Online Data Collection and Disclosure to Private Entities: Selected Federal Laws and Self-Regulatory Regimes

Kathleen Ann Ruane
Legislative Attorney

April 1, 2011

Congressional Research Service
7-5700
www.crs.gov
RL34693

CRS Report for Congress
Prepared for Members and Committees of Congress

Summary

In recent years, there has been an increase in concern over the amount of data that companies, both online and offline, gather about individuals and the private entities to which such data is disclosed. Companies generally use this information for marketing purposes. However, consumers often may be unaware when their data is being collected, particularly in our current era where each click of a mouse on a website may be recorded by a marketing or data gathering firm. Some of the data gathered may be highly sensitive information like Social Security numbers or bank account numbers. Furthermore, this data may be merged with data collected offline, or shared with third parties. These risks have been the subject of congressional and regulatory scrutiny. The 112th Congress and federal agencies will likely continue to examine these issues and debate legislative and regulatory solutions.

The first major issue presented by this debate is whether data gathering and disclosure practices violate current law. Privacy laws in the United States are generally industry specific. Certain laws govern the collection and disclosure of financial data. Other laws govern the collection and disclosure of health-related data. A large amount of data collected about consumers, however, does not fall into the categories of data that are covered by these industry-specific laws. Thus, the primary federal mechanism for enforcing privacy protections, where the data at issue are not covered by more specific statutory protection, is Section 5 of the Federal Trade Commission Act. Section 5 prohibits unfair and deceptive trade practices. The Federal Trade Commission (FTC) has successfully used this prohibition to hold companies liable for breaches of the privacy policies that they have developed.

There is also argument as to whether the Electronic Communications Privacy Act (both Title I, known as the Wiretap Act, and Title II, known as the Stored Communications Act) and the Communications Act of 1934, apply to online entities that are collecting data through click tracking, capturing search terms, providing web-based e-mail services and other methods. It is likely that in some cases these laws could be held to apply to such activities and that, in some cases, these methods of data collection could be forbidden unless consent is obtained from one of the parties to the communication or some other exception applies. This report will examine the application of these statutes in more detail.

The second major issue presented by this debate is whether new legislation or regulations are needed to govern consumer privacy. There are no current federal regulations specific to online advertising and data gathering. The FTC and the Department of Commerce recently published reports proposing frameworks for privacy in this rapidly developing market place. The proposed frameworks, in the agencies' views, could be a combination of both government and self-regulation. This report briefly will discuss these proposals.

Private organizations such as the Network Advertising Initiative, Interactive Advertising Bureau, and Privacy Group Coalition have created policies, which many online entities have pledged to follow, that represent industry best practices for protecting the privacy of web users. Some of their self-regulatory regimes are discussed as well. For more information about the online advertising industry, see CRS Report R40908, *Advertising Industry in the Digital Age*, by Suzanne M. Kirchhoff.

Contents

Introduction 1
Current Laws 1
Federal Trade Commission Act 1
Electronic Communications Privacy Act 2
The Wiretap Act 3
The Stored Communications Act 8
Section 631 of the Communications Act 13
Proposed Privacy Frameworks 15
Federal Trade Commission's Proposed Framework for Protecting Privacy Online and Offline 16
Department of Commerce Privacy Policy Framework 17
Self-Regulation 17
Federal Trade Commission Online Advertising Self-Regulatory Principles 18
Industry Self-Regulatory Principles 18

Contacts

Author Contact Information 20

Introduction

In recent years, there has been an increase in concern over the amount of data that companies, both online and offline, gather about individuals. Companies generally use this information for marketing purposes. However, consumers often may be unaware of when their data are being collected. This is so particularly in our current era where each click of a mouse on a website may be recorded by a marketing or data gathering firm. Some of the data available to be gathered may be highly sensitive information such as Social Security numbers or bank account numbers. Furthermore, this data may be merged with data collected offline, or shared with third parties, and there is a risk that even data that has been "anonymized" may be linked to individuals. These risks have been the subject of congressional and regulatory scrutiny. The 112th Congress and federal agencies, including the Federal Trade Commission (FTC) and the Department of Commerce (DOC), will likely continue to examine these issues and debate legislative and regulatory solutions.

Current Laws

One of the first major issues presented by this debate is whether data gathering and disclosure practices violate current law. This section will examine three of the primary federal laws that apply to data gathering online as well as the disclosure of the data gathered online to other private parties: the Federal Trade Commission Act (FTC Act), the Electronic Communications Privacy Act (ECPA), and the Communications Act of 1934.

