


# Privacy Protections for Personal Information Online

**Gina Stevens**
Legislative Attorney

April 6, 2011

**Congressional Research Service**
7-5700
www.crs.gov
R41756

**CRS Report for Congress**
*Prepared for Members and Committees of Congress*

c11173008

# Summary

There is no comprehensive federal privacy statute that protects personal information. Instead, a patchwork of federal laws and regulations govern the collection and disclosure of personal information and has been addressed by Congress on a sector-by-sector basis. Federal laws and regulations extend protection to consumer credit reports, electronic communications, federal agency records, education records, bank records, cable subscriber information, video rental records, motor vehicle records, health information, telecommunications subscriber information, children's online information, and customer financial information. Some contend that this patchwork of laws and regulations is insufficient to meet the demands of today's technology. Congress, the Obama Administration, businesses, public interest groups, and citizens are all involved in the discussion of privacy solutions. This report examines some of those efforts with respect to the protection of personal information. This report provides a brief overview of selected recent developments in the area of federal privacy law. This report does not cover workplace privacy laws or state privacy laws.

For information on access to electronic communications, see CRS Report R41733, *Privacy: An Overview of the Electronic Communications Privacy Act*, by Charles Doyle.

# Contents

Background ..... 1
Federal Legal Framework for the Privacy of Online Personal Information ..... 5
Constitutional Protections ..... 5
Statutory Protections ..... 7
The Federal Trade Commission ..... 8
FTC Enforcement Actions Concerning the Privacy of Personal Information ..... 8
Recent Policy Initiatives ..... 9
Electronic Communications Privacy Act Reform ..... 11

## Contacts

Author Contact Information ..... 12

GalleryWatch.com
http://www.crsdocuments.com
Penny Hill Press

# Background

The collection and use of personal information by websites, Internet service providers, direct marketers, data brokers, network advertisers, law enforcement entities, and others has raised privacy concerns.[1] Personal information is readily available because of the widespread usage of the Internet and of cloud computing, the availability of inexpensive computer storage, and increased disclosures of personal information by Internet users in participatory Web 2.0 technologies.[2] The increased availability of online personal information has fueled the creation of a new tracking industry.[3] Behavioral advertising, a form of online advertising, is delivered based on consumer preferences or interest as inferred from data about online activities. In 2010, over $22 billion was spent on online advertising.[4] This revenue allows websites to offer content and services for free. *What They Know*, an in-depth investigative series by the Wall Street Journal, found that one of the fastest growing Internet business models is of data-gatherers engaged in "intensive surveillance of people [visiting websites] to sell data about, and predictions of, their interests and activities, in real time."[5] Websites such as Spokeo, an online data aggregator and broker, give site visitors vast quantities of personal information.[6] Congress is examining the use

[1] For a description of how personal information is collected and how it is used, see Report of the New York State Bar Association's Task Force on Privacy 30-38, (April 4, 2009) available at http://www.nysba.org/AM/Template.cfm?Section=Home&TEMPLATE=/CM/ContentDisplay.cfm&CONTENTID=26006.

[2] Jacqueline D. Lipton, *Mapping Online Privacy*, 140 N.W. U. L Rev. 477, 481-82 (2010)

> Web 2.0 involves more voices than previous Internet technologies. Blogs, wikis, online social networks, and massively multiplayer online games allow more people to communicate more information than ever before, both about themselves and about others—sometimes deliberately, and sometimes incidentally. This proliferation of new technologies raises a whole host of privacy concerns differing in nature and scope from what has gone before. Earlier Internet privacy concerns related predominantly to the aggregation of personal information to create large-scale, text-based digital dossiers about individuals. These concerns were addressed—to the extent they were addressed at all—by laws aimed at regulating the aggregation and use of such dossiers by governments and corporate entities.
>
> Web 2.0 raises new challenges for privacy. With more voices online, there is a wider scope for privacy invasion. With more recording technologies readily at hand—such as cell phone cameras and text messaging services like Twitter—there is a wider scope for incidental gathering of details of people's private lives that can be uploaded and disseminated globally at the push of a button. Because of these developments, the boundaries between the public and private spheres are breaking down, or at least becoming more difficult to discern. Thus, any privacy laws premised on now-dated conceptions of a "reasonable expectation of privacy" are becoming more difficult to apply. (citations omitted)

[3] See CRS Report RL34693, *Online Data Collection and Disclosure to Private Entities: Selected Federal Laws and Self-Regulatory Regimes*, by Kathleen Ann Ruane.

[4] CRS Report R40908, *Advertising Industry in the Digital Age*, by Suzanne M. Kirchhoff.

[5] Julia Angwin & Tom McGinty, *Sites Feed Personal Details to New Tracking Industry*, Wall St. J., July 30, 2010, available at http://online.wsj.com/article/SB10001424052748703977004575393173432219064.html (discussing a Wall Street Journal study that found that the 50 largest U.S. websites on average installed 64 tracking devices onto the computers of visitors, usually with no warning; a dozen such sites each installed over 100 pieces of tracking technology); *What They Know Series*, The Wall Street Journal, July 31, 2010, available at http://online.wsj.com/public/page/what-they-know-digital-privacy.html (WSJ series documents the use of Internet-tracking technology and privacy implications for consumers).

