department's "Alphapage" messaging system. Faced with an internal affairs investigation based on the contents of those messages, the plaintiff and another officer filed suit, claiming that the police department's access to and retrieval of the months-old messages violated, among other things, the Federal Wiretap Statute. The court found that the city was a "service provider" as defined under the ECPA, and was "free to access the stored message as it pleased."[36] The court therefore held that the city had not violated the ECPA.

[vi]—Computer Trespasser[37]

A person may intercept a computer trespasser's wire or electronic communications transmitted to, through or from a computer, if (1) the owner or operator of the computer authorized the interception of the computer trespasser's communications using that computer; (2) the person intercepting such communications is lawfully engaged in an investigation; (3) the person intercepting such communications has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation; and (4) such interception does not acquire communications other than those transmitted to or from the computer trespasser.[38]

[vii]—Extension Telephone[39]

A person may intercept a wire or electronic communication if such communication is made using "any telephone or telegraph instrument, equipment or facility, or any component thereof":

---

[34] *Id*., 452 F. Supp. at 396.
[35] Bohach v. City of Reno, 932 F. Supp. 1232 (D. Nev. 1996).
[36] *Id*., 932 F. Supp. at 1237.
[37] 18 U.S.C. § 2511(2)(i) (USA Patriot Act § 217).
[38] 18 U.S.C. § 2511(2)(i).
[39] 18 U.S.C. § 2510(5)(a).

(1) furnished to the subscriber or user by a provider of wire or electronic communication services in the ordinary course of its business and such equipment is used by the subscriber or user in the ordinary course of its business;

(2) furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or

(3) being used by a provider of wire or electronic communication services in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties.[40]

A person may intercept an oral communication using "a hearing aid or similar device being used to correct subnormal hearing to not better than normal."[41]

[viii]—Accessible to the Public[42]

A person may "intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public."[43] A person may also intercept, among certain other transmissions, any radio communication transmitted for general public use or that otherwise relates to distress calls or public safety announcements, or that are transmitted on frequencies allocated for amateur, citizens band, general mobile radio services or for marine or aeronautical communications systems.[44]

[ix]—FISA Electronic Surveillance[45]

Providers of a wire or electronic communication service may provide "information, facilities, or technical assistance to persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance, as defined in [Title 50, Sections 1801 *et seq*. of the United States Code] of the Foreign Intelligence Surveillance Act of 1978." The provider must have received the following: (1) a court order directing such assistance signed by the

---

[40] 18 U.S.C. § 2510(5)(a)(i)-(ii).
[41] 18 U.S.C. § 2510(5)(b).
[42] 18 U.S.C. § 2511(2)(g)(i).
[43] 18 U.S.C. § 2511(2)(g)(i).
[44] 18 U.S.C. § 2511(2)(g)(ii).
[45] 18 U.S.C. § 2511(2)(a)(ii).

authorizing judge, or (2) a certification in writing by an "investigative or law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State"[46] or "the Attorney General of the United States that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required."[47]

The court order or certification must set "forth the period of time during which the provision of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required."[48] The provider shall not "disclose the existence of any interception or surveillance or the device used to accomplish the interception or surveillance with respect to which the person has been furnished a court order or certification under this chapter, except as may otherwise be required by legal process and then only after prior notification to the Attorney General or to the principal prosecuting attorney of a State or any political subdivision of a State, as may be appropriate."[49]

The provider may be subject to liability for civil damages arising from any disclosure in violation of the Wiretap Statute.[50] No action may be maintained against the provider for its compliance with the Wiretap Statute.[51]

[c]—Remedies for Violations of the Wiretap Statute

The Wiretap Statute allows for a private cause of action.[52] The Wiretap Statute permits a person aggrieved by violation of the statute to recover "such relief as may be appropriate" in a civil action, other than from the United States.[53] "Appropriate relief" includes (1) preliminary and other equitable or declaratory relief; (2) punitive damages in appropriate cases; (3) reasonable attorneys' fees and litigation costs; and (4) damages in the amount of (A) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or (B) statutory damages equal to the greater of $100 a day for each day of violation or $10,000.[54] A civil

---

[46] 18 U.S.C. § 2518 (7). See also, 18 U.S.C. § 2511(2)(a)(ii)(A) and (B).
[47] 18 U.S.C. § 2511(2)(a)(ii)(B).
[48] 18 U.S.C. § 2511(2)(a)(ii).
[49] 18 U.S.C. § 2511(2)(a)(ii).
[50] 18 U.S.C. § 2511(2)(a)(ii).
[51] 18 U.S.C. § 2511(2)(a)(ii).
[52] 18 U.S.C. § 2520(a).
[53] 18 U.S.C. § 2520(a).
[54] 18 U.S.C. § 2520(b)-(c).

action "may not be commenced later than two years after the date upon which the claimant first has a reasonable opportunity to discover the violation."[55]

A good faith reliance on any of the following is a complete defense against any civil or criminal action brought under the Wiretap Statute or any other law:

(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization;[56]

(2) a request of an investigative or law enforcement officer under Title 18, Section 2518(7) of the United States Code (wiretap by an officer in an emergency situation);[57] or

(3) a good faith determination that Section 2511(3)[58] or Section 2511(2)(i) (computer trespasser exception) permitted the conduct complained of.[59]

[d]—State Wiretap Statutes

Most state wiretap statutes are similar in scope to the Federal Wiretap Statute. Like Title III, most state statutes protect "wire, oral and electronic communications." Some afford greater protection to certain communications.

Several states require the consent of *all* parties to a conversation. These states require a warrant for a wiretap unless all parties consent. By contrast, the federal Wiretap Statute permits surveillance of a conversation if *any* party to it consents. States that require the consent of all parties include the following:

---

[55] 18 U.S.C. § 2520(e).
[56] 18 U.S.C. § 2520(d)(1).
[57] 18 U.S.C. § 2520(d)(2).
[58] 18 U.S.C. § 2511(3) includes the following exceptions:

(1) service provider exception (18 U.S.C. § 2511(2)(a)(i));
(2) FISA electronic surveillance exception (18 U.S.C. § 2511(2)(a)(ii));
(3) consent exception (18 U.S.C. § 2511(3)(b)(ii));
(4) subcontractor exception (18 U.S.C. § 2511(3)(b)(iii)); and
(5) inadvertently obtained criminal evidence exception (18 U.S.C. § 2511(3)(b)(iv)).

[59] 18 U.S.C. § 2520(d)(3).

State	Statute
California	Cal. Penal Code §§ 630 *et seq*.
Connecticut	Conn. Gen. Stat. Ann. § 52-570d
Florida	Fla. Stat. Ann. §§ 934.01 to 934.03
Illinois	Ill. Ann. Comp. Stat., Ch. 720, §§ 5/14-1, 5/14-2
Maryland	Md. Code Ann. § 10-402
Massachusetts	Mass. Gen. L. Ann., Ch. 272, § 99
Montana	Mont. Code Ann. § 45-8-213
Nevada	Nev. Rev. Stat. §§ 200.610 to 200.620
New Hampshire	N.H. Rev. Stat. Ann. §§ 570-A:1-A:2
Pennsylvania	18 Pa. Consol. Stat. §§ 5701 et seq.
Washington	Wash. Rev. Code § 9.73.030

[2]—Electronic Communications Privacy Act

The Electronic Communications Privacy Act of 1986[60] (ECPA) is an amendment to and extension of the original Wiretap Statute. It amended the Wiretap Statute to include the interception of electronic communications, which include wireless and wired transmissions, such as e-mail.[61] Title I of the ECPA protects wire, oral and electronic

(Text continued on page 1-27)

[60] 18 U.S.C. §§ 2510-2522 (Title I—"Wire and Electronic Communications Interception and Interception of Oral Communications"); 18 U.S.C. §§ 2701-2712 (Title II—"Stored Wire and Electronic Communications and Transactional Records Access").

[61] The ECPA added the definition of "electronic communication" at 18 U.S.C. § 2510(12), and modified other definitions to bring the Wiretap Statute more current with modern methods of electronic communications.

communications while in transit.[61.1] The ECPA also extended protection to *stored* communications by prohibiting the unauthorized access to information concerning communications *in electronic storage,* notably the content of e-mail and voice messages and the customer information pertaining thereto. Title II of the ECPA pertains to stored electronic communications and is sometimes referred to as the Stored Communications Act[61.2] (SCA). The ECPA prohibits the access to and disclosure of electronic communications and stored communications, except as authorized by statute.[62]

[a]—Internet Service Providers and Other Online Providers

The ECPA imposes disclosure restrictions on Internet Service Providers (ISPs) and other online service providers by prohibiting such providers of an "electronic communication service" and providers of a "remote computing service," in each case *to the public,* from *knowingly* disclosing the contents of such stored communications, or the record or other information pertaining to a customer of such service, except as expressly permitted by the statute.[63] The ECPA thus creates certain statutory privacy rights for customers and subscribers of computer network service providers (e.g., with regard to the customer's stored e-mail, account records, and subscriber information). A service provider may not disclose such information unless such disclosure falls within a statutory exception.

[i]—"Electronic Communication Service" and "Remote Computing Service"

The term "remote computing service" is defined as "the provision to the public of computer storage or processing services by means of an electronic communications system"[64] and includes online computing services, such as electronic bulletin boards, that may be accessed remotely via the Internet.[65] Although undefined in the statute, the term "electronic communication service" has been interpreted to

---

[61.1] 18 U.S.C. §§ 2510-2522.

[61.2] 18 U.S.C. §§ 2701-2712.

[62] See the exceptions to such access and disclosure set out in the Wiretap Statute at § 1.03[1][b] *supra.*

[63] 18 U.S.C. § 2702(a).

[64] 18 U.S.C. § 2711(2).

[65] Steve Jackson Games, Inc. v. United States Secret Service, 816 F. Supp. 432, 443 (W.D. Tex. 1993) (holding that provider of bulletin board services was a remote computing service).

mean a service that facilitates the exchange of communications, such as e-mail, via electronic means, such as through the Internet.[66] Together, these terms encompass virtually all conceivable means of transmitting and receiving communications electronically, through the Internet, for example, and via other modes of transmission, such as via wireless and mobile communications.

[ii]—To the Public

The disclosure restrictions imposed by the ECPA pertain to service providers that furnish an electronic communication service or remote computing service to the public.[67] They do not pertain to entities that provide such services in a private, or non-public, context, such as employers that may provide an electronic communication service such as e-mail to their employees.

[iii]—Exceptions

[A]—Stored Contents

A service provider may disclose the *contents* of a stored communication:

(1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;[68]

(2) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;[69]

(3) to a person employed or authorized or whose facilities are used to forward such communication to its destination;[70]

(4) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;[71]

(5) to a law enforcement agency:

(A) if the contents

(i) were inadvertently obtained by the service provider; and

(ii) appear to pertain to the commission of a crime.[72]

---

[66] FTC v. Netscape Communications Corp., 196 F.R.D. 559, 560 (N.D. Cal. 2000) (noting that Netscape, a provider of e-mail accounts through netscape.net, is a provider of an electronic communication service).

[67] See 18 U.S.C. § 2702(a)(3).

[68] 18 U.S.C. § 2702(b)(1).

[69] 18 U.S.C. § 2702(b)(3); 18 U.S.C. § 2511(3)(b)(ii).

[70] 18 U.S.C. § 2702(b)(4).

[71] 18 U.S.C. § 2702(b)(5).

[72] 18 U.S.C. § 2702(b)(7).

(6) to a federal, state or local governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.[73]

[B]—Customer Records

A service provider may disclose the *record* or other information (e.g., account logs, contact information) pertaining to a customer of such service (not including the *contents* of communications):

(1) as authorized in Title 18, Section 2703 of the United States Code (required disclosure of customer communications or records to the government[74]);

(2) with the lawful consent of the customer;

(3) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(4) to a governmental entity, if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information; or

(5) to any person other than a governmental entity.[75]

[b]—Warrants, Subpoenas, Orders: 18 U.S.C. Section 2703

[i]—Stored Contents

The government may obtain the contents of a wire or electronic communication:

(1) in electronic storage for 180 days or fewer from a provider of an *electronic communication service*—only pursuant to a federal or state issued warrant.[76] The warrant must be served in accordance with the Federal Rules of Criminal Procedure or equivalent state procedures.

(2) in electronic storage for more than 180 days from a provider of an *electronic communication service*—pursuant to (i) a federal or state issued warrant, *without* required notice to the subscriber or

---

[73] 18 U.S.C. § 2702(b).
[74] See § 1.03[3][b] *infra*.
[75] 18 U.S.C. § 2702(c).
[76] 18 U.S.C. § 2703(a).

customer; (ii) an administrative subpoena authorized by a federal or state statute or a federal or state grand jury or trial subpoena, *with* notice to the customer; or (iii) an ECPA Section 2703(d) court order, *with* notice to the customer.[77] Notice to the customer may be delayed for up to ninety days if set out in the subpoena or court order.[78]

(3) in electronic storage from a provider of a *remote computing service*—pursuant to (i) a federal or state issued warrant, *without* required notice to the customer; (ii) an administrative subpoena authorized by a federal or state statute or a federal or state grand jury or trial subpoena, *with* notice to the customer; or (iii) an ECPA Section 2703(d) court order, *with* notice to the customer.[79] Notice to the customer may be delayed for up to ninety days if set out in the subpoena or court order.[80] The communication must be stored on the service (a) on behalf of a customer of such remote computing service, and (b) solely for the purpose of providing storage or computer processing services to such customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

[ii]—Customer Records

The government may obtain the *records* or other information pertaining to a customer[81] of an electronic communication service or a remote computing service (not including the contents of communications), *without* notice to the customer, pursuant to the following:

(1) a federal or state issued warrant;[82]
(2) an ECPA Section 2703(d) court order;[83]
(3) the consent of the customer;[84] or

---

[77] 18 U.S.C. § 2703(b).

[78] 18 U.S.C. § 2705. Notice may be delayed up to 90 days, which such delay will be set out in the court order or subpoena. Extensions (of up to 90 days each) may be granted by court order. 18 U.S.C. § 2705(a)(5).

[79] 18 U.S.C. § 2703(b).

[80] 18 U.S.C. § 2705.

[81] The ECPA requires the provider to disclose the following information about the customer: (A) name; (B) address; (C) local and long-distance telephone connection records, or records of session times and durations; (D) length of service (including start date) and types of service used; (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and (F) means and source of payment for such service (including any credit card or bank account number). 18 U.S.C. § 2703(c)(2).

[82] 18 U.S.C. § 2703(c)(1)(A).

[83] 18 U.S.C. § 2703(c)(1)(B).

[84] 18 U.S.C. § 2703(c)(1)(C).

(4) a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address and place of business of a customer engaged in telemarketing.[85]

[iii]—ECPA Section 2703(d) Court Order

An ECPA Section 2703(d) court order may be issued by a court of competent jurisdiction only if the governmental entity seeking such order offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.[86] The service provider upon which such order is served may apply to the court issuing the order to quash or modify the order, "if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider."[87]

[iv]—Delayed Notice to Customer

With respect to a court order or an administrative subpoena, the court or supervisory official, respectively, may indicate in such order or subpoena that the customer not be notified of the order for a period of up to ninety days,[88] if there is reason to believe that that notification of the existence of the order or subpoena may:

- endanger the life or physical safety of an individual;
- lead the person under investigation to flee from prosecution;
- lead to the destruction of or tampering with evidence;
- cause intimidation of potential witnesses; or
- otherwise seriously jeopardize an investigation or unduly delay a trial.[89]

The delay of notification may be extended for additional ninety-day periods.[90] Notice shall be provided by the government to the customer upon expiration of the ninety-day period and any extensions thereof.[91]

---

[85] 18 U.S.C. § 2703(c)(1)(D).
[86] 18 U.S.C. § 2703(d).
[87] 18 U.S.C. § 2703(d).
[88] 18 U.S.C. § 2705(a)(1)(A).
[89] 18 U.S.C. § 2705(a)(2).
[90] 18 U.S.C. § 2705(a)(4).
[91] 18 U.S.C. § 2705(a)(5).

The government may secure a court order directing "a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order."[92]

[v]—Customer Challenge

The customer may challenge the government's subpoena or order by filing a motion to quash the subpoena or vacate the order within fourteen days after notice from the government.[93] Copies of the motion must be served upon the government, with written notice to the service provider.[94]

[c]—Preservation of Evidence

Upon the request of a governmental entity, which may be made informally in writing or orally, a provider of wire or electronic communication services or a remote computing service "shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process."[95] The provider shall retain the records for ninety days.[96] This period may be extended for an additional ninety days at the request of the governmental entity.[97]

A subpoena or court order may also require a provider to create a backup of the contents of electronic communications to preserve them.[98] The provider shall make such a backup within two (2) days after receipt of the subpoena or court order, without notifying the customer, and confirm to the government that such backup has been made.[99] The government must notify the customer within three (3) days of receipt of such confirmation, unless notice is delayed pursuant to Title 18, Section 2705(a) of the United States Code.[100] If the government seeks the information by using a warrant issued by a court having jurisdiction over the offense under investigation, and pursuant to the Federal Rules of Criminal Procedure or the equivalent

---

[92] 18 U.S.C. § 2705(b).
[93] 18 U.S.C. § 2704(b)(1).
[94] 18 U.S.C. § 2704(b)(1).
[95] 18 U.S.C. § 2703(f)(1).
[96] 18 U.S.C. § 2703(f)(2).
[97] 18 U.S.C. § 2703(f)(2).
[98] 18 U.S.C. § 2704(a)(1).
[99] 18 U.S.C. § 2704(a)(1).
[100] 18 U.S.C. § 2704(a)(2).

state warrant requirements, the government may acquire such information without providing the required notice to the customer.[101]

[d]—Release of Backup Copy

The provider must retain the backup until the later of delivery of it to the government, or the resolution of any proceedings concerning the government's subpoena or order.[102] The provider shall release the backup copy to the government no sooner than fourteen days after the government's notice to the customer, unless the provider has received notice from the customer challenging the government's request or if the provider has initiated proceedings to challenge the government's request.[103]

[e]—Civil Remedies

The ECPA allows for a private cause of action.[104] So long as the violator acted knowingly or intentionally as to the violation, a person aggrieved by a violation of the ECPA may, in a civil action, recover from the violator (other than the United States):

(1) such preliminary and other equitable or declaratory relief as may be appropriate;

(2) actual damages suffered and any profits made by the violator as a result of the violation (but in no case shall a person entitled to recover receive less than $1,000); if the violation is willful or intentional, the court may assess punitive damages; and

(3) reasonable attorneys' fees and other litigation costs reasonably incurred.[105]

[f]—Limitation on Civil Actions

No civil action may be "commenced later than two years after the date upon which the claimant first discovered or had a reasonable opportunity to discover the violation."[106]

[g]—Defenses

A good faith reliance on any of the following is a complete defense to any civil or criminal action brought under the ECPA or any other law:

---

[101] 18 U.S.C. § 2703(b)(1).
[102] 18 U.S.C. § 2704(a)(3).
[103] 18 U.S.C. § 2704(a)(4). See § 1.03[2][b][iv] *supra*.
[104] 18 U.S.C. § 2707.
[105] 18 U.S.C. § 2707(a) and (b).
[106] 18 U.S.C. § 2707(f).