Federal Trade Commission Act

There are a myriad of federal laws that protect specific types of data. For example, the Gramm-Leach-Bliley Act protects financial data.[1] The Health Insurance Portability and Accountability Act, as well as other statutory provisions, protects health related data.[2] However, most data collected about consumers do not fall into the categories of data protected by specific privacy laws. As a result, the primary federal mechanism for enforcing privacy protections is Section 5 of the FTC Act. Section 5 generally prohibits unfair and deceptive trade practices.[3] The Federal Trade Commission (FTC) has used this prohibition to characterize violations of the privacy policies that companies have developed as unfair and deceptive trade practices.[4] The result has been some success for the FTC in holding companies liable for breaches of companies' privacy policies, essentially holding companies to their word about the ways in which they have promised that data will be collected and used.[5] It is nonetheless important to note that Section 5 is general

[1] CRS Report RS20185, *Privacy Protection for Customer Financial Information*, by M. Maureen Murphy.

[2] CRS Report R40546, *The Privacy and Security Provisions for Health Information in the American Recovery and Reinvestment Act of 2009*, by Gina Stevens and Edward C. Liu.

[3] 15 U.S.C. § 45.

[4] The prohibitions in Section 5 apply to all data gathering practices and privacy policies, not only data gathering practices and privacy policies that occur online, as well as a broad array of other activities in commerce that might be considered unfair and deceptive. This section will focus on FTC enforcement of online privacy policies.

[5] *See e.g.*, In the Matter of Chitika, Inc., Proposed Agreement Containing Consent Order, 76 Fed. Reg. 15313 (March 21, 2011) (finding violations of the company's privacy policy and proposing an order of more effective disclosures among other remedies) available at http://www.ftc.gov/os/caselist/1023087/110314chitikaagree.pdf; In the Matter of (continued...)

and does not create uniform privacy standards by which companies must abide. Rather, the FTC uses Section 5 to hold companies liable for their individually developed privacy policies, which may differ widely in their scope.

A recent example of the FTC's enforcement in this area is the agency's proposed settlement with Google over violations of its privacy policy in the rollout of its Google Buzz social networking program.[6] In rolling out Buzz, the FTC alleged that Google used data it had collected pursuant to its Gmail program in ways that had not been disclosed in its privacy and data usage policy for Gmail.[7] The FTC alleged that Google initially allowed consumers to choose whether to "check out" Buzz. Some of those who opted not to be included in Buzz were enrolled in Buzz anyway.[8] The FTC argued that this unauthorized enrollment, which transferred user data from Gmail accounts to Google Buzz, among other breaches of its Gmail data usage policy, amounted to a violation of Section 5.[9] Google has agreed to a number of conditions in the consent decree. Among them, assuming that the order is adopted by the full Commission, Google will subject itself to independent privacy audits every two years for the next 20 years. Furthermore, following the order's adoption, if Google wishes to share data it collects from any of its applications or online programs with a third party in a way that is different from the practices stated at the time the data was collected, Google must obtain "opt-in" consent to share the data.

Electronic Communications Privacy Act

The Electronic Communications Privacy Act (ECPA)100 Stat. 1848, 18 U.S.C. 2510-2521,[10] contains two titles that are relevant to our discussion. ECPA is an amendment to Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 87 Stat. 197, 18 U.S.C. 2510-2520 (1970 ed.).[11] Title I, known as the Wiretap Act, governs the interception of communications while they are in transit. Title II, known as the Stored Communications Act, governs access to and disclosure of data that is not in transit, but is stored, even temporarily, in a third party's facilities. Each of these titles could potentially be applied to data that is gathered and disclosed by online companies. However, some data gathered and disclosed by online entities may not be covered by ECPA at all. Each case requires a fact-specific inquiry to determine whether and which part of ECPA applies, and a further inquiry to determine, even if ECPA does apply, whether the act has

(...continued)

Twitter, Inc., Decision and Order of the Federal Trade Commission, Docket No. C-4316 (2011) (finding that Twitter failed to prevent security breaches in violation of its privacy policy, and ordering Twitter to improve disclosure and barring the company from misleading consumers for 20 years, among other conditions) available at http://www.ftc.gov/os/caselist/0923093/110311twitterdo.pdf.

[6] In the Matter of Google, Inc., FTC File No. 102 3136, Proposed Agreement Containing Consent Order (March 30, 2011) available at http://ftc.gov/os/caselist/1023136/110330googlebuzzagreeorder.pdf.