[6] Spokeo is a "people search engine that organizes vast quantities of white-pages listings, social information, and other people-related data from a large variety of public sources." http://www.spokeo.com; see also John Brandon, "Spokeo a Growing Threat to Internet Privacy, Cyber Security Experts Warn," ("The popular information-gathering website offers a multitude of options for finding information about anyone. It purports to know your income, religion, spouse's name, (continued...)

of new technologies (such as flash cookies),[7] and the privacy practices of the 15 websites identified as installing the most tracking technology on their visitors' computers.[8] Consumers and public interest groups are filing complaints to challenge the collection and use of consumer data without consumer consent or knowledge.[9] Online privacy[10] concerns are widespread.[11]

Stakeholders routinely acknowledge that the continued success of electronic commerce depends upon the resolution of issues related to the privacy and security of online personal information.[12] The U.S. Department of Commerce recently reiterated that the large-scale collection, analysis, and storage of personal information is central to the Internet economy; and that regulation of online personal information must not impede commerce. The Commerce Department's report on Commercial Data Privacy calls on Congress to create a "privacy bill of rights,"[13] and concludes

(...continued)

credit status and the number of people in your household. It even offers a satellite shot of your house, complete with an estimated value."), available at http://www.foxnews.com/scitech/2011/01/19/spokeo-cyber-security-warn-threat-privacy/; see also *In the Matter of Spokeo, Inc.* (The Center for Democracy and Technology petitioned the Federal Trade Commission to investigate the business practices of Spokeo alleging that Spokeo's provision of detailed consumer reports violates the Fair Credit Reporting Act, and is an unfair and deceptive practice in violation of Section 5 of the Federal Trade Commission Act), available at http://www.cdt.org/files/pdfs/Spokeo.pdf.

[7] "A Flash cookie, or a Flash local shared object, is a data file that is stored on a consumer's computer by a website that uses Adobe's Flash player technology. Like a regular http cookie, a Flash cookie can store information about a consumer's online activities. Unlike regular cookies, Flash cookies are stored in an area not controlled by the browser. Thus, when a consumer deletes or clears the cookies from his browser using tools provided through the browser, this may not delete Flash cookies stored on his computer." FTC Staff Report, A Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers 16, n. 38 (Dec. 1, 2010), available at http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

[8] Letter from Representatives E. Markey and Barton, Co-Chairs, House Bi-partisan Privacy Caucus, to Brian L. Roberts, Chairman and CEO, Comcast Corporation, August 5, 2010, http://markey.house.gov/docs/letter_-_edge_providers_-_comcast_-_8-5-10.pdf.

[9] Lalo v. Apple Inc., Backflip, Dictionary.com, Pandora, Inc., The Weather Channel, No. CV10-5878 (D. N.D. Ca. filed Dec. 23, 2010) (class action complaint on behalf of iPhone and iPad users alleging that some of the applications downloaded from the Apple-sponsored website submitted their personal identifying information to advertising networks without obtaining their consent in violation of privacy and consumer protection); Rodimer et al. v. Apple, Inc., et. al. No. CV11-0700 (D. N.D. Ca. filed Feb. 15, 2011) (complaint alleges defendants gained unauthorized access and use of plaintiffs mobile devices in order to collect, monitor, and remotely store electronic data there from).

[10] The term "online privacy" includes several different subjects such as government surveillance of online activities, the rights of employers to monitor employee activities, the collection, use, and dissemination of data via the Internet, and computer security issues. This report focuses on one aspect of online privacy – collection, use, and dissemination of data via the Internet.

[11] U.S. Congress, Senate Committee on Commerce, Science, and Transportation, *The State of Online Consumer Privacy*, 112th Cong., 1st sess., March 16, 2011 (statement of Chairman Rockefeller recognized that "[o]nline privacy is a matter that concerns Americans everywhere. According to the Pew Internet and American Life Project, 96 percent of working Americans use the Internet as part of their daily life. We are increasingly plugged-in and logged-on: working, playing, learning, shopping and socializing using computers, smart phones and tablets. And every time we use a device, such as an Android or iPad, to interact online, a machine—a computer server—somewhere in the world is recording this information. Much of this information is used for targeted advertising purposes, but not all of it….Worse, even when Americans are aware this is happening, too often there is little they can do to stop it….I believe that consumers should be able to clearly understand and control what information is being collected and how this information is being used…."), available at http://commerce.senate.gov/public/index.cfm?p=Hearings&ContentRecord_id=e018f33b-d047-4fba-b727-5513c66a6887&ContentType_id=14f995b9-dfa5-407a-9d35-56cc7152a7ed&Group_id=b06c39af-e033-4cba-9221-de668ca1978a&MonthDisplay=3&YearDisplay=2011.

[12] Data security is beyond the scope of this report and is discussed in CRS Report RL34120, *Federal Information Security and Data Breach Notification Laws*, by Gina Stevens.