(1) a court warrant or order, a grand jury subpoena, a legislative authorization or a statutory authorization (such as a request from the government under Title 18, Section 2703(f) of the United States Code to preserve records and other evidence pending issuance of a court order[107]);

(2) a request of an investigative or law enforcement officer under Title 18, Section 2518(7) of the United States Code[108] or

(3) a good faith determination that Title 18, Section 2511(3) of the United States Code permitted the conduct complained of.[109]

[h]—Punishment for Unauthorized Access

Anyone who intentionally accesses without authorization any stored electronic communication, and thereby obtains, alters or prevents authorized access to such communication while it is in electronic storage, shall be punished as follows:

"(1) if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or any State—

"(A) a fine . . . or imprisonment for not more than 5 years, or both, in the case of a first offense . . . ; and

"(B) a fine under this title or imprisonment for not more than 10 years, or both, for any subsequent offense . . . .; and

"(2) in any other case:

(A) a fine . . . or imprisonment for not more than 1 year, or both, in the case of a first offense . . . ; and

"(B) a fine . . . or imprisonment for not more than 5 years,

---

[107] 18 U.S.C. § 2707(e)(1). See also, 18 U.S.C. § 2703(e). The USA Patriot Act added a new defense to civil or criminal liability under the ECPA for providers who preserve stored data at the request of a law enforcement official pursuant to 18 U.S.C. § 2703(f).

[108] 18 U.S.C. § 2707(e)(2). Title 18, Section 2518(7) of the United States Code permits an investigative or law enforcement officer to request, in an emergency situation, before an order authorizing interception can, with due diligence, be obtained, that a wire, oral or electronic communication be intercepted.

[109] 18 U.S.C. § 2707(e)(3). Title 18, Section 2511(3) of the United States Code permits the provider of an electronic communication service to the public to divulge the contents of such communication under certain circumstances. See § 1.03[1][b][ii], [iii], and [iv] *supra*. See Davis v. Gracey, 111 F.3d 1472, 1484 (10th Cir. 1997) (applying good faith defense because seizure of stored communications incidental to a valid search was objectively reasonable).

or both, in the case of an offense . . . that occurs after a conviction of another offense . . . ."[110]

[i]—Exceptions

Punishment shall not apply to:

(1) the "person or entity providing a wire or electronic communications service;"[111]

(2) "a user of that service with respect to a communication of or intended for that user;"[112] or

(3) anyone complying with Title18, Section 2703 (required disclosure by warrant, court order or subpoena), Section 2704 (back-up preservation of records) or Section 2518 (court order for interception of a wire, oral or electronic communication) of the United States Code.[113]

[3]—Pen/Trap Statute

The pen register and trap and trace device statute[114] was enacted by Congress in 1986 in connection with the ECPA and prohibits the unauthorized use of a pen register or a trap and trace device, except as permitted by the statute. A pen register captures outgoing addressing information (e.g., a phone number dialed, e-mail "to" and "from" header information). A trap and trace device captures incoming addressing information (e.g., caller ID information, e-mail "to" and "from" header information). Neither captures the *content* of the communication. A device that captures outgoing and incoming addressing information is sometimes referred to as a pen/trap device.

[a]—Exceptions

The Pen/Trap Statute does not apply to the use of devices by a provider of electronic or wire communication service:

"(1) relating to the operation, maintenance and testing of a wire or electronic communication service or to the protection of the rights or property of such provider, or to the protection of users of that service from abuse of service or unlawful use of service; or

---

[110] 18 U.S.C. § 2701(b).
[111] 18 U.S.C. § 2701(c)(1).
[112] 18 U.S.C. § 2701(c)(2).
[113] 18 U.S.C. § 2701(c)(3).
[114] 18 U.S.C. §§ 3121-3127.

"(2) to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire communication, or a user of that service, from fraudulent, unlawful or abusive use of service; or

"(3) where the consent of the user of that service has been obtained."[115]

[b]—Orders

A pen/trap order is issued by a court, based upon a certification by the government that "the information likely to be obtained is relevant to an ongoing criminal investigation."[116] An order must indicate:

(1) the identity, if known, of the person whose name is listed for the telephone number, e-mail account, or other facility to which the pen register or trap and trace device is to be attached or applied;

(2) the identity, if known, of the person who is the subject of the criminal investigation;

(3) the attributes of the communications to which the order applies, including the number or other identifier and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied, and, in the case of an order authorizing installation and use of a trap and trace device a state (as opposed to federal) investigative or law enforcement officer, the geographic limits of the order; and

(4) a statement of the offense to which the information likely to be obtained by the pen register or trap and trace device relates.[117]

[c]—Cooperation and Secrecy

Upon request of the applicant, the order shall direct the service provider to furnish "information, facilities, and technical assistance necessary to accomplish the installation of the pen register or trap and

---

[115] 18 U.S.C. § 3121(b).

[116] 18 U.S.C. §§ 3122(b)(2), 3123. This differs from the standard for a Title III wiretap order, which is based on a finding of the court. In Smith v. Maryland, 442 U.S. 735, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979), the U.S. Supreme Court upheld the constitutionality of the use of pen registers, holding that the use of a pen register is not an invasion of privacy. Although the Court in *Smith* upheld the constitutionality of the use of a pen register without a warrant, 18 U.S.C. § 3123 (of the 1986 Pen/Trap Statute) now requires a court order, based upon a law enforcement officer's declaration that the information is relevant to an ongoing investigation, before a pen register may be used.

[117] 18 U.S.C. § 3123(b)(1).

trace device."[118] The order shall direct that the provider "not disclose the existence of the pen register or trap and trace device or the existence of the investigation to the listed subscriber, or to any other person, unless or until otherwise ordered by the court."[119]

(Text continued on page 1-37)

---

[118] 18 U.S.C. § 3123(b)(2).
[119] 18 U.S.C. § 3123(d).

[d]—Roving Order

An order need not specify all of the providers subject to the order, although it must specify the initial provider ("roving" order). Instead, the order "shall apply to any person or entity providing wire or electronic communication service in the United States whose assistance may facilitate the execution of the order," even if the provider is not named in the order.[120] When the order is served upon a provider not specifically named in the order, at the provider's request, law enforcement must furnish "written or electronic certification" that the order applies to the provider.[121]

[e]—Emergency Situations

In emergency situations, the government may require a provider of a wire or electronic service to install and cooperate with a pen/trap device in the absence of a court order. An investigative or law enforcement officer "may have installed and use a pen register or trap and trace device if, within forty-eight hours after the installation has occurred, or begins to occur, an order approving the installation or use is issued in accordance with [Title 18, Section 3123 of the United States Code]" if he or she "reasonably determines that:

> "(1) an emergency situation exists that involves—
>
> "(A) immediate danger of death or serious bodily injury to any person;
>
> "(B) conspiratorial activities characteristic of organized crime;
>
> "(C) an immediate threat to a national security interest; or
>
> "(D) an ongoing attack on a protected computer (as defined in [Title 18, Section 1030 of the United States Code])[122] that constitutes a crime punishable by a term of imprisonment greater than one year;

---

[120] 18 U.S.C. § 3123(a)(1). See also, § 1.03[1][b][i][A] *supra*.

[121] 18 U.S.C. § 3123(a)(1). The statutory requirement that law enforcement clarify whether an order pertains to a particular provider was added by the USA Patriot Act § 216.

[122] A "protected computer" is a computer (1) used exclusively by "a financial institution or the United States Government"; (2) used non-exclusively by "a financial institution or the United States Government" where the "conduct constituting the offense affects that use"; or (3) used "in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States." 18 U.S.C. § 1030(e)(2).

that requires the installation and use of a pen register or a trap and trace device before an order authorizing such installation and use can, with due diligence, be obtained, and

"(2) there are grounds upon which an order could be entered under this chapter to authorize such installation and use."[123]

If no order is issued, use of the pen/trap device shall "immediately terminate when the information sought is obtained, when the application for the order is denied or when forty-eight hours have lapsed since the installation of the pen register or trap and trace device, whichever is earlier."[124] The provider who furnished facilities or technical assistance "shall be reasonably compensated for such reasonable expenses incurred in providing such facilities and assistance."[125]

[f]—Defenses

The Pen/Trap Statute provides that "No cause of action shall lie in any court against any provider of a wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with a court order under this chapter or request pursuant to [Title 18, Section 3125 of the United States Code (emergency installation)]."[126] A good faith reliance on a court order, a request pursuant to Section 3125, a legislative authorization, or a statutory authorization is a complete defense against any civil or criminal action brought under the Pen/Trap Statute or any other law.[127]

[4]—Right to Financial Privacy Act

The Right to Financial Privacy Act (RFPA)[128] prohibits any agency or department of the United States government from access to the financial records of any customer of a financial institution, except when:

(1) The release of the records is authorized by the customer;[129] or

(2) The release of the records is pursuant to:

---

[123] 18 U.S.C. § 3125(a).
[124] 18 U.S.C. § 3125(b).
[125] 18 U.S.C. § 3125(d).
[126] 18 U.S.C. § 3124(d).
[127] 18 U.S.C. § 3124(e).
[128] 12 U.S.C. §§ 3401-3422.
[129] 12 U.S.C. § 3402(1).

(A) An administrative subpoena or summons;[130]

(B) A search warrant;[131]

(C) A judicial subpoena;[132] or

(D) A formal written request by the government, provided that:

(i) "there is reason to believe that the records sought are relevant to a legitimate law enforcement inquiry";[133]

(ii) "no administrative summons or subpoena authority reasonably appears to be available to [the government]";[134]

(iii) "the request is authorized by regulations promulgated by the head of the agency or department";[135] and

(iv) the government has notified the customer of the request, unless a court order directs that such notice may be delayed,[136] and the customer has not filed an application to enjoin the government within ten days of his or her receipt of such notice or within fourteen days from the date of mailing of such notice.[137]

---

[130] 12 U.S.C. § 3402(2). The administrative subpoena or summons must meet the requirements of 12 U.S.C. § 3405, and a copy must be served on the customer with notice of the investigation on or before the date the subpoena was served on the financial institution (12 U.S.C. § 3405(2)), unless a court order directs that such notice to the customer may be delayed. 12 U.S.C. § 3409. The customer may, within ten days of his or her receipt of such notice, file a motion to quash. 12 U.S.C. § 3405(3).

[131] 12 U.S.C. § 3402(3). The search warrant must meet the requirements of 12 U.S.C. § 3406, and the government must mail to the customer a copy of the search warrant within ninety days after serving the warrant on the financial institution (12 U.S.C. § 3406(b)), unless a court order directs that such notice may be delayed. 12 U.S.C. §§ 3406(c), 3409.

[132] 12 U.S.C. § 3402(4). The judicial subpoena must meet the requirements of 12 U.S.C. § 3407, and a copy must be served on the customer with notice of the investigation on or before the date the subpoena was served on the financial institution (12 U.S.C. § 3407(2)), unless a court order directs that such notice to the customer may be delayed. 12 U.S.C. §§ 3409, 3407(2). The customer may, within ten days of his or her receipt of such notice, file a motion to quash. 12 U.S.C. § 3405(3).

[133] 12 U.S.C. § 3402(5); 12 U.S.C. § 3408(2).

[134] 12 U.S.C. § 3408(1).

[135] 12 U.S.C. § 3408(2).

[136] The written request must meet the requirements of 12 U.S.C. § 3408, and a copy of the request must be served upon the customer or mailed to his or her last know address with notice of the investigation on or before the date on which the request was made to the financial institution (12 U.S.C. § 3408(4)(A)), unless a court order directs that such notice to the customer may be delayed. 12 U.S.C. § 3409.

[137] 12 U.S.C. § 3408(4)(B).

A financial institution shall not release financial records until the government certifies in writing that it has complied with the RFPA.[138]

[a]—Financial Institution

A "financial institution" is "any office of a bank, savings bank, card issuer as defined in [Title 15, Section 1602(n) of the United States Code], industrial loan company, trust company, savings association, building and loan, or homestead association (including cooperative banks), credit union, or consumer finance institution, located in any State or territory of the United States, the District of Columbia, Puerto Rico, Guam, American Samoa, or the Virgin Islands."[139]

[b]—Financial Record

The term "financial record" is broadly defined and refers to any information derived from "any record held by a financial institution pertaining to a customer's relationship with the financial institution."[140]

[c]—Access for Intelligence and Protective Purposes

RFPA restrictions on the release of financial records to the government do not apply to government requests pertaining to counterintelligence and protective functions:

> "Nothing in [the RFPA] shall apply to the production and disclosure of financial records pursuant to requests from—
>
> "(A) a Government authority authorized to conduct foreign counter- or foreign positive-intelligence activities for purposes of conducting such activities;
>
> "(B) the Secret Service for the purpose of conducting its protective functions (18 U.S.C. 3056; 3 U.S.C. 202, Public Law 90-331, as amended); or
>
> "(C) a Government authority authorized to conduct investigations of, or intelligence or counterintelligence analyses related to, international terrorism for the purpose of conducting such investigations or analyses."[141]

The financial institution shall not release any records until it receives written certification from the government that it has complied

---

[138] 12 U.S.C. § 3403(b).
[139] 12 U.S.C. § 3401(1).
[140] 12 U.S.C. § 3401(2).
[141] 12 U.S.C. § 3414(a)(1).

with the applicable provisions of the RFPA.[142]

[d]—Delay in, Restrictions on Notifying Customer

The government may apply to the court for an order delaying its giving notice to the customer for up to ninety days (which may be renewed for ninety-day intervals).[143] The order shall also direct the financial institution to delay notice to the customer that records have been obtained or that a request for records has been made, for up to ninety days (which may be renewed for ninety-day intervals).[144]

A financial institution shall not notify anyone of a government request for financial records made pursuant to a National Security Letter or otherwise for intelligence and protective purposes (e.g., concerning counterintelligence activities related to terrorism).[145] A financial institution shall not notify anyone named in a grand jury subpoena in connection with an investigation of certain controlled substances laws.[146]

The notice requirements of the RFPA do not apply to a legitimate law enforcement inquiry that seeks only the name, address, account number and type of account of a customer or ascertainable group of customers associated with "a financial transaction or class of financial transactions" or "a foreign country or subdivision thereof in the case of a Government authority exercising financial controls over foreign accounts in the United States under [Appendix 50, Section 5(b) of the United States Code (of the Trading with the Enemy Act)], the International Emergency Economic Powers Act [Title 50, Sections 1701 *et seq*. of the United States Code]; or [Title 22, Section 287c of the United States Code, economic and communication sanctions pursuant to United Nations Security Council Resolution]."[147]

Additional exceptions to RFPA's requirements are set out in Title 12, Section 3413 of the United States Code.

---

[142] 12 U.S.C. §§ 3414(a)(2), 3403(b).

[143] 12 U.S.C. § 3409. With regard to the service of a warrant, the government may apply to the court for an order delaying its giving notice to the customer, and directing as well the service provider not to notify the customer that records have been obtained by the government pursuant to the warrant, for up to 180 days (which may be renewed for ninety-day intervals). 12 U.S.C. § 3406(c).

[144] 12 U.S.C. § 3409(b).

[145] 12 U.S.C. § 3414(a)(3), (5)(D).

[146] 12 U.S.C. § 3420(b)(1).

[147] 12 U.S.C. § 3413(g).

[e]—Customer Objections

A customer may object to the disclosure of his or her financial records to the government by filing "a sworn statement and a motion to quash in an appropriate court" within ten days of service of the notice (with a copy of the subpoena or summons) on the customer.[148]

[f]—Voluntary Disclosure

A financial institution may notify the government if it believes it has "information which may be relevant to a possible violation of any statute or regulation."[149] Such information should include only the name or other identifying information about the suspected individual, corporation or account, and the nature of any suspected illegal activity.[150] Such disclosure shall not subject the financial institution to liability "to the customer under any law or regulation of the United States or any constitution, law, or regulation of any State or political subdivision thereof."[151]

[g]—Defenses

A financial institution shall not be subject to liability under the RFPA, "the constitution of any State, or any law or regulation of any State or any political subdivision of any State," for any disclosure of financial records pursuant to the RFPA, if made in good-faith reliance:

(1) upon a certificate by any government authority; or

(2) pursuant to Title 12, Section 3413(l) of the United States Code relating to disclosures by a financial institution having reason to believe that there is a possible crime against a financial institution by insiders.[152]

[5]—Privacy Protection Act

The Privacy Protection Act[153] prohibits a government officer or employee, in connection with the investigation or prosecution of a

---

[148] 12 U.S.C. § 3405(3) (administrative subpoena and summons); 12 U.S.C. § 3407(3) (judicial subpoena).

[149] 12 U.S.C. § 3403(c).

[150] 12 U.S.C. § 3403(c).

[151] 12 U.S.C. § 3403(c).

[152] 12 U.S.C. § 3417(c).