[7] FTC Charges Deceptive Privacy Practices in Google's Rollout of its Buzz Social Network, http://ftc.gov/opa/2011/03/google.shtm.

[8] *Id.*

[9] In the Matter of Google, Inc., FTC File No. 102 3136, Proposed Agreement Containing Consent Order (March 30, 2011) available at http://ftc.gov/os/caselist/1023136/110330googlebuzzagreeorder.pdf.

[10] Testimony of Ms. Leslie Harris, CEO of the Center for Democracy and Technology, *Privacy Implications of Online Advertising: Hearing Before the S. Comm. On Commerce, Science, and Transportation*, 110th Cong. (2008)(hereinafter CDT Testimony), available at http://commerce.senate.gov/public/_files/LeslieHarrisCDTOnlinePrivacyTestimony.pdf.

[11] For a more detailed discussion of the history of ECPA, see CRS Report R41733, *Privacy: An Overview of the Electronic Communications Privacy Act*, by Charles Doyle; CRS Report 98-326, *Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping*, by Gina Stevens and Charles Doyle.

been violated. This section will discuss the general application of the Wiretap and Stored Communications Act to information gathered online.

The Wiretap Act

Concerns have been raised that online advertising providers, websites, and Internet service providers (ISPs) that agree to collect certain data generated by Internet traffic to behaviorally target advertising may be violating the Wiretap Act, or Title I of ECPA. The Wiretap Act prohibits the interception of electronic communications and prohibits electronic communications service providers from intentionally divulging information while in transit to third parties, unless an exception to these general rules applies. [12]

The Online Advertising Provider

The first question that must be addressed is whether the Wiretap Act applies to the activities of online advertising providers. Online advertising providers acquire information such as the fact that a user clicked on a particular link (an action which is the equivalent of asking the site providing the link to send the user information), and while the communication is in transit.[13] Furthermore, these advertisers may acquire information regarding user searches, etc., while in transit.[14] Under ECPA, it is illegal, with certain enumerated exceptions, for any person to "intentionally intercept, endeavor to intercept, or procure any other person to intercept or endeavor to intercept, any wire, oral or electronic communication."[15] It is important to lay out the statutory definitions of each of the key terms in order to assess whether the ECPA prohibition and/or any of its exceptions apply to activities conducted by online behavioral advertisers.

- "Intercept" means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.[16]
- "Contents" when used with respect to any wire, oral, or electronic communication includes any information concerning the substance, purport, or meaning of that communication.[17]
- "Electronic Communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photo optical system that affects interstate or foreign commerce.[18]

[12] The exceptions are numerous and depend on the context of the interception. The exception most relevant in the context of an interception of online communications by a private third party is the consent exception. 18 U.S.C. §2511(2)(d). The other exceptions to the prohibition on interception are discussed in CRS Report R41733, *Privacy: An Overview of the Electronic Communications Privacy Act*, by Charles Doyle and CRS Report 98-326, *Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping*, by Gina Stevens and Charles Doyle.

[13] *See e.g.*, NebuAd Testimony at 3-4.

[14] *See id.*; In re DoubleClick, Inc. Privacy Litigation, 154 F.Supp. 2d 497 (S.D.N.Y. 2001).

[15] 18 U.S.C. §2511(1)(a).

[16] 18 U.S.C. §2510(4).

[17] 18 U.S.C. §2510(8).

[18] 18 U.S.C. §2510(12).

Because the advertisers record that a particular user requested information from a website by clicking on a particular link or sent information to a website via a search entry or other method, the advertisers appear to be "intercepting" the "contents" of those "electronic communications." Therefore, the interceptions are likely covered by Title I.[19]

Merely determining that this type of data acquisition by online advertisers is an interception for the purposes of the Wiretap Act does not end the analysis. The Wiretap Act excepts certain communication interceptions from its prohibition. The exception to the Wiretap Act that would most likely apply to these types of interceptions is the exception that allows for interception of communications with the consent of one of the parties.[20] The question of when and how consent to the interception may be given is addressed below.

The Internet Service Provider (ISP)

The second question to be addressed is whether the Wiretap Act applies to ISPs that allow online advertising providers to gather data from traffic over the ISP's network. The Wiretap Act prohibits any person or entity providing an electronic communications service from intentionally divulging the "contents of any communications ... while in transmission on that service to any person or entity other than an addressee or intended recipient of such communications or an agent of such addressee or intended recipient."[21] This section appears to apply to ISPs that would agree to allow online advertising providers to acquire portions of the web traffic of ISP customers, as neither the advertising provider nor the ISP would, in most cases, be the addressee or intended recipient of the communications.