[13] *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*, available at http://www.commerce.gov/sites/default/files/documents/2010/december/iptf-privacy-green-paper.pdf.

that privacy policies are now widely viewed as ineffective for the protection of personal information.[14] A recent Federal Trade Commission (FTC) Staff Report recommended implementation, either through legislation or self-regulation, of a Do Not Track system to allow consumers to opt out of online tracking or advertising.[15] Developers, organizations, and businesses are voluntarily working on ways to allow users to opt out of behavior advertising.[16]

The U.S. Congress continues to examine the federal legal framework that protects personal information. Historically, Congress has played a major role in protecting personal information online. Beginning in the late 1990s, Congress passed laws aimed at specific online harms and amended existing laws to reflect the ways in which technology was being used to collect, use, and share personal information. Beginning with the 109th Congress, every Congress has held numerous privacy-related hearings. The current Congressional privacy agenda is broad and includes items that Congress has worked on for several years,[17] new issues posed by advances in technology,[18] and items related to efforts to update the electronic surveillance laws for advances in technology.[19]

Reportedly, several Members in the 112th Congress plan to introduce or reintroduce substantive privacy legislation. Online consumer privacy is an issue that is at the forefront of the Senate Commerce Committee's agenda, and it is a top priority for Chairman Rockefeller. Senator Kerry, Chairman of the Commerce Subcommittee on Communications, Technology and the Internet, along with Senator McCain, intend to introduce a privacy bill similar to the Obama Administration's legislative framework.[20] Representative Rush reintroduced a comprehensive privacy bill, H.R. 611, to require businesses to disclose details about their data-collection practices and allow consumers to make choices about such activities. Representative Stearns announced that he had drafted a consumer privacy bill with a provision to establish an FTC-approved self-regulatory program.[21] The House Energy and Commerce Subcommittee on Commerce, Manufacturing, and Trade Chair Bono Mack said that the subcommittee will examine

---

[14] *Id.*; For a legal discussion of "terms of use" and "privacy policies", see Report of the New York State Bar, *supra* note 1, at 38-49 ("Terms of Use ("TOU") policies govern the relationship between the company that owns the website and the users of the company's website ("Users") and specifies what the company expects from Users as well as what Users can expect from the company's website. TOU include information on the website owner's Privacy Policy, usually as a link. A Privacy Policy is a written description on a specific website explaining to the public how the company that owns the website applies specific fair information practices to the collection, use, storage, and dissemination of personal information provided by Users.).

[15] A Preliminary Federal Trade Commission Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers (Dec. 1, 2010), available at http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

[16] Browser developers, including Mozilla and Microsoft, have announced plans to build do-not-track options for online behavioral advertising into their new browsers. The Digital Advertising Alliance has developed self-regulatory guidelines and an opt-out mechanism for behavioral advertising, *See*, "Welcome to the online home of the Self-Regulatory Program for Online Behavioral Advertising." http://www.aboutads.info/. In addition, Google reportedly has developed a browser add-on that can be used to block targeted advertisements.

[17] *E.g.* data security and breach notification.

[18] *E.g.* online behavioral advertising.

[19] *E.g.* social networking, cloud computing, location-based applications, mobile applications.

[20] Christopher Wolf, Chronicle of Data Protection, *Draft "Commercial Privacy Bill of Rights Act of 2011" Published*, (March 23, 2011), available at http://www.hldataprotection.com/2011/03/articles/consumer-privacy/draft-commercial-privacy-bill-of-rights-act-of-2011-published/.

[21] "Stearns Outlines Goals and Major Provisions of Hs Draft Privacy Legislation," (March 16, 2011), available at https://stearns.house.gov/News/DocumentSingle.aspx?DocumentID=227408.

online privacy issues in hearings.[22] Senate Judiciary Chairman Leahy has a long-standing interest in privacy, and his committee has several initiatives underway.[23] A new Senate Committee on the Judiciary Subcommittee on Privacy, Technology and the Law was created in the 112th Congress with jurisdiction covering oversight of laws and policies governing the collection, protection, use, and dissemination of commercial information by the private sector, including online behavioral advertising, privacy within social networking websites, and other online privacy issues.[24] Senator Wyden has also announced plans to draft a bill to clarify what legal standards law enforcers and intelligence agents must satisfy before tracking an individual's physical movements using geolocation data generated by a mobile device.[25]

Important policy questions include whether Congress should draft legislation tailored to specific privacy threats (such as online behavioral advertising) or whether a broader, comprehensive federal privacy law is desirable. There is a growing consensus among stakeholders that basic privacy rules are necessary. However, consensus is lacking about the elements of a federal privacy law: what types of information it should cover (personal identifying information or more general information that is associated with a computer or device); how far it should reach; whether it should cover data collection or merely use; and who should be able to enforce it. One legal scholar posits that

> [i]t may be helpful to pull back the lens and see if it is possible to create a larger-scale outline of privacy. This broader perspective may help to illuminate the constituent elements of a privacy incursion, and the interrelationships between those elements. In this context, . . [there are] six discrete aspects of privacy relating to: (1) actors–relationships; (2) conduct; (3) motivations; (4) harms–remedies; (5) nature of information; and (6) format of information.[26]

Businesses view U.S. sector-by-sector regulation of personal information as an impediment to commerce and seek simplification. For example, Microsoft recommends a multi- pronged approach to the protection of individuals' privacy that includes legislation, industry self-regulation, technology tools, and consumer education.[27] Three principles—transparency, control, and security—underpin Microsoft's approach to privacy. Under this approach, privacy protections would not be specific to any one technology, industry, or business model; would apply across sectors; would provide consistent baseline protections for consumers; and would simplify compliance. In addition, privacy legislation would preempt state laws that are inconsistent with federal policy.