[153] 42 U.S.C. § 2000aa.

criminal offense, from searching for or seizing "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."[154] This prohibition shall not apply if:

(1) "there is probable cause to believe that the person possessing such materials has committed or is committing the criminal offense to which the materials relate";[155] or

(2) "there is reason to believe that the immediate seizure of such materials is necessary to prevent the death of, or serious bodily injury to, a human being."[156]

Similarly, the act prohibits a government officer or employee, in connection with the investigation or prosecution of a criminal offense, from searching for or seizing "documentary materials, other than work product materials, possessed by a person in connection with a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication, in or affecting interstate or foreign commerce."[157] In addition to the two exceptions indicated in (1) and (2) above, this prohibition shall not apply if:

(1) "there is reason to believe that the giving of notice pursuant to a subpoena duces tecum would result in the destruction, alteration, or concealment of such materials"[158]; or

(2) "such materials have not been produced in response to a court order directing compliance with a subpoena duces tecum, and (i) all appellate remedies have been exhausted; or (ii) there is reason to believe that the delay in an investigation or trial occasioned by further proceedings relating to the subpoena would threaten the interests of justice."[159]

---

[154] 42 U.S.C. § 2000aa(a).

[155] 42 U.S.C. § 2000aa(a)(1). The act excludes from this exception instances in which "the offense to which the materials relate consists of the receipt, possession, communication, or withholding of such materials or the information contained therein." The act then gives a number of exceptions to this exception to the initial exception. See 42 U.S.C. § 2000aa(a)(1).

[156] 42 U.S.C. § 2000aa(a)(2).

[157] 42 U.S.C. § 2000aa(b).

[158] 42 U.S.C. § 2000aa(b)(3).

[159] 42 U.S.C. § 2000aa(b)(4). Where a search warrant is sought pursuant to 42 U.S.C. § 2000aa(b)(4)(B), "the person possessing the materials shall be afforded adequate opportunity to submit an affidavit setting forth the basis for any contention that the materials sought are not subject to seizure." 42 U.S.C. § 2000aa(c).

[6]—Foreign Intelligence Surveillance Act

The Foreign Intelligence Surveillance Act of 1978 (FISA)[160] addresses the government's authority to conduct electronic surveillance to acquire "foreign intelligence information" from a "foreign power," an "agent of a foreign power," and, under certain circumstances, a "United States person." "Foreign intelligence information" refers to:

> "(1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against:
>
> "(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
>
> "(B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or
>
> "(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
>
> "(2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to:
>
> "(A) the national defense or the security of the United States; or
>
> "(B) the conduct of the foreign affairs of the United States."[161]

[a]—Scope of Intelligence Gathering

Under FISA, intelligence gathering is limited to surveillance of a "foreign power," an "agent of a foreign power," and a "United States person." A "foreign power" refers to:

> "(1) a foreign government or any component thereof, whether or not recognized by the United States;
>
> "(2) a faction of a foreign nation or nations, not substantially composed of United States persons;
>
> "(3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;
>
> "(4) a group engaged in international terrorism or activities in preparation therefor;

---

[160] 50 U.S.C. §§ 1801-1811.

[161] 50 U.S.C. §§ 1801(e).

"(5) a foreign-based political organization, not substantially composed of United States persons; or

"(6) an entity that is directed and controlled by a foreign government or governments."[162]

An "agent of a foreign power" refers to any person (other than a United States person) who, among other things:

(1) "acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, . . . knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities";[163]

(2) "knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power" or knowingly aids or abets any person, or knowingly conspires with any person to engage, in such activities;[164]

(3) "knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power."[165]

"United States person" refers to "a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in [Title 8, Section 1101(a)(20) of the United States Code]), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States."[166]

Applications to undertake electronic surveillance are made by a federal officer and must be approved by the Attorney General of the United States or the Deputy Attorney General.[167] For obvious reasons, applications are made *ex parte,* without notice to the target suspect as to whom such surveillance is to be taken. To grant such an *ex parte* order, the special court must find, among other things, probable cause that:

---

[162] 50 U.S.C. §§ 1801(a).
[163] 50 U.S.C. §§ 1801(b).
[164] 50 U.S.C. §§ 1801(b)(2)(C) and (E).
[165] 50 U.S.C. §§ 1801(b)(2)(D).
[166] 50 U.S.C. §§ 1801(i).
[167] 50 U.S.C. §§ 1804(a).

"(A) the target suspect of the electronic surveillance is a foreign power or an agent of a foreign power . . .;[168] and

"(B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power."[169]

[b]—Business Records/Tangible Things

FISA permits the government to, pursuant to court order, require the production of certain "tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities."[170] No one shall disclose to anyone else (other than those persons necessary to produce the tangible things) "that the Federal Bureau of Investigation has sought or obtained tangible things under this section."[171]

[c]—FISA Orders

The Foreign Intelligence Surveillance Act establishes a special court to hear applications for and grant orders approving electronic surveillance.[172] FISA also establishes a special appeals court to review the denial of any application made under FISA.[173] Denials by the appeals court may be petitioned for a writ of *certiorari* to the United States Supreme Court, with the record transmitted under seal.[174]

The Attorney General of the United States or his designee may authorize surveillance in emergency situations, so long as an application for an order is made to the FISA court within seventy-two hours of such authorization.[175]

---

[168] No United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the First Amendment to the Constitution of the United States. 50 U.S.C. § 1805(a)(3)(A).

[169] 50 U.S.C. § 1805(a)(3)(B).

[170] 50 U.S.C. § 1861(a). The USA Patriot Act expanded the items subject to government seizure from the more narrowly defined "business records" to "tangible items." Pub. L. No. 107-56, 115 Stat. 272, § 215 (2001).

[171] 50 U.S.C. § 1861(d).

[172] 50 U.S.C. § 1803(a).

[173] 50 U.S.C. § 1803(b).

[174] 50 U.S.C. § 1803(b).

[175] 50 U.S.C. § 1805(f).

The President of the United States, through the Attorney General of the United States, may authorize electronic surveillance *without* a court order if, among other things, the electronic surveillance is solely directed at:

> (1) the acquisition of (a) the contents of communications exclusively among foreign powers, or (b) technical intelligence from property or premises under the open and exclusive control of a foreign power; and
>
> (2) "there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party."[176]

A FISA order shall specify:

> "(1) the identity, if known, or a description of the target of the electronic surveillance;
>
> "(2) the nature and location of each of the facilities or places at which the electronic surveillance will be directed, if known;
>
> "(3) the type of information sought to be acquired and the type of communications or activities to be subjected to the surveillance;
>
> "(4) the means by which the electronic surveillance will be effected and whether physical entry will be used to effect the surveillance;
>
> "(5) the period of time during which the electronic surveillance is approved; and
>
> "(6) whenever more than one electronic, mechanical, or other surveillance device is to be used under the order, the authorized coverage of the devices involved and what minimization procedures shall apply to information subject to acquisition by each device."[177]

The person served (e.g., a telecommunications or other common carrier, landlord, custodian) with the FISA order must, to the extent set forth in the order, comply with the order in a manner that will protect the secrecy of the electronic surveillance so as to avoid the target's thwarting the government's surveillance efforts, and shall maintain under security any records concerning the surveillance.[178]

---

[176] 50 U.S.C. § 1802(a)(1).
[177] 50 U.S.C. § 1805(c)(1).
[178] 50 U.S.C. § 1805(c)(2).

FISA provides immunity from third party claims for any person who furnishes information or assistance in compliance with a FISA order or a request for emergency assistance.[179]

[d]—Civil Remedies

FISA allows for a private cause of action.[180] An aggrieved person (other than a foreign power or an agent of a foreign power) who has been the subject of an electronic surveillance or about whom information obtained by electronic surveillance has been disclosed or used in violation of Title 50, Section 1809 of the United States Code, may commence an action against any person who committed such violation.[181] Such aggrieved person may recover: "(a) actual damages, but not less than liquidated damages of $1,000 or $100 per day for each day of violation, whichever is greater; (b) punitive damages; and (c) reasonable attorney's fees and other investigation and litigation costs reasonably incurred."[182]

---

[179] 50 U.S.C. § 1805(i).
[180] 50 U.S.C. § 1810.
[181] 50 U.S.C. § 1810.
[182] 50 U.S.C. § 1810.

§ 1.04 USA Patriot Act

In response to the September 11, 2001 terrorist attacks, Congress passed legislation entitled "The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act" (more commonly referred to as the "USA Patriot Act").[1] The USA Patriot Act is a culmination of a number of amendments to existing statutes, and is intended to give law enforcement greater authority to track and intercept communications, both for criminal investigation and for foreign surveillance. For example, it extends law enforcement surveillance powers to include the monitoring of e-mail, the Internet and cellular communications. It also allows for information to be shared more easily in that information may be exchanged between state and federal authorities as well as agencies. The act also affects businesses that provide financial and communication services. The act requires these types of businesses to disclose data, under a government order, to law enforcement officials to assist in their investigations. In certain contexts, the act grants immunity from third party liability to these companies that disclose such information under government orders.[2]

The USA Patriot Act is not a "stand-alone" statute, but instead amends many other substantive statutes. These amendments have since been incorporated into the respective statutes.[3] Accordingly, the underlying statutes are to be consulted.

The following charts identify and note the impact of certain provisions of Title II of the USA Patriot Act. These provisions exemplify amendments by the USA Patriot Act. The act addresses many additional amendments not discussed here.[4]

[1]—Sunset Provision

Title II of the USA Patriot Act contained a sunset provision that stated that sixteen of the provisions of the act were to expire on

---

[1] Pub. L. No. 107-56, 115 Stat. 272 (2001), available at http://thomas.loc.gov/bss/d107/d107laws.html (last visited Aug. 8, 2006).

[2] Pub. L. No. 107-56, § 225, 115 Stat. 272 (2001).

[3] For example, the USA Patriot Act temporarily added computer crimes (Pub. L. No. 107-56, §§ 202, 224, 115 Stat. 272 (2001)) and terrorism (Pub. L. No. 107-56, §§ 201(2), 224) to the Wiretap Statute predicate offense list, amending the Wiretap Statute at 18 U.S.C. § 2516(1)(c) and 18 U.S.C. § 2516(1)(q), respectively.

[4] For example, Title III amends financial laws that require financial institutions to provide the government with suspicious activity reports (SARs), and requires financial institutions to communicate more openly with the federal government regarding customers.

December 31, 2005, unless extended.[5] That deadline was extended to March 10, 2006[6] to allow time for Congress to consider reauthorizing the temporary provisions to make them permanent. A new act was signed into law on March 9, 2006, and is called the USA Patriot Improvement and Reauthorization Act of 2005.[7] This act made fourteen out of sixteen of these provisions permanent. The other two provisions (Sections 206 and 215 of the USA Patriot Act under Title II), were not made permanent and were scheduled to expire December 31, 2005, but have been extended several times.[8]

USA Patriot Act Section	Statute amended	Relevance of provision
206 ("Roving John Doe wiretap")	50 U.S.C. § 1805(c)(2)(B) FISA	Broadens surveillance authority under the Foreign Intelligence Surveillance Act (FISA). Failure to specify the location of a target or the device to be monitored does not prevent law enforcement from obtaining a wiretap order. Instead, law enforcement officials may obtain a roving wiretap order without identifying the specifics, which allows them to conduct broader surveillance. Law enforcement may use the order to monitor their targets at multiple places and to monitor multiple devices being used.
215	50 U.S.C. § 1861 FISA	Expands FISA access to tangible items under FISA. Before this amendment, FISA permitted the FBI to have access to "business records" of hotels, motels, car and truck rental agencies, and storage rental facilities. Now FISA permits the FBI to obtain "tangible items" and not just business records from any type of business or organization. Also prevents third parties who disclose such information from providing notification to the customer about such disclosure. Grants immunity from liability to third parties for disclosing such information to the government.

[5] Pub. L. No. 107-56, § 224, 115 Stat. 272 (2001). Perhaps more controversial in nature, only Title II of the USA Patriot Act contains a sunset provision. The provisions under the other titles are permanent.

[6] H.R. 3199, 109th Cong., 1st Sess. (2005), available at http://thomas.loc.gov/bss/109search.html (last visited Aug. 8, 2006).

[7] Pub. L. No. 109-177, 120 Stat. 192 (2006). The act was initiated in 2005, but signed into law on March 9, 2006.

[8] Sections 206 and 215 of the USA Patriot Act were to expire December 31, 2005, but were extended until December 31, 2009. In late 2009, these provisions were extended a second time, until February 28, 2010. On February 27, 2010, they were extended a third time, until February 28, 2011, and extended again on May 25, 2011.

[2]—Permanent Provisions

Title II of the USA Patriot Act also lists provisions that are permanent.[9] The following provisions were originally set to expire December 31, 2005, but were made permanent by the USA Patriot Improvement and Reauthorization Act of 2005:

USA Patriot Act Section	Statute amended	Relevance of provision
201	18 U.S.C. § 2516(1) Wiretap Statute	Expands law enforcement's use of wiretapping in criminal investigations. The predicate offenses where wiretapping is permitted now include terrorism and the production or dissemination of chemical weapons.
202	18 U.S.C. § 2516(1)(c) Wiretap Statute	Permits law enforcement to intercept oral, wire and electronic communications in cases involving computer fraud and abuse against the government. Allows a federal wiretap to be obtained and used on individuals suspected of illegally obtaining information from government computers for use in terrorist activities.
203(b)	18 U.S.C. § 2517 Wiretap Statute	Expands sharing of wiretap information in criminal investigations. Law enforcement officials or attorneys for the government may disclose contents of any wire, oral or electronic communication dealing with foreign intelligence or counterintelligence information to any other federal law enforcement, intelligence, immigration, national defense or national security official to assist that official in the performance of his or her duties.
203(d)	18 U.S.C. § 2517 Wiretap Statute	Permits sharing of foreign intelligence or counterintelligence information obtained as part of a criminal investigation to be disclosed to any federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to assist the official as necessary in his or her duties.
204	18 U.S.C. § 2511(2)(f) Wiretap Statute (indirectly implicates FISA)	Allows law enforcement officials under FISA to obtain search warrants to intercept wire, oral and electronic communications. Communications permitted to be intercepted now include voicemail messages.

[9] Pub. L. No. 107-56, § 224, 115 Stat. 272 (2001).

USA Patriot Act Section	Statute amended	Relevance of provision
207	50 U.S.C. §§ 1805(e)(1), 1805(d)(2), 1824(d)(1) FISA	Extends duration of surveillance under FISA of non-United States persons who are foreign agents from forty-five days to ninety days. In addition, law enforcement may receive an extension of an existing court order to conduct surveillance on a foreign agent for up to one year.
209	18 U.S.C. §§ 2510, 2703 Wiretap Statute and ECPA	Allows government to obtain voicemail messages pursuant to a search warrant by amending the definition of wire communication under Title 18, Section 2510 of the United States Code to remove electronically stored communication from the definition of wire communication. Previously, government had to secure a wiretap order (Title 18, Section 2518 of the United States Code). Also amends Title 18, Section 2703 of the United States Code to require communication providers to disclose wire and electronically stored communication to law enforcement pursuant to a search warrant. Before the amendment, communication providers were required to provide only stored communication of customers to law enforcement pursuant to a search warrant.
212	18 U.S.C. §§ 2702, 2703 ECPA	Voluntary Disclosure—Allows communication providers such as Internet service providers to disclose information about a customer to the FBI in light of a potential emergency involving serious danger to any person. Required Disclosure—Requires communication providers to disclose the contents of any wire or electronic communication when directed by the government under a warrant.
214	50 U.S.C. §§ 1842, 1843 FISA	A pen register/trap and trace order under FISA may be used with U.S. citizens as well as foreign agents. Government officials can obtain a pen register/trap and trace order to investigate U.S. citizens if this assists in preventing international terrorism or clandestine intelligence activities.

USA Patriot Act Section	Statute amended	Relevance of provision
217	18 U.S.C. §§ 2510, 2511(2) Wiretap Statute	Allows law enforcement to intercept communications of a computer trespasser using a protected computer. Communications transmitted to or from the computer trespasser may be intercepted if (1) there are reasonable grounds to believe the communications are relevant to an investigation; (2) the owner of the protected computer provides consent; (3) the person intercepting the communications is lawfully engaged in an investigation; and (4) the interception does not acquire communications other than those transmitted to or from the computer trespasser.
218	50 U.S.C. §§ 1804(a)(7)(B), 1823(a)(7)(B) FISA	Broadens the use of a wiretap order under FISA. Instead of requiring that law enforcement demonstrate that the primary purpose of the order is for intelligence reasons, they need only prove that intelligence is a significant purpose for the order.
220	18 U.S.C. §§ 2703, 2711 ECPA	Allows a court-ordered search warrant for electronic communications to have nationwide application. Allows a search warrant for electronic communications obtained in one jurisdiction to be used in other jurisdictions.
223	18 U.S.C. §§ 2520, 2707 ECPA, Wiretap Statute	Provides civil liability and administrative discipline for violations of the Electronic Communications Privacy Act (ECPA) and the Wiretap Statute.
225	50 U.S.C. § 1805 FISA	Provides immunity to anyone who discloses information to the government under a FISA wiretap order.

The other permanent provisions in Title II of the USA Patriot Act are:

USA Patriot Act Section	Statute amended	Subject of provision
203(a)	Fed. R. Crim. Proc. 6(e)(3)(C), (D) FRCP	Deliberations in grand jury proceedings are usually kept secret. Amends Federal Rules of Criminal Procedure Rule 6(e)(3)(C) to permit disclosure of grand jury information in certain instances as set forth below: (1) when ordered by a court in connection with a judicial proceeding; (2) when ordered by a court at the request of a defendant upon a showing that grounds may exist for a motion to dismiss the indictment; (3) when the disclosure is made by an attorney for the government to another federal grand jury; (4) disclosure may be made by a court order when an attorney for the government has evidence that matters disclosed may reveal a violation of state criminal law. In this situation, the attorney for the government may disclose such information to the appropriate state official for the purpose of enforcing such law; (5) when the matters involve foreign intelligence or counterintelligence, or foreign intelligence information, to any federal law enforcement, intelligence, protective, immigration, national defense or national security official in order to assist the official receiving that information in the performance of his official duties.
203(c)	18 U.S.C. § 2517 Wiretap Statute	Directs the Attorney General to establish procedures for the disclosures allowed in USA Patriot Act §§ 203(a) and 203(b).
205	28 U.S.C. § 532	Authorizes the Director of the FBI to expedite the employment of personnel as translators to support counterterrorism investigations and operations without regard to applicable federal personnel requirements and limitations. The Director of the FBI shall establish security requirements for the personnel employed as translators.