Again, determining that the data collection is likely covered by the Wiretap Act does not end the analysis. An exception may apply. ISPs are allowed to divulge the contents of communications while in transit if the divulgence is part of "any activity which is a necessary incident to the rendition of [that service] or to the protection of the rights or property of the provider of that service."[22] It does not seem likely that this exception applies to ISPs when contracting with online advertising providers. Though the service for which they contract may help keep the websites of the advertising provider's clients free to the public by producing advertising revenue, the

[19] It is worth noting that there has yet to be a court case to decide definitively that ECPA applies to this type of data collection. In the cases cited here, the online advertising providers made their cases by assuming, but not conceding, that ECPA applied to the data collection. *See* In re Pharmatrak, Inc. Privacy Litigations, 329 F.3d 9 (1st Cir. 2003); In re DoubleClick, Inc. Privacy Litigation, 154 F.Supp. 2d 497 (S.D.N.Y. 2001).

[20] "It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communications 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 any State." 18 U.S.C. §2511(2)(d).

[21] 18 U.S.C. §2511(3)(a). It is worth noting that this section does not require that the divulgence of information while it is in transit by an electronic communications service be an "interception" in order for it to be prohibited. Data acquisition can only be categorized as an "interception" for the purposes of ECPA "through the use of any electronic, mechanical, or other device." 18 U.S.C. §2510(4). The statute makes clear that "electronic, mechanical, or other device" does not mean the equipment or facilities of a wire or electronic communications service that are used in the ordinary course of the provider's business. 18 U.S.C. 2510(5). Therefore, it is possible that when an ISP allows a third party to collect data that is in transit over its network the ISP may not be "intercepting" that data as the term "intercept" is defined by ECPA. Nonetheless, "intentionally divulging the contents of any communication while in transmission" over an ISP's network is prohibited by 18 U.S.C. §2511(3)(a), unless it meets one of the exceptions outlined in 18 U.S.C. § 2511(3)(b).

[22] 18 U.S.C. §2511(2)(a)(i).

interception is not necessary to maintain an ISP's proper function or solvency and, therefore, likely is not necessary to the rendition of Internet access service.[23] ISPs also are allowed to divulge the contents of a communication in transit "with the lawful consent of the originator or any addressee or intended recipient of such communication."[24] If the ISPs obtain the consent of their customers to intercept some of their online activities, this exception to the Wiretap Act would seem to apply. Again, the questions of how and when consent may be obtained, and what constitutes "lawful consent," arise and are addressed in the following section.

The Consent Exception to the Wiretap Act

As noted above, interception of electronic communications is not prohibited by the Wiretap Act if one of the parties to the communications has consented to the interception. Consent is not defined by the act; nor do precise instructions of how and when consent may be obtained appear in regulation. Therefore, it has been left largely to the courts to determine when consent to intercept a communication otherwise covered by the Wiretap Act's prohibitions has been granted.[25] There have been few cases dealing with the act's application to online advertising providers and none examining the act's application to agreements between ISP providers and online advertising providers. As a result, many questions exist regarding how to obtain adequate consent.

Data Collection Agreements Between Website Operators and Online Advertising Providers

Agreements for online advertising providers to monitor certain web traffic may be made between the online advertising provider and the website operators seeking to have ads placed on their sites. Facebook, for example, would be a prominent example of a website that may enter into this type of agreement. The advertising providers receive information about user activity on participating websites (i.e., Facebook.com) and aggregate that data to better target ads. In litigation against the online advertising provider DoubleClick for violations of the Wiretap Act, the court examined whether websites were "users" of electronic communications services under the act.[26] The act defines a "user" as "any person or entity who (A) uses an electronic communication service; and (B) is duly authorized by the provider of such service to engage in such use."[27] The court

---

[23] *See, e.g.*, U.S. Census 2006 Annual Survey (Information Sector), *Internet Service Providers—Estimated Sources of Revenue and Expenses for Employer Firms: 2004 Through 2006* at 32, Table 3.4.1 (April 15, 2006) (indicating that internet access service are responsible for the greatest percentage of revenue earned by ISPs) available at http://www.census.gov/svsd/www/services/sas/sas_data/51/2006_NAICS51.pdf; Comcast Corporation, Quarterly Report (Form 10-Q) (June 30, 2008) (reporting that 95% of Comcast Corporation's consolidated revenue is derived from its cable operations, which includes the provision of high-speed internet services) available at http://sec.gov/Archives/edgar/data/1166691/000119312508161385/d10q.htm.