[22] "Bono Mack Says Online Privacy Issues Should Be Examined Carefully," (March 17, 2011), available at http://bono.house.gov/News/DocumentSingle.aspx?DocumentID=229899.

[23] Letter from Senators Franken, Schumer, Whitehouse, and Blumenthal, S. Comm. on the Judiciary, to Mr. Marck Zuckerberg, CEO, Facebook, March 9, 2011 (Committee urged Facebook to reconsider its "plan to allow application developers to request and obtain Facebook users' mobile phone numbers and home addresses").

[24] See http://judiciary.senate.gov/about/subcommittees/privacytechnology.cfm.

[25] *Sen. Wyden Drafts Measure To Protect Geolocation Data*, 16 BNA Electronic Comm. & L. Rep. 154, available at http://pub.bna.com/eclr/wydraftbill.pdf.

[26] Jacqueline D. Lipton, *Mapping Online Privacy*, 140 N.W.U. L. Rev. 477, 481-82 (2010), available at http://www.law.northwestern.edu/lawreview/v104/n2/477/LR104n2Lipton.pdf.

[27] Http://commerce.senate.gov/public/?a=Files.Serve&File_id=f8eb430d-c017-4ca1-b7e7-c2f7ec240c67 pp. 4-5.

# Federal Legal Framework for the Privacy of Online Personal Information

At the end of the 19th century, a seminal law review article was published that developed the basic principle of American privacy law—the "right to be let alone."[28] The article was written in response to invasions of personal privacy caused by the technological innovations of mass printing (newspapers) and the portable camera (photographs). Following this article, American common law jurisprudence developed four distinct tort remedies to protect personal privacy: false light, misappropriation, public disclosure of private facts, and intrusion upon seclusion.[29] With the late 20th century technological innovations of the Internet and the World Wide Web, the collection, use, and dissemination of electronic personal information is potentially much more invasive. As noted above, the right to privacy has long been characterized as the "the right to be let alone."[30] And yet, today the more practical view may be that "[i]n the digital era, privacy is no longer about being 'let alone.' Privacy is about knowing what data is being collected and what is happening to it, having choices about how it is collected and used, and being confident that it is secure."[31]

Some advocate the expansion of this concept to include the right to "information privacy" for online transactions and personally identifiable information.[32] The term "information privacy" refers to an individual's claim to control the terms under which "personal information"—information that can be linked to an individual or distinct group of individuals (e.g., a household)—is acquired, disclosed, and used.[33] Others urge the construction of a market for personal information, to be viewed no differently than other commodities in the market.[34]

## Constitutional Protections

In the United States there is no comprehensive legal protection for personal information. The Constitution protects the privacy of personal information in a limited number of ways, and extends only to the protection of the individual against government intrusions. Constitutional guarantees are not applicable unless "state action" has taken place. Many of the threats to the privacy of personal information addressed in this report occur in the private sector, and are unlikely to meet the requirements of the "state action" doctrine. As a result, any limitations placed

[28] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv.L.Rev. 193 (1890).

[29] David A. Elder, *The Law of Privacy* (Rochester, NY: Lawyers Cooperative Publishing, 1991).

[30] *Olmstead v. United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

[31] Testimony of Mr. Erich Anderson, Deputy General Counsel of Microsoft Corporation, *The State of Online Consumer Privacy, Hearing before S. Comm. on Commerce, Science, and Transportation*, 112th Cong., (2011)(hereinafter Microsoft testimony), available at http://commerce.senate.gov/public/?a=Files.Serve&File_id=f8eb430d-c017-4ca1-b7e7-c2f7ec240c67.

[32] See, Joel R. Reidenberg, Privacy in the Information Economy: A Fortress or Frontier for Individual Rights? 44 Fed. Comm. L.J. 195 (1992).

[33] See, U.S. Govt. Information Infrastructure Task Force, Information Policy Committee, Privacy Working Group, Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information, Commentary ¶ 2 (1995).

[34] See, Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 Stanford L. Rev. 1193, 1201 (1998).

on the data collection activities of the private sector will be found not in the federal Constitution but in federal or state statutory law or common law.

The federal Constitution makes no explicit mention of a "right of privacy," and the "zones of privacy" recognized by the Supreme Court are very limited. The Fourth Amendment search-and-seizure provision protects a right of privacy by requiring warrants before government may invade one's internal space or by requiring that warrantless invasions be reasonable.[35] However, "the 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."[36] Similarly, the Fifth Amendment's self-incrimination clause was once thought of as a source of protection from governmental compulsion to reveal one's private papers,[37] but the Court has refused to interpret the self-incrimination clause as a source of privacy protection.[38]

In *Whalen v. Roe*,[39] the Supreme Court recognized an implicit constitutional "right of informational privacy." *Whalen* concerned a New York law that created a centralized state computer file of the names and addresses of all persons who obtained medicines containing narcotics pursuant to a doctor's prescription. Although the Court upheld the state's authority, it found this gathering of information to affect two interests. The first was an "individual interest in avoiding disclosure of personal matters"; the other, "the interest in independence in making certain kinds of important decisions."[40] These two interests rest on the substantive due process protections found in the Fifth and Fourteenth Amendments.