USA Patriot Act Section	Statute amended	Subject of provision
208	50 U.S.C. § 1803(a) FISA	Expands the number of judges on the FISA court from seven to eleven, three of whom shall reside within twenty miles of the District of Columbia.
210	18 U.S.C. § 2703(c)(2) ECPA	Expands the scope of information that subpoenas may elicit from communication service providers. A subpoena may require a communication service provider to disclose a customer's source of payment, such as a credit card or bank account number. A subpoena may require disclosure of the customer's telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address. Before this amendment, 18 U.S.C. § 2703(c)(2) primarily required communication providers to disclose the name, address, telephone billing records, and length of service of a customer.
211	47 U.S.C. § 551 Cable Communications Policy Act of 1984	Allows a cable operator to disclose to the government personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber as authorized by the Wiretap Statute, ECPA, and Pen/Trap Statute.
213	18 U.S.C. § 3103a FRCP	Allows law enforcement to delay notice of a search warrant under certain circumstances.
216	18 U.S.C. §§ 3121(c), 3123, 3127(1)-(4) Pen/Trap Statute	Expands the permissible use of pen register/trap and trace devices. Amends statute to permit use of pen register/trap and trace devices to obtain the source and destination of electronic communications in addition to telephone calls. Also allows law enforcement to obtain permission from one court to use a pen register/trap and trace device anywhere within the United States.
219	FED. R. CRIM. PROC. 41(a) FRCP	Establishes nationwide application of search warrants to obtain evidence in matters involving domestic or international terrorism.

USA Patriot Act Section	Statute amended	Subject of provision
221	22 U.S.C. § 7210 Trade Sanctions Reform and Export Enhancement Act of 2000	Clarifies that the Trade Sanctions Reform and Export Enhancement Act of 2000 should not affect the provisions of the USA Patriot Act. Specifically, the Trade Sanctions Reform and Export Enhancement Act of 2000 shall not limit the criminal or civil punishments authorized under the USA Patriot Act for violations of antiterrorism laws. For example, the Trade Sanctions Reform and Export Enhancement Act of 2000 will not protect the unlawful export of any agricultural commodity, medicine, or medical device to a foreign terrorist organization or any foreign group that is involved with weapons of mass destruction or missile proliferation. Instead, these unlawful exports will be subject to criminal or civil penalties.
222	18 U.S.C. § 3124(c) Pen/Trap Statute	Indicates that anyone who assists law enforcement in executing a pen register/trap and trace device order shall be reimbursed for such expenditures incurred with providing such assistance.

[3]—Challenges to the USA Patriot Act

The USA Patriot Act has faced criticism in terms of its permitting the government to obtain and access information in counteracting terrorism. The following table identifies notable constitutional challenges to the USA Patriot Act:

Case	Challenge	Holding
Mayfield v. United States, 504 F. Supp.2d 1023 (D. Ore. 2007)	Plaintiffs challenged the USA Patriot Act amendments to FISA that allow federal agents to circumvent Fourth Amendment probable cause requirements when investigating persons suspected of crimes, and alleged a violation of the Fourth Amendment when the Federal Bureau of Investigation (FBI) wiretapped plaintiff and his family after he was suspected of involvement in the 2004 Madrid train bombings.	The district court held that 50 U.S.C. §§ 1804 and 1823 of FISA, as amended by the Patriot Act, are unconstitutional because they violate the Fourth Amendment.
Doe v. Ashcroft, 334 F. Supp.2d 471 (S.D.N.Y. 2004); Doe v. Gonzales, 386 F. Supp.2d 66 (D. Conn. 2005) Doe v. Gonzales, 500 F. Supp.2d 379 (S.D.N.Y. 2007) Doe v. Mukasey, 549 F.3d 861 (2d Cir. 2008)	Plaintiffs challenged the constitutionality of 18 U.S.C. § 2709, as amended by the USA Patriot Act, which authorizes the FBI to compel communications firms, such as Internet service providers (ISPs) or telephone companies, to produce certain customer records if the FBI certifies that those records are "relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities." The FBI's demands under § 2709 are issued by national security letters (NSLs), a unique form of administrative subpoena made in secrecy and pertaining to national security issues; the statute bars the recipient of an NSL from disclosing that the FBI issued the NSL.	The district court held that 18 U.S.C. § 2709 violated the Fourth Amendment insofar as it permits compulsory, secret and unreviewable production of information, and that the non-disclosure provision of 18 U.S.C. § 2709(c) violates the First Amendment. While an appeal of that decision was pending, Congress passed the USA Patriot Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat. 192 (March 9, 2006), altering § 2709 and adding several new procedures codified at 18 U.S.C. § 3511, which now govern judicial review of NSLs. The Second Circuit vacated and remanded. On remand, the district court held that 18 U.S.C. §§ 2709(c) and 3511(b) as amended by the Reauthorization Act violated the First Amendment. On appeal, the Second Circuit affirmed in part and reversed in part, holding 18 U.S.C. §§ 2709(c) and 3511(b)

§ 1.05 Other Federal Privacy Statutes

Other statutes affect the access to and use of personal information in specific contexts. These statutes limit access to and use of personal information by others generally, and are not limited to access and use by the government. Certain of the following statutes are discussed in more detail in other chapters of this book.

Statute	Cite
Fair Credit Reporting Act of 1970	15 U.S.C. § 1681a-v
Health Insurance Portability and Accountability Act of 1996	42 U.S.C. §§ 1301 *et seq*.
The Financial Modernization Act of 1999 (Gramm-Leach-Bliley Act)	15 U.S.C. §§ 6801-6809, §§ 6821-6827
Computer Fraud and Abuse Act of 1986	18 U.S.C. § 1030
Cable Communications Policy Act of 1984	47 U.S.C. § 551
Telecommunications Privacy Act of 1996	47 U.S.C. § 222
Family Educational Rights and Privacy Act of 1974	20 U.S.C. § 1232g
Video Privacy Protection Act of 1988	18 U.S.C. § 2710
Employee Polygraph Protection Act of 1988	29 U.S.C. § 2001
Telephone Consumer Protection Act of 1991	47 U.S.C. § 227

[1]—Fair Credit Reporting Act

The Fair Credit Reporting Act (FCRA)[1] addresses the use and disclosure of an individual's credit report information. FCRA generally prohibits the disclosure of "consumer report" information except as expressly authorized by that statute.[2]

---

[1] 15 U.S.C. §§ 1681, 1681a-1681v. See generally, § 3.12A and Ch. 3 *infra*.

[2] See 15 U.S.C. § 1681e. See Privacy of Consumer Financial Information; Final Rule, 65 Fed. Reg. 33,646 (2000) (FCRA "provides no limitation on communication by an entity solely of its own 'transactions or experiences' with the consumer (e.g., the individual's account history). However, it limits the reporting of information obtained from other sources, such as consumer application information or credit report information."). FCRA excludes from the definition of "consumer report" information concerning "transactions or experiences between the consumer and the person making the report." 15 U.S.C. § 1681a(d)(2)(A)(i). 15 U.S.C. § 1681b sets out those circumstances under which, and persons to whom, a consumer report may be disclosed, and includes, for example, to a person whom a credit reporting agency has reason to believe.

A consumer reporting agency may provide a consumer report to the government pursuant to a court order or a subpoena issued in connection with federal grand jury proceedings.[3] A consumer reporting agency may furnish the following "credit header" information to a governmental agency, without a court order or subpoena: name, current and former addresses, and current and former places of employment.[4]

A consumer reporting agency must provide the following identifying information to the FBI to combat international terrorism or clandestine intelligence activities, when presented with a written request signed by the Director or the Director's designee: names and addresses of all financial institutions at which a consumer maintains or has maintained an account, or the consumer's name, or both; current and former addresses; and current and former places of employment.[5] Pursuant to a court order, a consumer reporting agency shall furnish the FBI with the consumer report for an individual.[6] A consumer reporting agency shall furnish a consumer report of a consumer and all other information in the consumer's file to a government agency conducting an investigation of, or intelligence or counterintelligence activities or analysis related to, international terrorism, when presented with a written certification by such government agency.[7]

FCRA, as amended by the USA Patriot Act, prohibits consumer reporting agencies from notifying consumers that information about them has been provided to the government for counterintelligence or counterterrorism purposes.[8]

"(i) intends to use the information in connection with a credit transaction involving the consumer on whom the information is to be furnished and involving the extension of credit to, or review or collection of an account of, the consumer; or

"(ii) intends to use the information for employment purposes; or

"(iii) intends to use the information in connection with the underwriting of insurance involving the consumer . . . ."

15 U.S.C. § 1681b(a)(3)(A), (B) and (C).

[3] 15 U.S.C. § 1681b(a)(1).

[4] 15 U.S.C. § 1681i(f).

[5] 15 U.S.C. § 1681u(a), (b).

[6] 15 U.S.C. § 1681u(c).

[7] 15 U.S.C. § 1681v(a), (b).

[8] "No consumer reporting agency . . . shall disclose to any person . . . that the Federal Bureau of Investigation has sought or obtained the identity of financial institutions or a consumer report respecting any consumer . . . and shall [not] include in any consumer report any information that would indicate that the Federal Bureau of Investigation has sought or obtained such information or a consumer report." 15 U.S.C. § 1681u(d). "No consumer reporting agency . . . shall disclose to any person, or specify in any consumer report, that a government agency has sought or obtained access to information" related to international terrorism. 15 U.S.C. § 1681v(c).

[2]—Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability Act (HIPAA)[9] restricts the disclosure of protected health information. The HIPAA regulations generally provide that an individual has a right to receive an accounting identifying all disclosures of his or her protected health information during the six years prior to the request.[10] There are various exceptions, such as for disclosures for national security or intelligence purposes and when a law enforcement agency asks for a delay of notice.[11] If the government obtains medical records pursuant to FISA's business records provision, then notice to the affected individual is prohibited.[12]

[3]—Gramm-Leach-Bliley Act

The Financial Services Modernization Act of 1999 (more commonly known as the Gramm-Leach-Bliley Act or GLB) establishes for the

(Text continued on page 1-59)

---

[9] 42 U.S.C. §§ 1301 *et seq*. (1996). HIPAA is covered in detail in Ch. 2 *infra*.
[10] 45 C.F.R. § 164.528(a)(1).
[11] 45 C.F.R. §§ 164.528(a)(1)(vi), (2)(i).
[12] 50 U.S.C. § 1861(d).

financial industry a comprehensive legal framework governing the privacy and security of personal financial information.[13] In short, GLB prohibits a financial institution from disclosing to a nonaffiliated third party nonpublic personal information, except in certain statutorily enumerated instances, unless it has provided the consumer a privacy notice.[14] GLB is implemented by various regulations promulgated by the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of Comptroller of the Currency, the Department of the Treasury, the Office of Thrift Supervision, the Department of the Treasury, the National Credit Union Administration, the Securities and Exchange Commission, applicable state insurance departments or authorities of the states, and the Federal Trade Commission.

[4]—Computer Fraud and Abuse Act of 1986

Among other computer-related acts, the Computer Fraud and Abuse Act of 1986 (CFAA) prohibits the unauthorized access to a computer to obtain information considered to be protected data.[15] The act prohibits the intentional access of a computer without authorization to obtain:

> "(A) information contained in a financial record of a financial institution, or of a card issuer as defined in [Title 15, Section 1602(n) of the United States Code], or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act [Title 15, Sections 1681 *et seq*. of the United States Code]; (B) information from any department or agency of the United States; or (C) information from any protected computer if the conduct involved an interstate or foreign communication."[16]

The term "protected computer" is broadly defined as any computer "which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States."[17]

---

[13] 15 U.S.C. §§ 6801-6809 (disclosure of nonpublic personal information), and §§ 6821-6827 (fraudulent access to financial information). GLB is covered in detail in Ch. 3 *infra*.

[14] 15 U.S.C. § 6802(a).

[15] 18 U.S.C. § 1030(a).

[16] 18 U.S.C. § 1030(a)(2).

[17] 18 U.S.C. § 1030(e)(2)(B).

In addition to any other agency having authority, the United States Secret Service and the Federal Bureau of Investigation may investigate offenses of the CFAA. A violation of the act is punishable by a fine or imprisonment varying from up to one (1) year to life, depending upon aggravating circumstances, or both.[18]

[5]—Cable Communications Policy Act

The Cable Communications Policy Act of 1984 requires cable television operators to provide notice to their subscribers annually and at the time of initiating service, about the nature of personal data collected, data use and disclosure practices, and subscriber rights under the statute.[19] The act prohibits a cable television company from collecting individually identifiable information about its subscribers over the cable system without their prior written consent, except as disclosed by such notice.[20] The act generally bars cable operators from disclosing such data without prior written consent of the subscriber, except for disclosure of lists of subscriber names and addresses that do not reflect the subscribers' viewing habits or transactions over the cable system.[21]

The act requires the cable operator to allow subscriber access to all personally identifiable information about the subscriber and a right to correct any errors.[22] It requires the cable operator to destroy individually identifiable information when no longer necessary for the purpose for which it was collected.[23]

A governmental entity may obtain personally identifiable information concerning a cable subscriber:

> (i) as authorized under Title 18, Sections 2510 *et seq*. of the United States Code (Wiretap Statute), Title 18, Sections 2701 *et seq*. of the United States Code (ECPA), or Title 18, Sections 3121 *et seq*. of the United States Code (Pen/Trap Statute), "except that such disclosure shall not include records revealing cable subscriber selection of video programming from a cable operator";[24] and
>
> (ii) "pursuant to a court order only if, in the court proceeding relevant to such court order—

---

[18] 18 U.S.C. § 1030(c).
[19] 47 U.S.C. § 551(a)(1).
[20] 47 U.S.C. § 551(b)(1).
[21] 47 U.S.C. § 551(c).
[22] 47 U.S.C. § 551(d).
[23] 47 U.S.C. § 551(e).
[24] 47 U.S.C. § 551(c)(2)(D).

"(1) such entity offers clear and convincing evidence that the subject of the information is reasonably suspected of engaging in criminal activity and that the information sought would be material evidence in the case; and

"(2) the subject of the information is afforded the opportunity to appear and contest such entity's claim."[25]

It has been held that the privacy protections of the Cable Communications Policy Act are outweighed by the need to disclose a cable subscriber's identifying information where it has been alleged that such subscriber violated the Computer Fraud and Abuse Act by hacking into a computer without authorization, while using an Internet Protocol (IP) address issued by a cable operator.[25.1]

It has also been held that the privacy protections of the Cable Communications Policy Act do not apply to cable operators providing Internet services.[25.2]

[6]—Telecommunications Privacy Act

The Telecommunications Privacy Act restricts the disclosure of individually identifiable subscriber data to third parties without prior customer approval:

"Except as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary network information in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories."[26]

The act applies to data obtained by a telecommunications carrier concerning subscribers' subscription to and use of a telecommunications service (not Internet services).

---

[25] 47 U.S.C. § 551(h).

[25.1] Kimberlite Corp. v. Does 1-20, 2008 U.S. Dist. LEXIS 43071 at *6 (N.D. Cal. June 2, 2008).

[25.2] *Sixth Circuit:* Klimas v. Comcast Cable Communications, Inc., 465 F.3d 271, 279-280 (6th Cir. 2006).

Ninth Circuit: AT&T Corp. v. City of Portland, 216 F.3d 871, 876-877 (9th Cir. 2000).

[26] 47 U.S.C. § 222(c)(1).

The restrictions on use, disclosure and access do not apply:

(1) to aggregate customer information;[27]

(2) with respect to billing and collection for telecommunications services;[28]

(3) "to protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services";[29]

(4) "to provide any inbound telemarketing, referral, or administrative services to the customer for the duration of the call, if such call was initiated by the customer and the customer approves of the use of such information to provide such service";[30] and

(5) "to provide call location information concerning the user of a commercial mobile service" for emergency services (e.g., with regard to "911" calls).[31]

[7]—Family Educational Rights and Privacy Act[31.1]

The Family Educational Rights and Privacy Act prohibits schools receiving public funds from disclosing personally identifiable information (PII) in a student's education records, other than directory information, without the consent of the student or of the parent of a minor student.[32] The act achieves this objective by withholding funds from any educational agency or institution that acts in contravention to the requirements of the act.

The term "directory information" includes "the student's name, address, telephone listing, date and place of birth, major field of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, degrees and awards received, and the most recent previous educational agency or

---

[27] 47 U.S.C. § 222(c)(3).

[28] 47 U.S.C. § 222(d)(1).

[29] 47 U.S.C. § 222(d)(2).

[30] 47 U.S.C. § 222(d)(3).

[31] 47 U.S.C. § 222(d)(4).

[31.1] The Department of Education issued its Final Rule to FERPA on December 9, 2008, which became effective January 8, 2009 and implemented various changes including prohibiting the disclosure of a student's Social Security number, expanding the definition of "personally identifiable information" to include biometric data, and requiring that outside vendors who access student information covered by FERPA be under the "direct control" of the academic institution (discussed *infra)*. See, generally, Family Educational Rights and Privacy; Final Rule, 73 C.F.R. § 74806.