[24] 18 U.S.C. 2511(3)(b)(ii).

[25] *See e.g.*, United States v. Friedman, 300 F.3d 111, 122-23 (2d Cir. 2002)(inmate use of prison phone);United States v. Faulkner, 439 F.3d 1221, 1224 (10th Cir. 2006)(same); United States v. Hammond, 286 F.3d 189, 192 (4th Cir. 2002) (same); *United States v. Footman*, 215 F.3d 145, 154-55 (1st Cir. 2000) (same); Griggs-Ryan v. Smith, 904 F.2d 112, 116-17 (1st Cir. 1990) (use of landlady's phone); United States v. Rivera, 292 F. Supp. 2d 838, 843-45 (E.D. Va. 2003)(inmate use of prison phone monitored by private contractors). For a discussion of the consent exception to the Wiretap Act as it is applied in other contexts, see, CRS Report R41733, *Privacy: An Overview of the Electronic Communications Privacy Act*, by Charles Doyle and CRS Report 98-326, *Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping*, by Gina Stevens and Charles Doyle.

[26] In re DoubleClick, Inc. Privacy Litigation, 154 F.Supp. 2d 497 (S.D.N.Y. 2001).

[27] 18 U.S.C. §2510(13).

reasoned that websites are "users" (and, therefore, "parties to the communications" at issue) because they actively respond to requests they receive over electronic communications services by deciding whether to send the requested document, breaking the document down into TCP/IP protocol, and sending the packets over the Internet.[28] Because websites are "users" of electronic communications, the court found that websites are also "parties to the communications" in dispute; therefore, website owners have the ability to consent to a communication's interception.[29]

The court also held that the website operators had consented, by virtue of their contract with DoubleClick, to allow the company to intercept certain traffic on their websites in order to target advertising to website visitors.[30] Consent for private interceptions of electronic communications cannot be granted if the purpose of the interception is the commission of criminal or tortious conduct.[31] The court noted that the focus of the determination of criminal or tortious purpose under the Wiretap Act is "not upon whether the interception itself violated another law; it is upon whether the purpose for the interception—its intended use—was criminal or tortious."[32] Applying that standard, the court found that the plaintiffs had not alleged that DoubleClick's primary motivation for intercepting communications was to injure plaintiffs tortiously. In the court's view, even if DoubleClick's actions ultimately proved tortious or criminal, there was no evidence that DoubleClick was motivated by tortious intent. As a result, the court found that the consent exception to ECPA was satisfied.[33]

In a similar suit against online advertising provider Pharmatrak, the court outlined limitations to the consent exception regarding these types of agreements. In that case, Pharmatrak had contracted with certain drug companies to provide advertising on their websites. Included in the agreement was permission for the advertising provider to record certain web traffic that did not include personally identifiable information.[34] Perhaps inadvertently, the online advertising provider did collect a small amount of personally identifiable information though it had pledged not to do so. The advertiser argued that consent had been granted for such interception. The court disagreed. According to the court, it is for the party granting consent to define its scope, and the parties in this case had not consented to the collection of personally identifiable information.[35] In collecting personally identifiable information by intercepting data without the consent of one of the parties, the online advertiser potentially had violated the Wiretap Act, but may have lacked the requisite intent to be found liable under the statute.[36] The appeals court directed the trial court to conduct further investigation into the matter.

Given the conclusions in the above cases, it appears that online advertising providers, like DoubleClick, that partner to collect data from individual websites, like Facebook.com or the New York Times' website, generally are not violating the Wiretap Act, because the websites are "parties to the communication" with the ability to consent to interception. Based on these cases,

---

[28] In re DoubleClick, Inc. Privacy Litigation, 154 F.Supp. 2d at 508-09.

[29] *Id.* at 514.

[30] *Id.* at 509-513.

[31] 18 U.S.C. §2511(2)(d).

[32] In re DoubleClick, Inc. Privacy Litigation, 154 F.Supp. 2d at 516 (quoting Sussman v. ABC, 196 F.3d 1200, 1202 (9th Cir. 1999)).

[33] *Id.* at 518-19.