More recently, the Court appeared to reiterate its recognition of a constitutional right to information privacy when it rejected 8-0 the National Aeronautics and Space Administration (NASA) contract workers' contentions that NASA violated their privacy rights under the U.S.[41] Constitution by requiring them to answer questions about their drug treatment and asking their references whether they have any reason to question the individual's honesty or trustworthiness. Justice Samuel A. Alito, writing for the Court, said it was not necessary for the Court to decide whether NASA's questions about contract workers at the agency's Jet Propulsion Laboratory implicated privacy interests of "constitutional significance" because it was clear that any such constitutional interest, if it exists, did not prevent the government from taking reasonable steps that served legitimate government interests and gave the employees substantial protection against public disclosure of their personal information. Citing the Privacy Act's requirements that the government limit disclosure of information about the Jet Propulsion Lab (JPL) contract employees and the government's long-standing use of pre-employment investigations of federal job applicants, the court concluded "that the Government's inquiries do not violate a constitutional right to informational privacy."

---

[35] CRS Report R41663, *Law Enforcement Use of Global Positioning (GPS) Devices to Monitor Motor Vehicles: Fourth Amendment Considerations*, by Alison M. Smith.

[36] *Katz v. United States*, 389 U.S. 347, 350 (1967).

[37] *Boyd v. United States*, 116 U.S. 616, 627-630 (1886).

[38] *Fisher v. United States*, 425 U.S. 391, 399 (1976).

[39] 429 U.S. 589 (1977).

[40] *Id.* at 592-93.

[41] 131 S. Ct. 746 (2011).

## Statutory Protections

A patchwork of federal and state laws exists to protect the privacy of certain personal information. There is no comprehensive federal privacy statute that protects personal information held by both the public sector and the private sector. This report does not address state privacy laws. The private sector's collection and disclosure of personal information has been addressed by Congress on a sector-by-sector basis. Federal laws and regulations extend protection to consumer credit reports,[42] electronic communications,[43] federal agency records,[44] education records,[45] bank records,[46] cable subscriber information,[47] video rental records,[48] motor vehicle records,[49] health information,[50] telecommunications subscriber information, children's online information,[51] and customer financial information. [52]

---

[42] 15 U.S.C. 1681 – 81t. The Fair Credit Reporting Act of 1970 (FCRA), as amended by the Fair and Accurate Credit Transactions Act of 2003, 15 U.S.C.1681 – 81t, sets forth rights for individuals and responsibilities for consumer "credit reporting agencies" in connection with the preparation and dissemination of personal information in a consumer report. Under the FCRA consumer reporting agencies are prohibited from disclosing consumer reports to anyone who does not have a permissible purpose.

[43] 18 U.S.C. 2510-2522, 2701-2711, 3121-3126. The Electronic Communications Privacy Act of 1986 (ECPA), outlaws electronic surveillance, possession of electronic surveillance equipment, and use of information secured through electronic surveillance. The ECPA regulates stored wire and electronic communications (such as voice mail or electronic mail), transactional records access, pen registers, and trap and trace devices. The ECPA prohibits unauthorized access to stored electronic communications and prohibits the 'provider of an electronic communication service' from disclosing the contents of a communication it stores or transmits. The ECPA also limits a provider's disclosure of transactional data to the government, but not to private parties.

[44] 5 U.S.C. 552a. The Privacy Act of 1974, 5 U.S.C. 552a, places limitations on the collection, use, and dissemination of information about an individual maintained by federal agencies. Agencies may not disclose any record regarding an individual, except pursuant to a written request by, or with the prior written consent of, the record subject. The act allows most individuals to seek access to records about themselves, and requires that personal information in agency files be accurate, complete, relevant, and timely. The subject of a record may challenge a record's accuracy.

[45] 20 U.S.C. 1232g. The Family Educational Rights and Privacy Act of 1974 (FERPA), 20 U.S.C. 1232g, governs access to and disclosure of educational records to parents, students, and third parties.

[46] 12 U.S.C 3401. The Right to Financial Privacy Act of 1978, restricts the ability of the federal government to obtain bank records from financial institutions, and sets forth procedures for the federal government's access to bank customer records.

[47] 47 U.S.C. 551. The Cable Communications Policy Act of 1984, 47 U.S.C. 551, limits the disclosure of cable television subscriber names, addresses, and utilization information for mail solicitation purposes.

[48] 18 U.S.C. 2710. The Video Privacy Protection Act of 1988,18 U.S.C. 2710, regulates the treatment of personal information collected in connection with video sales and rentals.

[49] 18 U.S.C. 2721. The Driver's Privacy Protection Act of 1994, 18 U.S.C. 2721, regulates the use and disclosure of personal information from state motor vehicle records.