[32] 20 U.S.C §1232g(b)(1). A student eighteen years old, or who is attending an institution of postsecondary education, may give permission or consent, and not the parent. 20 U.S.C. § 1232g(d).

institution attended by the student."[33] "Directory information" specifically *excludes* a student's Social Security number (SSN) and student identification number (ID), but may include the SSN or ID only if it "cannot be used to gain access to education records except when used in conjunction with one or more factors that authenticate the user's identity, such as a personal identification number (PIN), password, or other factor known or possessed only by the authorized user."[33.1] PII includes, but is not limited to, "(a) [t]he student's name; (b) [t]he name of the student's parent or other family members; (c) [t]he address of the student or student's family; (d) [a] personal identifier, such as the student's [S]ocial [S]ecurity number, student number, or biometric record; (e) [o]ther indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name; (f) [o]ther information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or (g) [i]nformation requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates."[33.2]

The act exempts from consent disclosures for a variety of educational, statistical and public safety purposes.[34] A student's consent is not required to disclose PII to a "contractor, consultant, volunteer, or other party to whom an agency or institution has outsourced institutional services or functions" provided that the outside party "(1) [p]erforms an institutional service or function for which the agency or institution would otherwise use employees; (2) [i]s under the direct control of the agency or institution with respect to the use and maintenance of education records; and (3) [i]s subject to the requirements of § 99.33(a) governing the use and redisclosure of personally

---

[33] 20 U.S.C §1232g(a)(5)(A).

[33.1] 34 C.F.R. Part 99.3. See Family Educational Rights and Privacy; Final Rule, 73 C.F.R. § 74851. The exclusion of SSNs was introduced by the Department of Education's Final Rule, which became effective January 8, 2009.

[33.2] 34 C.F.R. § 99.3. See Family Educational Rights and Privacy; Final Rule, 73 C.F.R. 74852. The December 8, 2009 Final Rule added "biometric record" to the definition of PII. "Biometric record" is defined as "a record of one or more measurable biological or behavioral characteristics that can be used for automated recognition of an individual." Examples include "fingerprints; retina and iris patterns; voiceprints; DNA sequence; facial characteristics; and handwriting." See Family Educational Rights and Privacy; Final Rule, 73 C.F.R. 74851.

[34] 20 U.S.C §1232g(b)(1)(A)-(J).

identifiable information from education records."[34.1] Title 34, Section 99.33(a) of the Code of Federal Regulations permits an educational agency or institution to disclose PII only on the condition that the party to whom the information is disclosed will not disclose the information to any other party without the prior consent of the parent or student, except under certain limited circumstances, such as in response to a court order or lawfully issued subpoena.[34.2]

The Comptroller General of the United States, the Secretary of Education, and state educational authorities may have "access to student or other records which may be necessary in connection with the audit and evaluation of Federally-supported education programs, or in connection with the enforcement of the Federal legal requirements which relate to such programs," or any state supported education program, so long as the personal information of students and parents is not disclosed to others and such information is destroyed when no longer needed for the audit.[35] A school may disclose information oth-

(Text continued on page 1-63)

[34.1] 34 C.F.R. § 99.31. See Family Educational Rights and Privacy; Final Rule, 73 C.F.R. § 74853.

[34.2] 34 C.F.R. § 99.33(a).

[35] 20 U.S.C §1232g(b)(3); 20 U.S.C §1232g(b)(5).

erwise protected by this act in connection with various crimes or disciplinary matters, such as:

(1) "to an alleged victim of any crime of violence (as that term is defined in [Title 18, Section 16 of the United States Code]), or a nonforcible sex offense, the final results of any disciplinary proceeding conducted by such institution against the alleged perpetrator of such crime or offense with respect to such crime or offense";[36]

(2) disclosing information "concerning disciplinary action taken against such student for conduct that posed a significant risk to the safety or well-being of that student, other students, or other members of the school community," "to teachers and school officials, including teachers and school officials in other schools, who have legitimate educational interests in the behavior of the student";[37]

(3) "disclosing, to a parent or legal guardian of a student, information regarding any violation of any Federal, State, or local law, or of any rule or policy of the institution, governing the use or possession of alcohol or a controlled substance, regardless of whether that information is contained in the student's education records, if—

"(A) the student is under the age of 21; and

"(B) the institution determines that the student has committed a disciplinary violation with respect to such use or possession";[38] and

(4) via a written application, by an Attorney General, to a court of competent jurisdiction for an *ex parte* order to "collect education records in the possession of the educational agency or institution that are relevant to an authorized investigation or prosecution of an offense listed in [Title 18, Section 2332b(g)(5)(B) of the United States Code],[39] or an act of domestic or international terrorism as defined in Title 18, Section 2331 of the United States code]."[40]

---

[36] 20 U.S.C §1232g(b)(6)(A).

[37] 20 U.S.C §1232g(h).

[38] 20 U.S.C §1232g(i).

[39] 18 U.S.C. § 2332b(g)(5)(B) lists various crimes and statutory violations, such as the destruction of aircraft or aircraft facilities; violence at international airports; arson within special maritime and territorial jurisdiction; congressional, cabinet, and Supreme Court assassination and kidnapping; and pertaining to biological weapons, chemical weapons, and nuclear materials.

[40] 20 U.S.C §1232g(j) (investigation and prosecution of terrorism).

[8]—Video Privacy Protection Act of 1988

The Video Privacy Protection Act[41] prohibits a video tape service provider from knowingly disclosing personally identifiable information concerning its consumers.[42] A video tape service provider may disclose personally identifiable information concerning any consumer:

> "(A) to the consumer;
>
> "(B) to any person with the informed, written consent of the consumer given at the time the disclosure is sought;
>
> "(C) to a law enforcement agency pursuant to a warrant issued under the Federal Rules of Criminal Procedure, an equivalent State warrant, a grand jury subpoena, or a court order;
>
> "(D) to any person if the disclosure is solely of the names and addresses of consumers and if—
>
> > "(i) the video tape service provider has provided the consumer with the opportunity, in a clear and conspicuous manner, to prohibit such disclosure; and
> >
> > "(ii) the disclosure does not identify the title, description, or subject matter of any video tapes or other audio visual material; however, the subject matter of such materials may be disclosed if the disclosure is for the exclusive use of marketing goods and services directly to the consumer;
>
> "(E) to any person if the disclosure is incident to the ordinary course of business of the video tape service provider; or
>
> "(F) pursuant to a court order, in a civil proceeding upon a showing of compelling need for the information that cannot be accommodated by any other means, if—
>
> > "(i) the consumer is given reasonable notice, by the person seeking the disclosure, of the court proceeding relevant to the issuance of the court order; and
> >
> > "(ii) the consumer is afforded the opportunity to appear and contest the claim of the person seeking the disclosure."[43]

The USA Patriot Act permits law enforcement to obtain business, personal or medical records regarding an individual prior to obtaining a warrant, obtaining consent from the individual, or giving the individual notice.[44]

---

[41] 18 U.S.C. § 2710.

[42] 18 U.S.C. § 2710(b). Disclosures related to video-on-demand services from a cable television provider are covered by Cable Communications Policy Act 47 U.S.C. § 551.

[43] 18 U.S.C. § 2710(b)(2).

[44] Title II § 213 (authority for delaying notice of the execution of a warrant).

[9]—Employee Polygraph Protection Act of 1988

The Employee Polygraph Protection Act[45] prevents employers in the private sector from administering lie detector[46] tests either for pre-employment screening purposes or during the course of employment, with certain exceptions. An employee or prospective employee may not be disciplined, discharged or denied employment for refusing to take a lie detector test or for filing a complaint against an employer who administers these tests.

The act does not apply to the federal, state and local governments.[47] Furthermore, the federal government may administer lie detector tests:

> (1) in the performance of any counterintelligence function, to any consultant or employee of the Department of Defense;[48]
>
> (2) in the performance of any intelligence or counterintelligence function, to any consultant, employee or prospective employee of the National Security Agency, the Defense Intelligence Agency, the National Geospatial-Intelligence Agency, or the Central Intelligence Agency;[49]
>
> (3) in the performance of any intelligence or counterintelligence function, to any consultant "under contract with any Federal Government department, agency, or program whose duties involve access to information that has been classified at the level of top secret or designated as being within a special access program under section 4.2(a) of Executive Order 12356 (or a successor Executive order)";[50] and
>
> (4) in the performance of any counterintelligence function, to any consultant or employee of the Federal Bureau of Investigation of the Department of Justice.[51]

---

[45] 29 U.S.C. § 2001.

[46] A lie detector includes a polygraph, deceptograph, voice stress analyzer, psychological stress evaluator, or similar device (whether mechanical or electrical) used to render a diagnostic opinion as to the honesty or dishonesty of an individual.

[47] 29 U.S.C. § 2006(a).

[48] 29 U.S.C. § 2006(b)(1).

[49] 29 U.S.C. § 2006(b)(2)(A). The test may also be administered to "any individual assigned to a space where sensitive cryptologic information is produced, processed, or stored for any such agency." 29 U.S.C. § 2006(b)(2)(A)(v).

[50] 29 U.S.C. § 2006(b)(2)(B).

[51] 29 U.S.C. § 2006(c).

An employer may administer a lie detector test to an employee in certain instances 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."[52] An employer primarily involved in providing armored car personnel, personnel engaged in the design, installation and maintenance of security alarm systems, or other uniformed or plainclothes security personnel may administer a lie detector test to a prospective employee.[53] An employer authorized to manufacture, distribute or dispense a controlled substance listed in schedule I, II, III, or IV of Title 21, Section 812 of the United States Code may administer a lie detector test to a current or prospective employee under certain circumstances.[54]

[10]—Telephone Consumer Protection Act of 1991

The Telephone Consumer Protection Act[55] allows the Federal Communications Commission (FCC) to regulate unwanted commercial solicitation or telemarketing calls to residential telephones. The FCC created a national do-not-call registry in which individuals may add their telephone numbers to avoid receiving telemarketing calls. Telemarketing calls are exempt from this act if they are made (1) on behalf of a tax-exempt nonprofit organization; (2) with the consent of a consumer; or (3) to a consumer with whom the calling company has an established business relationship.[56]

---

[52] 29 U.S.C. § 2006(d).
[53] 29 U.S.C. § 2006(e).
[54] 29 U.S.C. § 2006(f).
[55] 47 U.S.C. § 227.
[56] 47 U.S.C. § 227(a)(3).

§ 1.06 Statutes Restricting Government's Disclosure of Personal Information

Several statutes specifically restrict the government's authority to disclose certain information. They include the following.

Statute	Cite
Privacy Act of 1974	5 U.S.C. § 552a
Freedom of Information Act of 1966	5 U.S.C. § 552
Driver's Privacy Protection Act of 1994	18 U.S.C. §§ 2721-2725

[1]—Privacy Act of 1974

The Privacy Act of 1974 limits third party access to personal information maintained by the federal government.[1] No government agency may disclose any "record" except:

(1) with the written consent of the individual to whom the record pertains;[2]

(2) to those officers and employees of the agency that maintains the record who have a need for the record in the performance of their duties;[3]

(3) as required under Title 5, Section 552 of the United States Code (the Freedom of Information Act);[4]

(4) for a "routine use"[5] ("'routine use' means, with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected");[6]

(5) to the Bureau of the Census for purposes of planning or carrying out a census or survey or related activity pursuant to the provisions of Title 13 of the United States Code;[7]

(6) "to a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable";[8]

---

[1] 5 U.S.C. § 552a.
[2] 5 U.S.C. § 552a(b).
[3] 5 U.S.C. § 552a(b)(1).
[4] 5 U.S.C. § 552a(b)(2).
[5] 5 U.S.C. § 552a(b)(3).
[6] 5 U.S.C. § 552a(a)(7).
[7] 5 U.S.C. § 552a(b)(4).
[8] 5 U.S.C. § 552a(b)(5).

(7) "to the National Archives and Records Administration as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, or for evaluation by the Archivist of the United States or the designee of the Archivist to determine whether the record has such value";[9]

(8) "to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought";[10]

(9) "to a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure notification is transmitted to the last known address of such individual";[11]

(10) "to either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress or subcommittee of any such joint committee";[12]

(11) "to the Comptroller General, or any of his authorized representatives, in the course of the performance of the duties of the General Accounting Office";[13]

(12) "pursuant to the order of a court of competent jurisdiction";[14] or

(13) to a consumer reporting agency in accordance with Title 31, Section 3711(e) of the United States Code.[15]

"Record" means "any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph."[16]

---

[9] 5 U.S.C. § 552a(b)(6).

[10] 5 U.S.C. § 552a(b)(7).

[11] 5 U.S.C. § 552a(b)(8).

[12] 5 U.S.C. § 552a(b)(9).

[13] 5 U.S.C. § 552a(b)(10).

[14] 5 U.S.C. § 552a(b)(11).

[15] 5 U.S.C. § 552a(b)(12). 31 U.S.C § 3711(e) permits the government, under certain circumstances, to disclose information in an individual's record to a consumer reporting agency when attempting to collect from that individual a monetary claim of the government.

[16] 5 U.S.C. § 552a(a)(4).

The Privacy Act requires the government to allow an individual access to his or her record upon request.[17] An individual may request that his or her record be amended if it is not "accurate, relevant, timely, or

(Text continued on page 1-69)

---

[17] 5 U.S.C. § 552a(d)(1).

complete."[18] The government will either make such amendment or inform the individual that it refuses to amend the record.[19] If the government refuses to amend the record, the individual may request a review, in which case the government shall review the matter and make a final determination within thirty days from the request (which may be extended for good cause).[20] If the government still refuses to amend the record, the individual may "file with the agency a concise statement setting forth the reasons for his disagreement with the refusal of the agency," and may seek civil remedies under Title 5, Section 552a(g) of the United States Code by bringing a civil action against the agency in district court.[21]

[2]—Freedom of Information Act

The Freedom of Information Act (FOIA) permits public access to certain government records.[22] Any government agency, upon the request of a person that "reasonably describes such records," shall promptly make available to that person those records.[23] The records shall be made available in accordance with published rules pertaining to the "time, place, fees (if any), and procedures to be followed" for access to such records.[24]

"Record" includes "any information that would be an agency record subject to the requirements of this section when maintained by an agency in any format, including an electronic format."[25]

FOIA does not permit public access to matters:

(1) "specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and [ ] in fact properly classified pursuant to such Executive order;[26]

(2) "related solely to the internal personnel rules and practices of an agency;[27]

---

[18] 5 U.S.C. § 552a(d)(2).

[19] 5 U.S.C. § 552a(d)(2)(B).

[20] 5 U.S.C. § 552a(d)(3).

[21] 5 U.S.C. § 552a(d)(3); 5 U.S.C. § 552a(g).

[22] 5 U.S.C. § 552.

[23] 5 U.S.C. § 552(a)(3)(A).

[24] 5 U.S.C. § 552(a)(3)(A)(ii). See also, 5 U.S.C. § 552(a)(4)(A) on procedures for establishing fees for access to records.

[25] 5 U.S.C. § 552(f)(2).

[26] 5 U.S.C. § 552(b)(1).

[27] 5 U.S.C. § 552(b)(2).

(3) "specifically exempted from disclosure by statute (other than [Title 5, Section 552b of the United States Code]), provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;[28]

(4) "trade secrets and commercial or financial information obtained from a person and privileged or confidential;[29]

(5) "inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;[30]

(6) "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;[31]

(7) "records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information (A) could reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of a confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of a record or information compiled by criminal law enforcement authority in the course of a criminal investigation or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual;[32]

(8) "contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions;[33] or

---

[28] 5 U.S.C. § 552(b)(3).
[29] 5 U.S.C. § 552(b)(4).
[30] 5 U.S.C. § 552(b)(5).
[31] 5 U.S.C. § 552(b)(6).
[32] 5 U.S.C. § 552(b)(7).
[33] 5 U.S.C. § 552(b)(8).

(9) geological and geophysical information and data, including maps, concerning wells."[34]

[3]—Driver's Privacy Protection Act of 1994

The Driver's Privacy Protection Act prohibits state departments of motor vehicles or officers, employees or contractors thereof from knowingly disclosing or otherwise making available to any person or entity personal information obtained by the department in connection with a motor vehicle record, except as otherwise permitted by the act.[35]

The act distinguishes between "personal information" and "highly restricted personal information."[36] "Personal information" is "information that identifies an individual, including an individual's photograph, [S]ocial [S]ecurity number, driver identification number, name, address (but not the 5-digit zip code), telephone number, and medical or disability information, but does not include information on vehicular accidents, driving violations, and driver's status."[37] "Highly restricted personal information" is "an individual's photograph or image, [S]ocial [S]ecurity number, medical or disability information."[38]

The act permits the disclosure of "personal information" and "highly restricted personal information" under the following circumstances:

(1) "For use by any government agency, including any court or law enforcement agency, in carrying out its functions, or any private person or entity acting on behalf of a Federal, State, or local agency in carrying out its functions."[39]

(2) "For use in connection with any civil, criminal, administrative, or arbitral proceeding in any Federal, State, or local court or agency or before any self-regulatory body, including the service of process, investigation in anticipation of litigation, and the execution or enforcement of judgments and orders, or pursuant to an order of a Federal, State, or local court."[40]

(3) "For use by any insurer or insurance support organization, or by a self-insured entity, or its agents, employees, or contractors, in connection with claims investigation activities, antifraud activities,

---

[34] 5 U.S.C. § 552(b)(9).
[35] 18 U.S.C. § 2721(a).
[36] 18 U.S.C. § 2721(a).
[37] 18 U.S.C. § 2721(3).
[38] 18 U.S.C. § 2725(4).
[39] 18 U.S.C. § 2721(b)(1).
[40] 18 U.S.C. § 2721(b)(4).

rating or underwriting."[41]

(4) "For use by an employer or its agent or insurer to obtain or verify information relating to a holder of a commercial driver's license that is required under [Title 49, Section 313 of the United States Code]."[42]

The act permits the disclosure of "personal information" under the following additional circumstances:

(1) "For use in connection with matters of motor vehicle or driver safety and theft; motor vehicle emissions; motor vehicle product alterations, recalls, or advisories; performance monitoring of motor vehicles, motor vehicle parts and dealers; motor vehicle market research activities, including survey research; and removal of non-owner records from the original owner records of motor vehicle manufacturers."[43]

(2) "For use in the normal course of business by a legitimate business or its agents, employees, or contractors, but only—(A) to verify the accuracy of personal information submitted by the individual to the business or its agents, employees, or contractors; and (B) if such information as so submitted is not correct or is no longer correct, to obtain the correct information, but only for the purposes of preventing fraud by, pursuing legal remedies against, or recovering on a debt or security interest against, the individual."[44]

(3) "For use in research activities, and for use in producing statistical reports, so long as the personal information is not published, redisclosed, or used to contact individuals."[45]

(4) "For use in providing notice to the owners of towed or impounded vehicles."[46]

(5) "For use by any licensed private investigative agency or licensed security service for any purpose permitted under this subsection."[47]

(6) "For use in connection with the operation of private toll transportation facilities."[48]

---

[41] 18 U.S.C. § 2721(b)(6).
[42] 18 U.S.C. § 2721(b)(9).
[43] 18 U.S.C. § 2721(b)(2).
[44] 18 U.S.C. § 2721(b)(3).
[45] 18 U.S.C. § 2721(b)(5).
[46] 18 U.S.C. § 2721(b)(7).
[47] 18 U.S.C. § 2721(b)(8).
[48] 18 U.S.C. § 2721(b)(10).