[34] In re Pharmatrak, Inc. Privacy Litigations, 329 F.3d 9 (1st Cir. 2003).

[35] *Id.* at 20.

[36] *Id.* at 23.

the advertising providers will not be seen as running afoul of the act so long as the data the advertising providers collect do not fall outside the scope of that which the website has agreed to disclose.

Data Collection Agreements Between ISPs and Online Advertising Providers

On the other hand, when the partnership is between the ISP and the online advertising provider, neither of the parties to the agreement to intercept web traffic is a party to the communications that are being intercepted. Therefore, it would appear that consent for the interceptions must be obtained from individual customers of the ISPs. The questions, in these circumstances, are whether consent must be "affirmative," or if it can be "implied," and if consent must be "affirmative" what process must be used to obtain such consent from individual users.

- "Affirmative" or "Implied" Consent

Consent to interceptions has been implied by the surrounding circumstances of communications. While consent may be implied, it may not be "casually inferred."[37] It seems unlikely, as a result, that merely by using an ISP's service, a customer of that service has implied her consent to the interception of her electronic communications by online advertising providers. If consent likely may not be implied simply from use of an ISP's service, then a form of affirmative consent from the ISP's customer would be necessary.

- "Opt-in" v. "Opt-out" Consent

In other statutes requiring consent for certain types of disclosure, regulatory regimes have developed to define when and how affirmative consent should be obtained.[38] A similar debate is occurring now involving how ISPs should obtain consent from their customers to share data about online activities with online advertising providers. The debate centers around whether ISPs and advertisers must obtain "opt-in" consent or if they may continue to obtain "opt-out" consent for these interceptions.

"Opt-in" consent is obtained when a party to the communication is notified that his or her ISP has agreed to allow an online advertiser to track that person's online activity in order to better target advertising to that person. The advertiser, however, may not begin to track that individual's web activity until the individual responds to the notification granting permission for such activity.[39] If the individual never responds, interception can never begin. "Opt-out" consent, by contrast, requires a party to the communication to notify the ISP or the advertiser that he or she does not

---

[37] Williams v. Poulos, 11 F.3d 271, 281 (1st Cir. 1993)(finding that defendant corporation violated the Wiretap Act, because it did not have implied consent or a business necessity to place wiretaps).

[38] *See e.g., In the Matter of Implementation of the Telecommunications Act of 1996; Telecommunications Carriers; Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services*, 22 FCC Rcd 6927 (2007)(outlining under what circumstances voice service providers must obtain "opt-in" v. "opt-out" consent in order to disclose Customer Proprietary Network Information(CPNI)). For a discussion of the FCC's CPNI disclosure regulations, see CRS Report RL34409, *Selected Laws Governing the Disclosure of Customer Phone Records by Telecommunications Carriers*, by Kathleen Ann Ruane.

[39] *See* The Network Advertising Initiative's Self-Regulatory Code of Conduct for Online Behavioral Advertising, Draft: For Public Comment, available at http://networkadvertising.org/networks/NAI_Principles_2008_Draft_for_Public.pdf (last visited July 28, 2008). *See also*, 47 C.F.R. §2003(k)(defining "opt-in" approval in the CPNI context).

grant permission for such activity.[40] If the individual never responds, interception will begin. Currently, it appears that companies such as NebuAd are obtaining or planning to obtain "opt-out" consent for the information gathering they engage in with ISPs.[41] The present question is whether "opt-out" consent is sufficient to satisfy the Wiretap Act consent requirement. This question has yet to be addressed by a federal court or clarified by legislation or regulation.

The Stored Communications Act

Title II of ECPA, known as the Stored Communications Act (18 U.S.C. §§ 2701 – 2712; SCA) creates a system of statutory privacy rights for consumer data that is stored by third parties. There is little case law or interpretation of the SCA. This may be because it was not until the current decade that it has become common again for consumer information to be maintained and stored by third parties.[42] Now, with web-based e-mail and online profiles, reams of data most consumers may want to be protected from broad disclosure are being held by private companies. Some data may be protected by the SCA, but some data may fall entirely outside of the SCA's scope.

The SCA creates a tiered structure for the protection of information. The most highly protected information is the information stored in "electronic storage" by companies providing electronic communications services (ECS). The next level of protection is for information stored by companies providing remote computing services (RCS), which essentially are services that store and process data remotely.[43] Beneath that is information that is not protected at all. Information may lack protection either because the company in question is not providing an ECS or an RCS, or because the data in question are not protected by the act. Furthermore, depending on the circumstances, a particular entity may be providing an ECS, an RCS, both an ECS and an RCS, or neither.[44] As a result, for each potential data gathering or disclosure question in today's online environment, there may be a different analysis under the SCA .