[50] 42 U.S.C. 1320d note. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) (P.L. 104-191). The HIPAA Privacy Rule was adopted as the national standard for the protection of individually identifiable health information. The HIPAA Privacy Rule applies to protected health information (PHI) and limits the circumstances under which an individual's PHI may be used or disclosed by covered entities. Enhanced HIPAA penalties and breach notification provisions for protected health information were included in the Health Information Technology for Economic and Clinical Health Act of 2009.

[51] 47 U.S.C. 222. Communications Act of 1934, as amended, 47 U.S.C. 222, limits the use and disclosure of customer proprietary network information (CPNI) by telecommunications service providers, and provides a right of access for individuals.

[52] 15 U.S.C. 6801-6809. The Gramm-Leach-Bliley Act of 1999 (GLBA), 15 U.S.C. 6801 – 6809, Title V requires financial institutions to disclose their privacy policies to their customers. Customers may opt out of sharing of personal information, and the institutions may not share account numbers with non-affiliated telemarketers and direct marketers. The Consumer Financial Protection Act of 2010 (CFPA), Title X of the Dodd-Frank Wall Street Reform and Consumer (continued...)

# The Federal Trade Commission

**Federal Trade Commission Act.** The Federal Trade Commission Act (the FTC Act)[53] prohibits unfair and deceptive practices in and affecting commerce. The FTC Act authorizes the Commission to seek injunctive and other equitable relief, including redress, for violations of the act, and provides a basis for government enforcement of certain fair information practices (e.g., failure to comply with stated information practices may constitute a deceptive practice or information practices maybe inherently deceptive or unfair).

## FTC Enforcement Actions Concerning the Privacy of Personal Information

The first online behavioral advertising case was brought against an online network advertiser that acts as an intermediary between website publishers and advertisers.[54] The Commission alleged that the online network advertiser violated the FTC Act by offering consumers the ability to opt out of the collection of information to be used for targeted advertising without telling them that the opt-out lasted only 10 days. The Commission's order prohibits the online network advertiser from making future privacy misrepresentations, requires the online network advertiser to provide consumers with an effective opt-out mechanism, and requires destruction of any data associated with a consumer collected during the time its opt-out was ineffective.

The FTC recently approved a final consent order in a case involving the social networking service Twitter.[55] The FTC charged that data security lapses allowed hackers to obtain unauthorized administrative control of Twitter. As a result, hackers had access to private "tweets" and non-public user information and took over user accounts. The order prohibits misrepresentations about the extent to which Twitter protects the privacy of communications, requires Twitter to maintain reasonable security, and mandates independent, comprehensive audits of Twitter's security practices.

In December 2010, the FTC announced a case against a company selling a software program called Sentry Parental Controls that enables parents to monitor their children's activities online. The Commission alleged that the software company sold certain information that it collected from children via this software to third parties for marketing purposes, without parental consent. The Commission's order prohibits the company from sharing information gathered from its monitoring software and requires the company to destroy any such information in its database of marketing information.[56]

---

(...continued)

Protection Act of 2010 (Dodd-Frank), transfers much of the federal agency rulemaking and enforcement authority under the Gramm-Leach-Bliley Act to the newly created Consumer Financial Protection Bureau (CFPB).

[53] 15 U.S.C. 41 et. Seq. Children's Online Privacy Protection Act of 1998 (COPPA), 15 U.S.C. 6501 et seq., addresses the collection of personal information from children under 13.

[54] Chitika, Inc., FTC File No. 102 3087 (Mar. 14, 2011) (consent order accepted for public comment).

[55] Twitter, Inc., FTC File No. 092 3093 (Mar. 11, 2011) (consent order) (resolving allegations that Twitter deceived its customers by failing to honor their choices to designate certain "tweets" as private).

[56] FTC v. Echometrix, Inc., No. CV10-5516 (E.D.N.Y. Nov. 30, 2010) (consent order).

In September 2010, the Commission settled a case against a data broker that maintained an online service, which allowed consumers to search for information about others. The company allowed consumers to opt out of having their information appear in search results for a $10 fee. Four thousand consumers paid the fee and opted out, but their personal information still appeared in search results. The Commission's settlement requires the data broker to disclose limitations on its opt-out offer, and to provide refunds to consumers who had previously opted out.[57]

In March 2011, the FTC reached a settlement with Google over charges that it violated user privacy when it launched the Google Buzz social network.[58] Google Buzz was offered to Google users through Gmail. Many who chose not to join the Google social network were enrolled anyway, and those who chose to join were not fully informed regarding the extent their personal information might be shared with, or exposed to, Google users outside of their own personal network. The Google privacy policy at the time stated, "When you sign up for a particular service that requires registration, we ask you to provide personal information. If we use this information in a manner different than the purpose for which it was collected, then we will ask for your consent prior to such use."[59] The FTC alleged that the representations in Google's privacy policy were false or misleading, and despite its privacy policy that Google would ask for consumers' consent before using their information for another purpose, Google used it to populate its social network without getting user permission. The FTC charged that the policy was false or misleading and constituted a deceptive practice. The proposed settlement bars Google from future privacy misrepresentations, requires the company to implement a comprehensive privacy program, and requires independent privacy audits for the next 20 years. The Federal Trade Commission announced that it has accepted, subject to final approval, a consent agreement from Google that would resolve the Commission's allegations. This is the first time an FTC settlement order has required a company to implement a comprehensive privacy program to protect consumers' information.