(7) "For any other use in response to requests for individual motor vehicle records if the State has obtained the express consent of the person to whom such personal information pertains."[49]

(8) "For bulk distribution for surveys, marketing or solicitations if the State has obtained the express consent of the person to whom such personal information pertains."[50]

(9) "For use by any requester, if the requester demonstrates it has obtained the written consent of the individual to whom the information pertains."[51]

(10) "For any other use specifically authorized under the law of the State that holds the record, if such use is related to the operation of a motor vehicle or public safety."[52]

Except for a recipient under Title18, Section 2721(b)(11) or (12) of the United States Code, an authorized recipient of personal information may resell or redisclose the information only for a use permitted under Section 2721(b), but not for uses under Section 2721(b)(11) or (12).[53] An authorized recipient under Section 2721(b)(11) may resell or redisclose personal information for any purpose.[54] An authorized recipient under Section 2721(b)(12) may resell or redisclose personal information pursuant to that section.[55] Except for a recipient under Section 2721(b)(11), any authorized recipient that resells or rediscloses personal information must keep for five years records identifying each person or entity that receives information and the permitted purpose for which the information will be used.[56]

---

[49] 18 U.S.C. § 2721(b)(11).
[50] 18 U.S.C. § 2721(b)(12).
[51] 18 U.S.C. § 2721(b)(13).
[52] 18 U.S.C. § 2721(b)(14).
[53] 18 U.S.C. § 2721(c).
[54] 18 U.S.C. § 2721(c).
[55] 18 U.S.C. § 2721(c).
[56] 18 U.S.C. § 2721(c).

§ 1.07 Social Security Numbers

[1]—Background

The Social Security Act of 1935 authorized the Social Security Administration (SSA) to establish a record-keeping system to manage the Social Security program.[1] In 1936, the Social Security Administration created the Social Security number (SSN) to aid in that effort. The original intended purpose for SSNs was narrow—they were used to track workers' earnings for Social Security benefit purposes. SSNs have since become a commonly used personal identifier for many other purposes, including child support collections, law enforcement, and issuing credit to individuals. An unfortunate consequence of this wider use is that the SSN has become a key piece of information used in identity theft.[2]

There are federal and state laws that restrict the use of SSNs. The tables below identify a number of these laws.

[2]—Federal Laws Restricting Use of SSNs

There are several federal laws that directly and indirectly restrict the use or disclosure of SSNs, or both. The table below identifies such laws.

LAW	RESTRICTION
Fair Credit Reporting Act (FCRA), 1970	Restricts access to credit data (which includes SSNs) to those who have a permissible purpose under the law.
Fair and Accurate Credit Transactions Act (FACTA), 2003	Amends FCRA to allow, among other things, consumers who request a copy of their file to also request that the first five digits of the SSN (or similar identification number) not be included in the file; also requires consumer reporting agencies and any businesses that use a consumer report to implement procedures for proper disposal of the report information; also requires credit and debit card receipts to be truncated to show no more than the last five digits of the SSN and to not show the card's expiration date.

---

[1] The Social Security Act of 1935 created the Social Security Board, which was renamed the Social Security Administration in 1946. See Social Security Numbers-Federal and State Laws Restrict Use of SSNs, yet Gaps Remain, U.S. Government Accountability Office, Testimony Before the Committee on Consumer Affairs and Protection and Committee on Governmental Operations, New York State Assembly, Sept. 15, 2005, available at http://www.gao.gov/new.items/d051016t.pdf (last visited Jan. 30, 2008).

[2] Social Security Numbers-Use is Widespread and Protection Could Be Improved, U.S. Government Accountability Office, Testimony Before the Subcommittee on Social Security, Committee on Ways and Means, House of Representatives, June 21, 2007, available at http://www.gao.gov/new.items/d071023t.pdf (last visited Jan. 30, 2008).

LAW	RESTRICTION
Gramm-Leach-Bliley Act (GLBA)	Protects the privacy of nonpublic personal information (which includes SSNs) by limiting when financial institutions may disclose that information to nonaffiliated third parties.
Drivers Privacy Protection Act (DPPA) by law.	Prohibits the obtaining and disclosing of SSNs from a motor vehicle record except as expressly permitted
Health Insurance Portability and Accountability Act (HIPAA)	Protects the privacy of an individual's health information (which includes SSNs) by limiting health care organizations from disclosing such information without the patient's consent.

[3]—State Laws Restricting Use of SSNs

There are a number of state laws that were enacted in the first decade of the twenty-first century, many of which became effective in 2006 and 2007 and in certain instances become effective as late as 2009, that specifically address the use or disclosure of SSNs, or both. The table below identifies such laws.

STATE	LAW	PURPOSE
Alabama	Ala. Code § 41-13-6	Prohibits state agencies from revealing the SSN of a person on any document available for public inspection.
Alaska	Alaska Stat. § 45.48.400 (2008) [Effective July 1, 2009]	Prohibits persons from engaging in certain activities with SSNs, such as posting or publicly displaying SSNs or requiring people to transmit SSNs over the Internet unless the connections are secure or the SSNs are encrypted; restricts the printing of SSNs on ID cards required to access products or services.
Arizona	Ariz. Rev. Stat. Ann. § 15-1823	Prohibits the use of a student's SSN as an identification number.
	Ariz. Rev. Stat. Ann. § 44-1373	Prohibits companies and persons from engaging in certain activities with SSNs; restricts the printing of SSNs on ID cards required to access products or services, or requiring people to transmit an SSN over the Internet unless the connection is secure or the SSN is encrypted.

STATE	LAW	PURPOSE
Arkansas	Ark. Code Ann. § 4-86-107	Prohibits companies and persons from engaging in certain activities with SSNs, such as posting or publicly displaying SSNs; restricts the printing of SSNs on ID cards required to access products or services; restricts transmitting SSNs over the Internet unless the connection is secure or the SSN is encrypted.
	Ark. Code Ann. § 6-18-208	Prohibits the use of a student's SSN as an identification number.
California	Cal. Civ. Code § 1798.85	Prohibits companies and persons from engaging in certain activities with SSNs, such as posting or publicly displaying SSNs, printing SSNs on ID cards required to access products or services, or requiring people to transmit an SSN over the Internet unless the connection is secure or the number is encrypted.
Colorado	Col. Rev. Stat. § 6-1-715	Prohibits companies and persons from engaging in certain activities with SSNs, such as posting or publicly displaying SSNs, printing SSNs on ID cards required to access products or services, or requiring people to transmit an SSN over the Internet unless the connection is secure or the number is encrypted.
	Col. Rev. Stat. § 23-5-127	Prohibits the use of a student's SSN as an identification number.
	Col. Rev. Stat. § 24-72.3-102	Prohibits public entities from issuing a license, permit, pass or certificate containing SSNs, or requesting an SSN over the phone, Internet or via mail, unless required by law or essential to services by the public entity.
Connecticut	Conn. Gen. Stat. Ann. § 42-470	Prohibits companies and persons from engaging in certain activities with SSNs, such as posting or publicly displaying SSNs, printing SSNs on ID cards required to access products or services, or requiring people to transmit an SSN over the Internet unless the connection is secure or the number is encrypted.
	2008 Conn. H.B. 5658, Conn. ALS 167	Any person who collects SSNs in the course of business shall create a privacy protection policy that will be published or publicly displayed. Such policy shall protect the confidentiality of SSNs, prohibit unlawful disclosure of SSNs, and limit access to SSNs.

STATE	LAW	PURPOSE
Delaware	No analogous provisions.	
District of Columbia	No analogous provisions.	
Florida	No analogous provisions.	
Georgia	Ga. Code Ann. § 10-1-393.8	Prohibits companies and persons from engaging in certain activities with SSNs, such as posting or publicly displaying SSNs, or requiring people to transmit an SSN over the Internet unless the connection is secure or the number is encrypted.
	Ga. Code Ann. § 40-5-28.1	Prohibits drivers' licenses or permits from containing SSNs of such persons.
Hawaii	Haw. Rev. Stat. § 487J-2 (amended by 2008 Haw. L. Act 19 (S.B. 2402))	Prohibits companies and persons from engaging in certain activities with SSNs, such as posting or publicly displaying SSNs, printing SSNs on ID cards required to access products or services, or requiring people to transmit an SSN over the Internet unless the connection is secure or the number is encrypted.
	Haw. Rev. Stat. § 487R-2 (amended by 2008 Haw. L. Act 19 (S.B. 2402))	Any business or government agency that maintains or otherwise possesses personal information of a Hawaii resident (including SSNs) shall take reasonable measures to protect against unauthorized access.
Idaho	Idaho Code §§ 18-3122 and 18-3126 (2008)	Prohibits any person from obtaining or recording personal identifying information (including SSNs) of another person without authorization of that person, with the intent that the information be used to obtain, or attempt to obtain, credit, money, goods or services without that person's consent.
Illinois	110 ILCS 305/30; 110 ILCS 520/16; 110 ILCS 660/5-125; 110 ILCS 665/10-125; 110 ILCS 670/15-125; 110 ILCS 675/20-130; 110 ILCS 680/25-125; 110 ILCS 685/30-135; 110 ILCS 690/35-130; and 110 ILCS 805/3-60	Various state university statutes providing that colleges and universities may not provide a student's SSN to a financial institution that issues credit cards, unless the student is over 21. In addition, the colleges and universities may not print an individual's SSN on any card or other document required for the individual to access products or services provided by such institution.

STATE	LAW	PURPOSE
	815 Ill. Ann. Stat. 505/2RR	Prohibits companies and persons from engaging in certain activities with SSNs, such as posting or publicly displaying SSNs, printing SSNs on ID cards required to access products or services, or requiring people to transmit an SSN over the Internet unless the connection is secure or the number is encrypted.
Indiana	Ind. Code §§ 4-1-10-1 *et seq*.	Prohibits state agencies from releasing SSNs unless otherwise required by law.
Iowa	No analogous provisions.	
Kansas	Kan. Stat. Ann. § 75-3520	Restricts the solicitation of SSNs; limits the denial of goods and services to an individual who declines to give an SSN.
Kentucky	No analogous provisions.	
Louisiana	No analogous provisions.	
Maine	10 Me. Rev. Stat. Ann. § 1272-B	Restricts the solicitation of SSNs; limits the denial of goods and services to an individual who declines to give an SSN.
Maryland	Md. Code Ann., Com. Law §§ 14-3401 *et seq*.	Prohibits companies and persons from engaging in certain activities with SSNs, such as posting or publicly displaying SSNs, printing SSNs on ID cards required to access products or services, or requiring people to transmit an SSN over the Internet unless the connection is secure or the number is encrypted.
	Md. Code Ann., Art. 24, § 1-109, Md. EDUCATION Code Ann. § 6-114, Md. EDUCATION Code Ann. § 7-113, Md. EDUCATION Code Ann. § 15-110, Md. STATE PERSONNEL AND PENSIONS Code Ann. § 1-202	A local government, schools or the state may not print an employee's or student's SSN on any ID card.
Massachusetts	Gen. L. Ann., Ch. 93H, § 2 and 201 Code Mass. Reg. §§ 17.01 *et seq*.	Persons who own, license, store or maintain personal information (including SSNs) about a resident of Massachusetts must meet minimum standards in safeguarding such personal information, including a comprehensive written information security program and the establishment and maintenance of a security

STATE	LAW	PURPOSE
		system covering computers to restrict access to such personal information.
Michigan	Mich. Comp. L. §§ 445.81 *et seq*.	Prohibits companies and persons from engaging in certain activities with SSNs; prohibits the use of more than four sequential digits of the SSN; prohibits the use of SSNs on identification and membership cards, permits and licenses.
	Mich. Comp. L. § 445.84	A person who obtains SSNs in the ordinary course of business shall create a privacy policy that does at least all of the following: (a) ensures confidentiality of SSNs, (b) prohibits unlawful disclosure of SSNs, (c) limits who has access to information containing SSNs, (d) describes how to properly dispose of documents containing SSNs and (e) establishes penalties for violation of the policy.
Minnesota	Minn. Stat. Ann. § 325E.59	Prohibits companies and persons from engaging in certain activities with SSNs, such as posting or publicly displaying SSNs, printing SSNs on ID cards required to access products or services, or requiring people to transmit an SSN over the Internet unless the connection is secure or the number is encrypted.
Mississippi	No analogous provisions.	
Missouri	Mo. Rev. Stat. § 407.1355	Prohibits companies and persons from engaging in certain activities with SSNs, such as posting or publicly displaying SSNs, or requiring people to transmit an SSN over the Internet unless the connection is secure or the number is encrypted; prohibits requiring an individual to use his or her SSN as an employee number.
Montana	No analogous provisions.	
Nebraska	2007 Neb. LB 674, § 16 [effective September 1, 2008] to R.R.S. Neb. §§ 8-2601 *et seq*.	Section of Credit Report Protection Act, effective as of September 1, 2008, prohibits an employer from publicly posting or displaying more than the last 4 digits of an employee's SSN; requiring an employee to transmit no more than the last four digits of an SSN over the Internet unless the connection is secure or the information is encrypted; or requiring an employee to use no more than the last four digits

STATE	LAW	PURPOSE
		of an SSN to access an Internet Web site or as an employee number for any employee-related activity.
Nevada	Nev. Rev. Stat. § 239B.030	A person shall not include and a governmental agency shall not require a person to include an SSN on any document filed with the governmental agency after January 1, 2007. Each governmental agency shall ensure that any SSN contained in a document that has been filed will be maintained in a confidential manner or otherwise removed from the document.
	Nev. Rev. Stat. § 239B.050	If a public body maintains a Web site on the Internet, it shall not disclose personal information (including SSNs) unless required by law.
New Hampshire	No analogous provisions.	
New Jersey	N.J. Stat. Ann. § 56:8-164	Prohibits companies and persons from engaging in certain activities with SSNs, such as publicly posting SSNs or any four or more consecutive numbers from an SSN; restricts the printing of SSNs on ID cards required to access products or services; restricts requiring people to transmit an SSN over the Internet unless the connection is secure or the number is encrypted.
New Mexico	N.M. Stat. Ann. §§ 57-12B-4, 57-12B-3	Restricts the solicitation of SSNs; limits the denial of goods and services to an individual who declines to give an SSN.
	N.M. Stat. Ann. §§ 57-12B-1 *et seq*.	Requires businesses that have obtained SSNs to limit access to authorized employees; prohibits a business from making an SSN available to the public (including printing an SSN on a receipt for the purchase of products or services); restricts a business requiring use of an SSN (including over the Internet without a secure connection).
New York	N.Y. Gen. Bus. L. § 399-dd	Prohibits companies and persons from engaging in certain activities with SSNs, such as intentionally disclosing an SSN to the public; restricts the printing of SSNs on ID cards required to access products or services; restricts requiring

STATE	LAW	PURPOSE
		people to transmit an SSN over the Internet unless the connection is secure or the number is encrypted.
	N.Y. Lab. L. § 203-d	An employer shall not unless otherwise required by law: (a) publicly post or display an employee's SSN; (b) visibly print an SSN on any ID card; (c) place an SSN in files with unrestricted access; or (d) communicate an employee's personal identifying information (including SSN) to the general public.
North Carolina	N.C. Gen. Stat. § 75-62	Prohibits companies and persons from engaging in certain activities with SSNs, such as intentionally disclosing an SSN to the public; restricts the printing of SSNs on ID cards required to access products or services; restricts requiring people to transmit an SSN over the Internet unless the connection is secure or the number is encrypted.
	N.C. Gen. Stat. § 132-1.10	Prohibits government agencies from engaging in certain activities with SSNs, such as intentionally disclosing an SSN to the public or printing SSNs on ID cards required to access government services; restricts requiring people to transmit an SSN over the Internet unless the connection is secure or the number is encrypted.
North Dakota	No analogous provisions.	
Ohio	No analogous provisions.	
Oklahoma	40 Okla. Stat. § 173.1	Prohibits employers' use of SSNs, including publicly displaying SSNs, printing SSN on cards required for employees to access products or services, or requiring an employee to transmit an SSN over the Internet unless the connection is secure.
Oregon	2007 Ore. S.B. 583	Prohibits companies and persons from engaging in certain activities with SSNs, such as printing an SSN on materials not requested and mailed to a consumer or on cards required to access products or services, or publicly posting or displaying an SSN unless redacted.
Pennsylvania	74 Pa. Consol. Stat. § 201	Prohibits companies, persons and government agencies from engaging in certain activities with SSNs, such as

STATE	LAW	PURPOSE
		publicly posting SSNs; restricts the printing of SSNs on ID cards required to access products or services; prohibits requiring the transmission of an SSN over the Internet unless the connection is secure.
Rhode Island	R.I. Gen. L. § 6-48-8	Prohibits companies and persons from engaging in certain activities with SSNs, including intentionally communicating SSNs to the public; restricts the printing of SSNs on ID cards required to access products or services; prohibits requiring the transmission of an SSN over the Internet unless the connection is secure.
	R.I. Gen. L. §§ 6-13-15 *et seq*.	Restricts recording SSNs on checks given by a purchaser during a retail sale of goods or merchandise. No person shall require a consumer to disclose an SSN for the sale of consumer goods or services.
South Carolina	S.C. Code Ann. § 37-20-180	Prohibits companies and persons from engaging in certain activities with SSNs or a portion of SSNs containing six digits or more, including intentionally communicating SSNs to the public or requiring transmission of SSNs over the Internet unless the connection is secure; restricts the printing of SSNs on ID cards required to access products or services.
South Dakota	S.D. Codif. L. § 32-12-17.10; § 32-12-17.13	Prohibits the display of SSNs on driver's licenses and non-driver's identification cards.
	2008 S.D. SB 80	Prohibits state agencies from knowingly releasing or posting any person's SSN over the Internet or requiring any person to transmit his SSN over the Internet or requiring any person to use her SSN to access an Internet Web site.
Tennessee	Tenn. Code Ann. § 47-18-2110	Prohibits companies, persons and nonprofits from engaging in certain activities with SSNs, including posting or displaying SSNs in public or requiring that SSNs be transmitted over the Internet unless a secure connection is provided; restricts SSNs printed on mailed materials.