Electronic Communications Services and Electronic Storage

An ECS is "any service which provides to users thereof the ability to send or receive wire or electronic communications."[45] Those who provide telephone, text message, or e-mail services are generally considered to be providing an ECS.[46] However, mere users of ECS are not providers of

[40] *See* The Network Advertising Initiative's Self-Regulatory Code of Conduct for Online Behavioral Advertising, Draft: For Public Comment, available at http://networkadvertising.org/networks/NAI_Principles_2008_Draft_for_Public.pdf (last visited July 28, 2008). *See also*, 47 C.F.R. §2003(l)(defining "opt-out" approval in the CPNI context).

[41] NebuAd Testimony at 4.

[42] *See* FTC Complaint of Electronic Privacy Information Center at 4, In Re Google, Inc. and Cloud Computing Servs. (Mar. 17, 2009) ("Cloud Computing Services are an emerging network architecture by which data and applications reside on third party servers, managed by private firms, that provide remote access through web-based devices.").

[43] *See* 18 U.S.C. § 2711(2).

[44] 18 U.S.C. §§ 2510 (15); 2711 (2). *See* Flagg v. City of Detroit, 252 F.R.D. 346, 362 (E.D. Mich. 2008) (finding that a provider "may be deemed to provide both an ECS and a RCS to the same customer.") *But see* Quon v. Arch Wireless Operating Co., 529 F.3d 892, 902-03 (9th Cir. 2008) (finding that if a company provided an ECS it could not be providing an RCS as well).

[45] 18 U.S.C. § 2510 (14).

[46] *See Quon* 529 F.3d at 892 (text messaging service is an ECS); In Re Application of United States, 509 F. Supp. 2d 76 (D. Mass. 2007) (cell phone service is an ECS); Freedman v. American Online, Inc., 325 F. Supp. 2d 638 (E.D. Va. 2004) (AOL is an ECS); Frazer v. Nationwide Mut. Ins. Co., 352 F.3d 107 (3d Cir. 2004) (insurance company (continued...)

ECS. As discussed above, websites generally are users of ECS and are not providers of ECS.[47] However, a website or online business might provide an ECS if the website allows communication with third parties.

Under the SCA, entities providing an ECS to the public are not allowed to divulge the contents of a communication while the communication is in electronic storage by the service, unless an exception applies.[48] Electronic storage means "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and any storage of such communication by an [ECS] for purposes of backup protection."[49] The question of whether a communication is in electronic storage is an unsettled one. Some courts and the Department of Justice have found that a communication such as an e-mail remains in electronic storage until it is retrieved by its intended recipient and read.[50] In other words, unopened e-mail, sitting on an ECS provider's server is in electronic storage. However, an opened e-mail that is on that server is not in electronic storage because it is not being stored "incidental to the transmission" of the communication. The Ninth Circuit, however, has found that even opened e-mails or communications may be in electronic storage, because they could be held on the ECS facilities for "backup purposes."[51] While this interpretation does lend meaning to the portion of the statute citing backup copies as copies in electronic storage, it also raises a number of questions, including what "backup" means. Many people using web-based e-mail like GMail and Yahoo! Mail may keep their only copy of a communication on the web-based service provider's systems. Would those only copies of communications be considered to be "backup"? The answer is unclear, and has yet to be resolved by a court. If sole copies are included in the definition of backup for the purposes of electronic storage, many more communications than previously thought may be covered by the prohibition on disclosure of the contents of communications in electronic storage.

Assuming that a provider of an ECS has copies of the contents of a communication in electronic storage and wishes to disclose them to a private third party, the ECS provider is prohibited from doing so unless an exception applies. The contents of communications held by an ECS in electronic storage may be disclosed to the intended recipient; the contents may be disclosed with the lawful consent of the "originator or addressee or intended recipient of such communication";

(...continued)

providing an e-mail service provided an ECS).

[47] *See* Crowley v. CyberSource Corp., 166 F. Supp. 2d 1263 (N.D. Cal. 2001)(finding that Amazon.com was not providing an ECS, though the website permitted communication with Amazon.com).