# Recent Policy Initiatives

The FTC recently released a Staff Report on a Preliminary Framework on Protecting Consumer Privacy which includes three major elements: (1) companies should integrate privacy into their regular business operations and throughout product development; (2) provide meaningful privacy options while preserving beneficial uses of data, and provide choices to consumers in a simpler, more streamlined manner; and (3) improve the transparency of all data practices.[60] The Framework's basic building blocks are scope, privacy by design, simplified choice, and greater transparency. The Framework applies to all commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or other device. The FTC recommends that companies provide consumers with reasonable access to data about themselves depending on the sensitivity of the data and the nature of its use, and provide prominent disclosures and obtain affirmative express consent before using consumer data in a materially

[57] US Search, Inc., FTC File No. 102 3131 (Sept. 22, 2010) (consent order accepted for public comment).

[58] *In the Matter of Google, Inc.* No. 102 3136 (filed Mar. 30, 2011), available at http://www.ftc.gov/os/caselist/1023136/110330googlebuzzagreeorder.pdf.

[59] Id.

[60] A Preliminary Federal Trade Commission Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers (Dec. 1, 2010), available at http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

different manner. The FTC Staff Report includes a recommendation to implement a universal choice Do Not Track mechanism for behavioral tracking or behavioral advertising.[61]

The Commerce Department's Internet Policy Taskforce (IPTF) is examining how commercial data privacy policy advances the goals of protecting consumer trust in the Internet economy and promotes innovation. The Taskforce released a "Green Paper" on consumer data privacy in the Internet economy on December 16, 2010, and made 10 separate recommendations about how to strengthen consumer data privacy protections. [62] The IPTF concluded that the basic element of current consumer data privacy framework, the privacy policy, is ineffective because it is often a lengthy, dense, and legalistic document. The IPTF recommended updating the commercial data privacy framework because the notice-and-choice system does not provide adequately transparent descriptions of personal data use. The IPTF also concluded that the rules of the road are hard to discern for businesses and sometimes become clear only after FTC enforcement actions, and differing international legal frameworks and new technologies present privacy challenges and complicate commercial data flows across national borders. The IPTF's report recommends considering a clear set of principles concerning how online companies collect and use personal information for commercial purposes. These principles would build on existing Fair Information Practice Principles (FIPPs) of transparency, data use limitation, and accountability. The IPTF report also recommended that Congress authorize the FTC to enforce baseline privacy protections, and create incentives, such as safe harbors, for businesses to adopt self-regulatory privacy codes of conduct, and consider how to harmonize security breach notification rules. The IPTF report calls on Congress to review the Electronic Communications Privacy Act (ECPA) for the cloud computing environment.[63] In light of calls for Congress to reform ECPA,[64] a brief discussion of ECPA follows.

---

[61] "[A] robust, effective Do Not Track system would ensure that consumers can opt out once, rather than having to exercise choices on a company-by-company or transaction-by-transaction basis. Such a universal mechanism could be accomplished through legislation or potentially through robust, enforceable self-regulation." The FTC Staff Report outlines several issues that should be taken into consideration in the development of a Do Not Track Mechanism: any Do Not Track system should be implemented universally, so that consumers do not have to repeatedly opt out of tracking on different sites; the choice mechanism should be easy to find, easy to understand, and easy to use; any choices offered should be persistent and should not be deleted if, for example, consumers clear their cookies or update their browsers; a Do Not Track system should be comprehensive, effective, and enforceable. It should opt consumers out of behavioral tracking through any means and not permit technical loopholes; and an effective Do Not Track system would go beyond simply opting consumers out of receiving targeted advertisements; it would opt them out of collection of behavioral data for all purposes that are not commonly accepted. A Preliminary Federal Trade Commission Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers (Dec. 1, 2010), available at http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

[62] *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*:., available at http://www.commerce.gov/sites/default/files/documents/2010/december/iptf-privacy-green-paper.pdf.

[63] A preeminent legal scholar notes that the electronic surveillance laws are a weapon of choice in the arsenal of policy makers, litigants, and commentators seeking to address the threats digital technology poses for privacy. Bellia, Patricia L., Spyware and the Limits of Surveillance Law. Berkeley Technology Law Journal, Vol. 20, Summer 2005; Notre Dame Legal Studies Research Paper No. 05-15. Available at SSRN: http://ssrn.com/abstract=757967.

[64] An ECPA reform advocacy coalition has advanced the following principles:

> A governmental entity may require an entity covered by ECPA (a provider of wire or electronic communication service or a provider of remote computing service) to disclose communications that are not readily accessible to the public only with a search warrant issued based on a showing of probable cause, regardless of the age of the communications, the means or status of their storage or the provider's access to or use of the communications in its normal business operations.
>
> A governmental entity may access, or may require a covered entity to provide, prospectively or retrospectively, location information regarding a mobile communications device only with a

(continued...)