STATE	LAW	PURPOSE
Texas	Tex. Bus. & Com. Code §§ 501.051-501.053 (2007) (effective April 1, 2009)	A person may not require an individual to disclose the individual's Social Security number to obtain goods or services from or enter into a business transaction with the person unless the person: (1) adopts a privacy policy as provided by Subsection (b); (2) makes the privacy policy available to the individual; and (3) maintains under the privacy policy the confidentiality and security of the Social Security number disclosed to the person. A privacy policy adopted under this section must include: (1) how personal information is collected; (2) how and when the personal information is used; (3) how the personal information is protected; (4) who has access to the personal information; and (5) the method of disposal of the personal information.
	Tex. Bus. & Com. Code 501.001 *et seq*. [effective April 1, 2009]; Tex. Bus. & Com. Code 35.58 (2003) [repealed April 1, 2009]	Prohibits companies and persons from engaging in certain activities with SSNs, including intentionally communicating SSNs to the public; restricts the printing of SSNs on ID cards required to access products or services; prohibits requiring the transmission of SSNs over the Internet unless the connection is secure.
	Tex. Bus. & Com. Code 501.101 *et seq*. [effective April 1, 2009]; Tex. Bus. & Com. Code 35.48 (2005) [repealed April 1, 2009]	Requires businesses properly to dispose of records that contain a customer's personally identifying information, which includes SSNs.
Utah	Utah Code Ann. § 31A-21-110	Prohibits insurance companies and persons from engaging in certain activities with SSNs.
	Utah Code Ann. § 63D-2-103 (as amended by 2008 Utah L. Ch. 382 (H.B. 63) (Part I))	A governmental entity may not collect personally identifiable information (including SSNs) from a user on a governmental entity Web site unless it meets certain requirements regarding privacy policy disclosures.

STATE	LAW	PURPOSE
Vermont	9 Vt. Stat. Ann. § 2440	Prohibits companies and persons from engaging in certain activities with SSNs, including intentionally communicating SSNs to the public; restricts the printing of SSNs on ID cards required to access products or services; prohibits requiring the transmission of SSNs over the Internet unless the connection is secure.
Virginia	Va. Code Ann. § 59.1-443.2 (amended by 2008 Va. L. Ch. 562 (S.B. 133) and 2008 Va. L. Ch. 820 (H.B. 633))	Prohibits companies and persons from engaging in certain activities with SSNs, including intentionally communicating SSNs to the public; restricts the printing of SSNs on ID cards required to access products or services; prohibits requiring SSNs in order to use a Web site unless a password is also used to access the site.
Washington	No analogous provisions.	
West Virginia	No analogous provisions.	
Wisconsin	Wis. Stat. Ann. § 36.32	Prohibits the use of a student's SSN a an identification number.
Wyoming	W. Va. Code § 18-2-5f	Prohibits the use of a student's SSN as an identification number.

[a]—Treatment of SSNs in Texas Public Records

In an opinion dated February 21, 2007, the Texas Attorney General opined that the SSN of a living person is confidential and subject to mandatory exception from required disclosure under Section 552.147(a) of the Texas Public Information Act (PIA).[3] The Texas Attorney General stated, "The plain text and legislative history of Tex. Gov't Code Ann. § 552.147 . . . , coupled with numerous other state and federal statutes, all clearly protect the confidentiality of SSNs, and thereby prohibit governmental bodies from disclosing SSNs under the PIA."[4]

Noting that, "[i]n general, the PIA requires a governmental body to make its information available to a member of the public upon request," Opinion GA-519 concluded that "SSNs are made confidential

[3] Tex. Att'y Gen. Op. GA-0519 (Feb. 21, 2007), available at http://www.oag.state.tx.us/opinions/opinions/50abbott/op/2007/pdf/ga0519.pdf (last visited June 18, 2008). See Texas Public Information Act, Tex. Gov't Code Ann., § 552.147. PIA is the Texas equivalent of the federal Freedom of Information Act (FOIA), 5 U.S.C. § 552.

[4] Letter of Texas Attorney General, Greg Abbott, to The Honorable Roy Cordes (Feb. 28, 2007), abating Opinion GA-519 for sixty days.

under the PIA" and "the PIA makes mandatory that a governmental body not release the SSN of a living person to a member of the public under the PIA, unless the requestor is the holder of the SSN or the holder's authorized representative."[5] Opinion GA-519 stated "that SSNs of living persons in all county clerk records subject to the PIA are confidential and protected from disclosure under section 552.147(a)" and continued, "[c]onstruing SSNs to be confidential under the PIA affords them significant protection under the PIA. The distribution of confidential information under the PIA constitutes official misconduct and a criminal misdemeanor punishable by a fine of up to $1,000, confinement in the county jail for up to six months, or both."[6]

Texas county clerk offices responded to Opinion GA-519 with apprehension, many suspending the disclosure of public records such as those affecting property searches and public access to land records.[7] Social Security numbers are also included on other public documents affected by Opinion GA-519, such as marriage license applications, tax liens, child support liens and court abstracts.[8]

On March 28, 2007, Texas enacted a law addressing Opinion GA-519; the law states that SSNs are not confidential and permits a county or district clerk to disclose "in the ordinary course of business a social security number that is contained in information held by the clerk's office," but also requires that, unless another law requires a SSN to be maintained in a government document, the clerk redact all but the last four digits of an individual's SNN in the information maintained in the clerk's official public records.[9] The law exempts clerks from civil and criminal liability for such permissible disclosures.[10]

---

[5] Tex. Att'y Gen. Op. GA-0519 (2007), pp. 2, 7, 8, available at http://www.oag.state.tx.us/opinions/opinions/50abbott/op/2007/pdf/ga0519.pdf (last visited June 18, 2008).

[6] Tex. Att'y Gen. Op. GA-0519 (Feb. 21, 2007), p. 7, available at http://www.oag.state.tx.us/opinions/opinions/50abbott/op/2007/pdf/ga0519.pdf (last visited June 18, 2008). See Tex. Gov't Code Ann. § 552.352.

[7] See Lee, "Opinion stills flow of public records, Directive on Social Security numbers draws vocal opposition," Houston Chronicle (Feb. 28, 2007), available at http://www.chron.com/disp/story.mpl/metropolitan/4588286.html. Some clerk offices offered online access to public records, while others did not.

[8] "House votes to allow release of SS numbers," Associated Press (March 6, 2007), available at http://www.chron.com/disp/story.mpl/metropolitan/4605118.html (last visited June 18, 2008).

[9] See § 552.147(c) of PIA. Tex. H.B. 2061 was enacted on March 28, 2007, amending § 552.147 of the Texas Public Information Act. See http://www.legis.state. tx.us/BillLookup/history.aspx?LegSess=80R&Bill=HB2061 (last visited June 18, 2008).

[10] See § 552.147(d) of PIA.

§ 1.08 State Privacy Statutes

There is a growing body of state legislation that addresses the privacy and security of personal information. These statutes supplement the federal legislative scheme, and concern discrete matters such as the following.

[1]—Data Security Breach Notification

California enacted the first data security breach notification law in 2003.[1] The law requires anyone conducting business in California that maintains electronic data containing personal information to notify the individuals to whom that data pertains in the event there is a breach of security leading to the misuse of their personal information. This legislation applies to any company that conducts business in California, regardless of where the data breach occurs. The law protects an individual's personal information.[2] If such information has been or is reasonably believed to have been acquired by an unauthorized person, then the business must provide notice to such individuals.[3] If the data breach is substantial—the cost of providing notice would exceed $250,000, or the number of persons required to be notified exceeds 500,000, or the business does not have sufficient contact information—then notice may be given by e-mail, posting on the business's Web site, or notification to major statewide media.[4] In 2004, California expanded its data protection laws by requiring any person that maintains personal information to "implement and maintain reasonable security procedures and practices . . . to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."[5-6]

Since the California law was passed, most other states have enacted similar legislation. At least forty-six states, the District of Columbia, Puerto Rico, and the Virgin Islands have enacted legislation

---

[1] Cal. Civ. Code §§ 1798.29 and 1798.82 through 1798.84.

[2] Such personal information includes an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: Social Security number; driver's license number or California Identification Card number; account numbers, credit or debit card numbers in combination with any required security code, access code, or password that would permit access to an individual's financial account; medical information; and health insurance information. Cal. Civ. Code § 1798.82(e).

[3] Cal. Civ. Code § 1798.82(a).

[4] Cal. Civ. Code § 1798.82(g)(3).

[5-6] Cal. Civ. Code § 1798.81.5(b).

requiring notification of security breaches involving personal information.[7]

[2]—Social Security Numbers

A number of states have enacted statutes restricting the disclosure of Social Security numbers.[8]

[3]—Merchant Liability

Minnesota law requires merchants and retailers to delete information obtained from the magnetic strip, microprocessor chip or other device on a credit card, debit card, stored value card or other similar transaction card, within forty-eight hours after authorization of the transaction.[9] Merchants and retailers suffering a data breach involving a violation of the foregoing must reimburse financial institutions for certain costs associated with such breaches, including the costs of complying with breach notification requirements, cancellation and reissuance of credit cards affected by the breach, the opening and closing of affected accounts, and refunds to customers for unauthorized charges resulting from the breach.[10]

[4]—Information Security

Several states have enacted legislation that address a business's obligation to implement security procedures and practices to protect personal information from unauthorized access or use, and in some instances impose requirements on the destruction of data containing personal information. For example, Massachusetts authorizes a state agency to procure data security regulations.[11] The Massachusetts Office of Consumer Affairs and Business Regulations ("OCABR") promulgated regulations requiring companies to develop written information security plans and to create safeguards to protect personal electronic data.[12] Consent judgments approved by the Massachu-

---

[7] State Security Breach Notification Laws, National Conference of State Legislatures, available at http://www.ncsl.org/issuesresearch/telecommunicationsinformationtechnology/securitybreachnotificationlaws/tabid/13489/default.aspx (last visited July 15, 2011). See App. A *infra* for a complete State Summary of Data Breach Notification Laws.

[8] A discussion of these laws is set forth in § 1.07 *supra*, and specifically in § 1.07[3].

[9] Minn. Stat. Ann. § 325E.64.2.

[10] Minn. Stat. Ann. § 325E.64.3.

[11] Mass. Gen. L. Ann., Ch. 93H. For the regulations, see 201 C.M.R. 17.01 *et seq*.

[12] 201 C.M.R. 17.03.

setts courts have also implemented the same requirements under OCABR regulations.[13]

A summary of the state laws follows.

Summary of State Information Security Legislation

State	Law	Purpose
Arkansas	Ark. Code Ann. § 4-110-104 (2005) (effective Aug. 12, 2005)	A person or business shall take all reasonable steps to destroy or arrange for the destruction of a customer's records within its custody or control containing personal information that is no longer to be retained by the person or business by shredding, erasing, or otherwise modifying the personal information in the records to make it unreadable or un-decipherable through any means. A person or business that acquires, owns, or licenses personal information about an Arkansas resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information from unauthorized access, destruction, use, modification or disclosure.
California	Cal. Civ. Code § 1798.81.5(b) (effective Jan. 1, 2006)	A business that owns or licenses personal information about a California resident must implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure. A business that discloses personal information about a California resident pursuant to a

[13] On March 28, 2011, the Massachusetts Superior Court issued a Final Judgment by Consent between the Commonwealth and Briar Group, LLC that resolved allegations that Briar Group failed to take measures to protect consumer credit and debit card information. The Final Judgment stemmed from an April 2009 information security breach in which the Commonwealth alleged that unauthorized individuals accessed Briar Group's computer network and gained customer credit card information. Pursuant to the Final Judgment, Briar Group must pay a $110,000 fine, implement a written information security program and conduct annual reviews of its security measures, which are also requirements under the Office of Consumer Affairs and Business Regulations (OCABR), 201 C.M.R. §§ 17.03(1), 17.03(2)(i). See Final Judgment by Consent, Commonwealth of Massachusetts v. Briar Group, LLC, C.A. 11-1185 Commonwealth of Massachusetts Superior Court Suffolk, available at http://www.securityprivacyandthelaw.com/uploads/file/Briar%20Group%20Final%20Judgment%20by%20Consent.pdf (last visited July 15, 2011).

State	Law	Purpose
		contract with a nonaffiliated third party shall require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification or disclosure.
Connecticut	Pub. Act 08-167 (Conn. 2008) (effective Oct. 1, 2008)	Any person in possession of personal information of another person must safeguard the data, computer files and documents containing such information from misuse by third parties, and must properly dispose of, erase or make unreadable such information prior to disposal.
Maryland	Md. Code Ann. § 14-3503 (2007) (effective Jan. 1, 2008)	A business that owns or licenses personal information of an individual residing in Maryland must implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal information owned or licensed and the nature and size of the business and its operations. A business that uses a nonaffiliated third party as a service provider to perform services for the business and discloses personal information about an individual state resident under a written contract with the third party must require by contract that the third party implement and maintain reasonable security procedures and practices that: (1) Are appropriate to the nature of the personal information disclosed to the nonaffiliated third party; and (2) Are reasonably designed to help protect the personal information from unauthorized access, use, modification, disclosure or destruction.
Massachusetts	201 C.M.R. 17.00 (Mass. 2008) (effective Jan. 1, 2010)	Every person who owns, licenses, stores or maintains personal information about a Massachusetts resident must implement, maintain and monitor a comprehensive, written information security program applicable to any records containing such personal information. The comprehensive information security system must contain physical safeguards meeting certain standards to ensure the security and confidentiality of the records. At a minimum, the comprehensive information security program must: (1) designate one or more employees to maintain the program; (2) identify and assess internal and external risks and evaluate and improve the effectiveness of

State	Law	Purpose
		the current safeguards for limiting such risks; (3) develop security policies for employees that take into account whether and how employees should be allowed to keep, access and transport records containing personal information outside of the business premises; (4) impose disciplinary procedures for violations of program rules; (5) prevent employees whose jobs have been terminated from accessing records; (6) take all reasonable steps to verify that third party service providers apply and maintain safeguards for the protection of personal information; (7) limit the amount of personal information collected, the time it is retained, and the access to those persons who are reasonably required to know such information, to accomplish the legitimate purpose for which the information is collected; (8) identify which records, systems and storage media contain personal information; (9) place reasonable restrictions on access to records containing personal information; and (10) conduct ongoing review of the program, including monitoring the program, reviewing the scope of the security measures and documenting responsive actions taken. Additional requirements apply to persons who electronically store or transmit personal information. Such persons shall include in their written, comprehensive information security program the establishment and maintenance of a security system protecting their computers, including any wireless system, that, at a minimum, shall have the following elements: (1) use of secure user authentication protocols, including user IDs, assigning and controlling passwords, restricting access, and blocking access after multiple unsuccessful attempts; (2) secure access control measures that restrict access to personal information and assign unique identifiers and passwords to each person with access; (3) to the extent technically feasible, encryption of all files containing personal information that are transmitted across public networks or wirelessly; (4) reasonable monitoring of systems for unauthorized use of or access to personal information; (5) encryption of all personal information stored on laptops or other portable devices; (6) up-to-date firewall protection and operating system security patches for personal information stored on systems connected to the Internet; (7) reasonably up-to-date versions of system security agent software, including malware and virus definitions; and (8) employee training and education on the importance and purpose use of the security system.

State	Law	Purpose
Minnesota	Plastic Card Security Act Minn. Stat. Ann. § 325E.64 (2010)	No person or entity conducting business in Minnesota that accepts an access device in connection with a transaction shall retain the card security code data, the PIN verification code number, or the full contents of any track of magnetic stripe data, subsequent to the authorization of the transaction, or in the case of a PIN debit transaction, subsequent to forty-eight hours after authorization of the transaction. A person or entity is in violation of this section if its service provider retains such data subsequent to the authorization of the transaction, or in the case of a PIN debit transaction, subsequent to forty-eight hours after authorization of the transaction. The violator of this section shall reimburse the financial institution that issued any access devices affected by the violation for the expenses and damages resulting from the violation. These remedies are cumulative and shall not restrict any other right or remedy available to the financial institution.
Nevada	Nev. Rev. Stat. § 239B.030 (2005); as amended (2007) (enacted June 17, 2005, Amendment effective Jan. 1, 2008)	A person shall not include, and a governmental agency shall not require a person to include, any personal information about a person on any document that is recorded, filed or otherwise submitted to the governmental agency on or after January 1, 2007. However, if personal information about a person is required to be included in a document that is recorded, filed or otherwise submitted to a governmental agency on or after January 1, 2007, a governmental agency shall ensure that the personal information is maintained in a confidential manner and may only disclose the personal information as required to carry out a specific law. The government agency must give notice of this provision and may require a person who submits any document to the governmental agency to provide an affirmation that the document does not contain personal information or, if the document contains any such personal information, identification of the specific law, public program or grant that requires the inclusion of the personal information. A governmental agency may refuse to record, file or otherwise accept a document that does not contain such an affirmation when required or any document that contains personal information about a person that is not required to be included in the document pursuant to a specific state or federal law, for the administration of a public program or for an application for a federal or state grant. On or before January 1, 2017, each governmental agency shall ensure that any personal

State	Law	Purpose
		information contained in a document that has been recorded, filed or otherwise submitted to the governmental agency before January 1, 2007, which the governmental agency continues to hold is: (a) Maintained in a confidential manner if the personal information is required to be included in the document pursuant to a specific state or federal law, for the administration of a public program or for an application for a federal or state grant; or (b) Obliterated or otherwise removed from the document, by any method, including, without limitation, through the use of computer software, if the personal information is not required to be included in the document pursuant to a specific state or federal law, for the administration of a public program or for an application for a federal or state grant. A person may request that a governmental agency obliterate or otherwise remove from any document submitted by the person to the governmental agency before January 1, 2007, any personal information about the person contained in the document that is not required to be included in the document pursuant to a specific state or federal law, for the administration of a public program or for an application for a federal or state grant or, if the personal information is so required to be included in the document, the person may request that the governmental agency maintain the personal information in a confidential manner.
	Nevada Security of Personal Information Law Nev. Rev. Stat. § 597.970 (effective Oct. 1, 2008 (repealed), amended by Nev. S.B. 227, which amended Ch. 603A, approved May 29, 2009, and effective Jan. 1, 2010)	Amends chapter 603A of NRS by adding the following new section: 1. If a data collector doing business in Nevada accepts a payment card in connection with a sale of goods or services, the data collector shall comply with the current version of the Payment Card Industry (PCI) Data Security Standard, as adopted by the PCI Security Standards Council or its successor organization, with respect to those transactions, not later than the date for compliance set forth in the PCI Data Security Standard or by the PCI Security Standards Council or its successor organization. 2. A data collector doing business in Nevada for whom subsection 1 does not apply shall not: (a) Transfer any personal information through an electronic, nonvoice transmission other than a facsimile to a person outside of the secure system of the data collector unless the data collector uses

State	Law	Purpose
		encryption to ensure the security of the electronic transmission; or (b) Move any data storage device containing personal information beyond the logical or physical controls of the data collector or its data storage contractor unless the data collector uses encryption to ensure the security of the information. 3. A data collector shall not be liable for damages for a breach of the security of the system data if: (a) The data collector is in compliance with this section; and (b) The breach is not caused by the gross negligence or intentional misconduct of the data collector, its officers, employees or agents. 4. The requirements of this section do not apply to: (a) A telecommunication provider acting solely in the role of conveying the communications of other persons, regardless of the mode of conveyance used, including, without limitation: (1) Optical, wire line and wireless facilities; (2) Analog transmission; and (3) Digital subscriber line transmission, voice over Internet protocol and other digital transmission technology. (b) Data transmission over a secure, private communication channel for: (1) Approval or processing of negotiable instruments, electronic fund transfers or similar payment methods; or (2) Issuance of reports regarding account closures because of fraud, substantial overdrafts, abuse of automatic teller machines or related information regarding a customer.
Oregon	Ore. Rev. Stat. § 646A.622 (2007) (effective Oct. 1, 2007)	Any person that owns, maintains or otherwise possesses data that include a consumer's personal information that is used in the course of the person's business, vocation, occupation or volunteer activities must implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the personal information, including disposal of the data. The following is in compliance with the above: (a) complying with a state or federal law

State	Law	Purpose
		providing greater protection to personal information than that provided by this section; (b) complying with regulations promulgated pursuant to Title V of the Gramm-Leach-Bliley Act of 1999 (15 U.S.C. §§ 6801 to 6809) as that Act existed on October 1, 2007; (c) complying with regulations implementing the Health Insurance Portability and Accountability Act of 1996 (45 C.F.R. parts 160 and 164) as that Act existed on October 1, 2007; (d) implementing an information security program that includes the following: (1) Administrative safeguards such as the following, in which the person: (i) Designates one or more employees to coordinate the security program; (ii) Identifies reasonably foreseeable internal and external risks; (iii) Assesses the sufficiency of safeguards in place to control the identified risks; (iv) Trains and manages employees in the security program practices and procedures; (v) Selects service providers capable of maintaining appropriate safeguards, and requires those safeguards by contract; and (vi) Adjusts the security program in light of business changes or new circumstances; (2) Technical safeguards such as the following, in which the person: (i) Assesses risks in network and software design; (ii) Assesses risks in information processing, transmission and storage; (iii) Detects, prevents and responds to attacks or system failures; and (iv) Regularly tests and monitors the effectiveness of key controls, systems and procedures; and (3) Physical safeguards such as the following, in which the person: (i) Assesses risks of information storage and disposal; (ii) Detects, prevents and responds to intrusions; (iii) Protects against unauthorized access to or use of personal information during or after the collection, transportation and destruction or disposal of the information; and (iv) Disposes of personal information after it is no longer needed for business purposes or as required by local, state or federal law by burning, pulverizing, shredding or modifying a physical record and by destroying or erasing electronic media so that the information cannot be read or reconstructed.
Rhode Island	R.I. Gen. L. § 11-49.2-2 (2005) (effective March 1, 2006)	(1) A business that owns or licenses computerized unencrypted personal information about a Rhode Island resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information

State	Law	Purpose
		from unauthorized access, destruction, use, modification, or disclosure. (2) A business that discloses computerized unencrypted personal information about a Rhode Island resident pursuant to a contract with a nonaffiliated third party shall require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification or disclosure.
Utah	Utah Code Ann. § 13-44-201 (2006)	Any person who conducts business in the state and maintains personal information shall implement and maintain reasonable procedures to: (a) prevent unlawful use or disclosure of personal information collected or maintained in the regular course of business; and (b) destroy, or arrange for the destruction of, records containing personal information that are not to be retained by the person. The destruction of records shall be by: (a) shredding; (b) erasing; or (c) otherwise modifying the personal information to make the information indecipherable. This section does not apply to a financial institution as defined by 15 U.S.C. Section 6809.
Washington	Wash. Rev. Code § 19.255.020, effective July 1, 2010	Imposes liability, to a financial institution, upon processors, businesses and vendors that suffer a security breach resulting in unauthorized access to account information, but also provides for a safe harbor in certain circumstances. If a *processor* or *business* fails to take reasonable care to guard against unauthorized access to account information that is in the possession or under the control of the business or processor, and the failure is found to be the proximate cause of a breach, the processor or business is liable to a financial institution for reimbursement of reasonable actual costs related to the reissuance of credit cards and debit cards that are incurred by the financial institution to mitigate potential current or future damages to its credit card and debit card holders that reside in the state of Washington as a consequence of the breach, even if the financial institution has not suffered a physical injury in connection with the breach. In any legal action brought pursuant to this subsection, the prevailing party is entitled to recover its reasonable attorneys fees and costs incurred in connection with the legal action. A *vendor*, instead of a processor or business, is liable to a financial institution for the

State	Law	Purpose
		damages described above to the extent that the damages were proximately caused by the vendor's negligence and if the claim is not limited or foreclosed by another provision of law or by a contract to which the financial institution is a party. Processors, businesses, and vendors are *not* liable under this section if (a) the account information was encrypted at the time of the breach, or (b) the processor, business, or vendor was certified compliant with the payment card industry data security standards adopted by the payment card industry security standards council, and in force at the time of the breach. A processor, business, or vendor will be considered compliant, if its payment card industry data security compliance was validated by an annual security assessment, and if this assessment took place no more than one year prior to the time of the breach. *Account information* means: (i) The full, unencrypted magnetic stripe of a credit card or debit card; (ii) the full, unencrypted account information contained on an identification device as defined under Washington law; or (iii) the unencrypted primary account number on a credit card or debit card or identification device, plus any of the following if not encrypted: cardholder name, expiration date, or service code.

[a]—Statutes Requiring Compliance with Technical Standards

Minnesota. The Minnesota Plastic Card Security Act requires businesses that use an "access device" in connection with a payment card (e.g., credit card, debit card, stored value card) transaction to delete, after the authorization of the transaction or, in the case of a PIN debit transaction, after forty-eight hours after authorization of the transaction, the card security code data, the PIN verification code number, and the contents of any track of magnetic stripe data.[14] These requirements effectively codify a key component of the Payment Card Industry (PCI) Data Security Standard,[15] which specifically prohibits

[14] Minn. Stat. Ann. § 325E.64 (2010).

[15] The Payment Card Industry (PCI) Security Standards Council is an industry forum responsible for the development and management of payment card industry

companies from storing on their systems card data such as the full contents of the magnetic stripe on the back of a card or the three- and four-digit verification codes.

A person who violates this law is liable to the financial institution that issued the access device for:

(1) the costs of the reasonable actions undertaken by the financial institution as a result of the breach in order to protect the information of its cardholders or to continue to provide services to its cardholders, as well as

(2) the costs for damages paid by the financial institution to cardholders injured by the violation.

The law expressly grants the financial institution the right to bring a private cause of action against the violator of the law.

Nevada. The Nevada Security of Personal Information Law expressly requires businesses that handle payment card transactions to comply with the Payment Card Industry (PCI) Data Security Standard.[16] Whereas several state laws direct organizations in certain industries to consider using encryption or to make encryption a factor in decisions regarding breach notifications, the Nevada law requires encryption of personal information in certain contexts, and compliance with a specific industry standard, the Payment Card Industry (PCI) Data Security Standard.

Washington. Amending Washington's data security breach notification law, House Bill 1149 was passed March 22, 2010, and became effective July 1, 2010, and imposes liability on "processors, businesses and vendors" to a financial institution in certain circumstances for security breaches resulting in unauthorized access to "account information," but also provides a safe harbor if:

(1) the account information was encrypted at the time of the breach, or

---

[16] The Nevada data security law mandating encryption for the transmission of customer personal information became effective October 1, 2008, and was thereafter repealed. See Nev. Rev. Stat. § 597.970. The new law became effective January 1, 2010, and requires any data collector doing business in Nevada who accepts a payment card to comply with the current version of the Payment Card Industry (PCI) Data Security Standard, as adopted by the PCI Security Standards Council. See http://www.leg.state.nv.us/Statutes/75th2009/Stats200916.html#Stats200916page1604 (last visited June 26, 2011).

(2) the business was certified compliant with the payment card industry data security standards adopted by the payment card industry security standards council, and in force at the time of the breach.[17]

"Account information" includes (i) The full, unencrypted magnetic stripe of a credit card or debit card; (ii) the full, unencrypted account information contained on an identification device; or (iii) the unencrypted primary account number on a credit card or debit card or identification device, plus any of the following if not encrypted, cardholder name, expiration date or service code.

[b]—Statutes Requiring Encryption

Massachusetts. Massachusetts's data protection law requires "encryption of all transmitted records and files containing personal information that will travel across public networks" and "of all data containing personal information to be transmitted wirelessly" as well as the creation of a written information security plan (WISP) that must be filed with the state of Massachusetts. The law also includes fines for data compromises—$5,000 per breach or lost record.

[c]—Statutes Requiring Businesses to Identify Personal Information They Disclose for Direct Marketing Purposes

Some states require businesses to disclose to customers, in writing or by electronic mail, the types of personal information they share with or sell to a third party for direct marketing purposes or for compensation.

California. Under California law,[18] a business that has an established business relationship with a customer, and has within the last calendar year disclosed personal information to third parties that the business knows or reasonably should know use the personal information for direct marketing purposes, "shall designate a mailing address, electronic mail address, or, if the business chooses to receive requests by telephone or facsimile, a toll-free telephone or facsimile number, to which customers may deliver

---

[17] Wash. Rev. Code § 19.255.020 (2010). See explanation in the Summary of State Information Security Legislation table in this § 1.08[4].

[18] Cal. Civ. Code §§ 1798.83 to 1798.84.

requests" regarding the disclosure of such information.[19] A business may either add to the home page of its Web site a link to a page titled "Your Privacy Rights" or add the words "Your Privacy Rights" to the home page's link to the business's privacy policy. The first page of the link shall describe a customer's rights to request the aforesaid information and shall provide the designated mailing address, e-mail address, as required, or toll-free telephone number or facsimile number, as appropriate.[20] Businesses may post a privacy statement that gives customers the opportunity to elect not to share personal information at no cost.[21]

Upon receipt of a request by a customer, a business will provide the customer in writing or by e-mail, free of charge, a list of the categories of personal information disclosed by the business to third parties for the third parties' direct marketing purposes during the immediately preceding calendar year, the names of the third parties that received such personal information, and, if the nature of the third parties' business cannot reasonably be determined from the third parties' names, examples of the products or services marketed, if known to the business, sufficient to give the customer a reasonable indication of the nature of the third parties' business.[22]

Personal information is defined under the law and includes, among other things, an individual's name and address, e-mail address, age or date of birth, information about children, height and weight, race, religion, occupation, telephone number, education, the kind of product the customer purchased, leased, or rented, Social Security number, bank account, credit card or debit card number.[23] The law provides for a private cause of action and statutory damages of $500 for each violation or $3,000 for each willful, intentional or reckless violation.[24]

Utah. The Utah Notice of Intent to Sell Nonpublic Personal Information Act[25] requires a commercial entity to provide notice to a person if the entity enters into a consumer transaction with the person and obtains nonpublic personal information concerning the person that the entity intends to or wants the ability to disclose to a third party for compensation.[26]

---

[19] Cal. Civ. Code § 1798.83(a) and (b).
[20] Cal. Civ. Code § 1798.83(b)(1)(B).
[21] Cal. Civ. Code § 1798.83(c)(2).
[22] Cal. Civ. Code § 1798.83(a).
[23] Cal. Civ. Code § 1798.83(e)(7).
[24] Cal. Civ. Code § 1798.84.
[25] Utah Code Ann. §§ 13-37-101, 102, 201-203.
[26] Utah Code Ann. §§ 13-37-201(1).

Notice must be given before the earlier of (a) the point at which the person is requested to provide the nonpublic personal information, or (b) the point at which the commercial entity otherwise obtains the nonpublic personal information as a result of the consumer transaction.[27] The notice shall read substantially as follows: "We may choose to disclose nonpublic personal information about you, the consumer, to a third party for compensation."[28] The notice may be made orally, if the consumer transaction itself is entirely conducted orally, or in writing, if the notice is written in dark bold, and shall be sufficiently conspicuous so that a reasonable person would perceive the notice before providing the nonpublic personal information.[29] The law provides for a private cause of action and statutory damages of $500 for each violation.[30]

[d]—Statutes Regulating Internet Service Providers[31]

Some states have enacted privacy legislation that applies to Internet service providers (ISPs) in the provision of services to consumers in the state.

Minnesota. The Minnesota Internet Privacy law[32] requires ISPs to (i) "take reasonable steps to maintain the security and privacy of a consumer's personally identifiable information" and to (ii) "not knowingly disclose personally identifiable information (PII) concerning a consumer of the Internet service provider" except as otherwise permitted by the Act.[33] The law permits an ISP to disclose PII in certain circumstances, including pursuant to a subpoena, warrant or court order, to an investigative or law enforcement officer while acting as authorized by law, in the ordinary course of business, and to another ISP for purposes of reporting or preventing violations of the published acceptable use policy or customer service agreement of the ISP, but the recipient may further disclose the PII only as provided by the law.[34] A consumer who prevails or substantially prevails in an action brought under the law may

---

[27] Utah Code Ann. § 13-37-201(2).
[28] Utah Code Ann. § 13-37-201(3).
[29] Utah Code Ann. § 13-37-201(3).
[30] Utah Code Ann. § 13-37-203.
[31] See generally, § 6.03 *infra*.
[32] Minn. Stat. Ann. § 325M.
[33] Minn. Stat. Ann. §§ 325M.02, 325M.05.
[34] Minn. Stat. Ann. §§ 325M.03, 325M.04.

recover the greater of $500 or actual damages, and may recover costs, disbursements and reasonable attorney fees.[35]

Nevada. Nevada law[36] requires a provider of Internet service to keep confidential (i) all "information concerning a subscriber, other than the electronic mail address of the subscriber, unless the subscriber gives permission, in writing or by electronic mail, to the provider of Internet service to disclose the information" and (ii) the "electronic mail address of a subscriber, if the subscriber requests, in writing or by electronic mail, to have the electronic mail address of the subscriber kept confidential."[37] A violation of the law is a misdemeanor and subject to a fine of not less than $50 or more than $500 for each violation.[38]

[5]—Financial Law

California enacted legislation intended to provide consumers greater protection than that afforded by the federal Gramm-Leach-Bliley Act.[39] The California Financial Privacy Act (popularly known as SB1) requires, generally, that a consumer (1) "opt in" before a financial institution may share nonpublic personal information with a nonaffiliated third party, and (2) be given the opportunity to "opt out" of sharing nonpublic personal information with the financial institution's financial marketing partners or with the financial institution's *affiliates*, with certain exceptions.[40]

[6]—Statutes Affecting Employment and Social Media

At least one state has enacted legislation prohibiting an employer from requesting or requiring that an employee or job applicant disclose personal account (including social media) log-in information in connection with his or her employment or application for employment.[41] Similar legislation has been introduced in other states.

---

[35] Minn. Stat. Ann. § 325M.07.
[36] Nev. Rev. Stat. § 205.498.
[37] Nev. Rev. Stat. § 205.498(1).
[38] Nev. Rev. Stat. § 205.498(3).
[39] See § 3.15 N. 1 *infra*.
[40] California SB1 is discussed in greater detail in § 3.15 *infra*.
[41] User Name and Password Privacy Protection and Exclusions, Md. Code Ann. Ch. 234, § 3-712, signed into law May 2, 2012, effective Oct. 1, 2012. The law is an amendment to the Maryland Labor and Employment Law. It states: "an employer may not request or require that an employee or applicant disclose any user name, password, or other means for accessing a personal account or service through an electronic communications device." Md. Code Ann. § 3-712(B)(1). "Electronic communications device is "any device that uses electronic signals to create, transmit, and receive information." Md. Code Ann. § 3-712(A)(3)(I).