# Electronic Communications Privacy Act Reform

In 1986, Congress enacted the Electronic Communications Privacy Act (ECPA) to strike a balance between the fundamental privacy rights of citizens and the legitimate needs of law enforcement with respect to data shared or stored in various types of electronic and telecommunications services.[65] Since the ECPA was passed the Internet and associated technologies have expanded exponentially.[66]

ECPA consists of three parts: a revised Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (also known as "Title III" or the "Wiretap Act");[67] the Stored Communications Act (SCA));[68] and provisions governing the installation and use of trap and trace devices and pen registers.[69] ECPA prohibits the interception of wire, oral, or electronic communications unless an exception to the general rule applies. Unless otherwise provided, Title III prohibits wiretapping and electronic eavesdropping; possession of wiretapping or electronic eavesdropping equipment; use or disclosure of information obtained through illegal wiretapping or electronic eavesdropping; and disclosure of information secured through court-ordered wiretapping or electronic eavesdropping, in order to obstruct justice.[70] The Stored Communications Act prohibits unlawful access to stored communications.[71] The Pen Register and Trap and Trace statute proscribes

(...continued)

> warrant issued based on a showing of probable cause.
>
> A governmental entity may access, or may require a covered entity to provide, prospectively or in real time, dialed number information, email to and from information or other data currently covered by the authority for pen registers and trap and trace devices only after judicial review and a court finding that the governmental entity has made a showing at least as strong as the showing under 2703(d).
>
> Where the Stored Communications Act authorizes a subpoena to acquire information, a governmental entity may use such subpoenas only for information related to a specified account(s) or individual(s). All non-particularized requests must be subject to judicial approval.

Digital Due Process, Our Principles, available at http://www.digitaldueprocess.org/index.cfm?objectid=99629E40-2551-11DF-8E02000C296BA163.

[65] 100 Stat. 1848; see also House Committee on the Judiciary, Electronic Communications Privacy Act of 1986, H. Rep. No. 99-647, 99th Cong. 2d Sess. 2, at 19 (1986).

[66] Electronic Communications Privacy and Cloud Computing: Hearing Before the H. Subcom. on the Constitution, Civil Rights and Civil Liberties, 112th Cong. (Sep. 23, 2010) (statement of Edward W. Felton, Professor Princeton University).

> In 1986, when ECPA was passed, the Internet consisted of a few thousand computers. The network was run by the U.S. government for research and education purposes, and commercial activity was forbidden. There were no web pages, because the web had not been invented. Google would not be founded for another decade. Twitter would not be founded for another two decades. Mark Zuckerberg, who would grow up to start Facebook, was two years old. In talking about advances in computing, people often focus on the equipment. Certainly the advances in computing equipment since 1986 have been spectacular. Compared to the high-end supercomputers of 1986, today's mobile phones have more memory, more computing horsepower, and a better network connection not to mention a vastly lower price.

[67] 18 U.S.C. 2510-2522.

[68] 18 U.S.C. 2701-2712.

[69] 18 U.S.C. 3121-3126.

[70] 18 U.S.C. 2511.

[71] 18 U.S.C. 2701.

unlawful use of a pen register or a trap and trace device.[72] ECPA establishes rules that law enforcement must follow before they can access data stored by service providers. Depending on the type of customer information involved and the type of service being provided, the authorization law enforcement must obtain in order to require disclosure by a third party will range from a simple subpoena to a search warrant based on probable cause.

ECPA reform efforts focus on crafting a legal structure that is up-to-date, can be effectively applied to modern technology, and that protects users' reasonable expectations of privacy. ECPA is viewed by many stakeholders as unwieldy, complex, and difficult for judges to apply.[73] Cloud computing[74] poses particular challenges to the ECPA framework. For example, when law enforcement officials seek data or files stored in the cloud, such as Web-based e-mail applications or online word processing services, the privacy standard that is applied is often lower than the standard that applies when law enforcement officials seek the same data stored on an individual's personal or business hard drive.[75]

## Author Contact Information

Gina Stevens
Legislative Attorney
gstevens@crs.loc.gov, 7-2581

[72] 18 U.S.C. 3121.

[73] "Cloud computing is an emerging form of computing that relies on Internet-based services and resources to provide computing services to customers, while freeing them from the burden and costs of maintaining the underlying infrastructure. Examples of cloud computing include Web-based e-mail applications and common business applications that are accessed online through a browser, instead of through a local computer." Information Security: Federal Guidance Needed to Address Control Issues with Implementing Cloud Computing, GAO-10-513 May 27, 2010, available at http://www.gao.gov/products/GAO-10-513.

[74] J. Beckwith Burr, The Electronic Communications Privacy Act of 1986: Principles for Reform, available at http://www.digitaldueprocess.org/files/DDP_Burr_Memo.pdf.

[75] Electronic Communications Privacy and Cloud Computing: Hearing Before the H. Subcomm. on the Constitution, Civil Rights, and Civil Liberties, 112th Cong. (Sep. 23, 2010) (statement Michael Hintze, Associate General Counsel, Microsoft Corp.).