[48] 18 U.S.C. §2702(a)(1). A provider of ECS or RCS may divulge the content of a communication to an addressee or intended recipient, as otherwise authorized by other provisions of ECPA, with consent of the originator or one of the parties to the communication, to a person employed or authorized whose facilities are used to forward such communication to its destination, as necessarily incident to the rendition of service or to protect the service provider's property, to the National Center for Missing and Exploited Children in connection with reports submitted pursuant to the Victims of Child Abuse Act, to a law enforcement agency under some circumstances, to a governmental entity if the service provider believes that an emergency involving risk of death or serious injury requires disclosure without delay. 18 U.S.C. § 2702 (b).

[49] 18 U.S.C. § 2510 (17).

[50] *See Fraser*, 352 F. 3d at 114 (finding that e-mail in post-transmission storage was not in electronic storage); *In re Doubleclick*, 154 F. Supp. 2d at 511 (finding that electronic storage should be narrowly defined); U.S. DEP'T OF JUSTICE, CCIPS, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS, Chapter 3 (2009), *available at* http://www.justice.gov/criminal/cybercrime/ssmanual/ssmanual2009.pdf (hereinafter DOJ Manual).

[51] Theofel v. Farey-Jones, 359 F. 3d 1066 (9th Cir. 2004).

and the contents of a communication may be disclosed "as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of the service."[52]

For data that are considered to be "non-content," disclosure rules are more lenient. ECS providers may disclose "a record or other information pertaining to a subscriber of such service (not including the contents of communications)" to any person who is not a governmental entity.[53] Therefore, for non-content information, an ECS may disclose subscriber information to non-governmental entities relatively freely. It becomes important, therefore, to tease out what is "content" and what is "non-content" information. That will be discussed below.

As well as prohibiting unauthorized disclosure of communications held in electronic storage by an ECS, the SCA prohibits the unauthorized access to electronic communications service facilities.[54] It also prohibits exceeding an authorization to access ECS facilities, which results in a person obtaining, altering, or preventing authorized access to a wire or electronic communication while it is in electronic storage.[55] Some online ECS providers may have operations diverse enough that the companies may not need to disclose the contents of communications that may be contained in electronic storage in order to use it to serve advertising to customers. For example, a company may provide web-based e-mail services and have the capacity to deliver ads based on the e-mails exchanged over its system without disclosing the e-mails to a third party, because the company has integrated an advertising delivery system into its e-mail programs.[56] However, this prohibition does not apply to conduct that is authorized by the entities providing the ECS.[57] As a result, if a company has the capability to analyze the contents of communications stored on its systems without disclosing the contents of the communication to non-governmental third parties, it may be legally possible for them to do so without violating the SCA.

Remote Computing Services

The SCA to a lesser degree prohibits sharing of data by companies providing remote computing services (RCS). The statute defines an RCS as "the provision to the public of computer storage or processing services by means of an electronic communications system."[58] This is a relatively narrow definition. According to the DOJ, "[roughly] speaking a [RCS] is provided by an off-site computer that stores or processes data for a customer."[59] Such services are becoming more popular with the rise of cloud computing. However, given the nascent nature of the cloud computing industry, little case law has developed to further interpret what exactly an RCS is. Most websites likely are not providing an RCS, unless the website is offering an online storage

[52] 18 U.S.C. § 2702 (b).

[53] 18 U.S.C. § 2702 (c).

[54] 18 U.S.C. § 2710 (a).

[55] *Id.* It is worth noting that this provision would not appear to apply to Google's system described *supra* note 54, because Google claims that no "person" ever obtains the contents of the communication.

[56] *See* Google Privacy Center, http://www.google.com/intl/en/privacy/ads/ ("Google scans the text of Gmail messages in order to filter spam and detect viruses. The Gmail filtering system also scans for keywords in users' emails which are then used to match and serve ads. The whole process is automated and involves no humans matching ads to Gmail content.").

[57] 18 U.S.C. § 2701 (c).

[58] 18 U.S.C. § 2711 (2).

[59] DOJ Manual, *supra* note 50.

service.[60] Many websites collect and store customer data, but the storage is incidental to the other services being provided.[61] It seems unlikely that storage of data collected online or through other means of communications, that is incidental to the provision of other services, would be considered to be an RCS.

The SCA prohibits those providing RCS to the public from knowingly divulging the content of any communication which is carried or maintained by the service "(A) on behalf of, and received by means of electronic transmission from … a subscriber or customer of such service; (B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of the communication for purposes of providing any services other than storage or computer processing," unless an exception applies.[62]

The qualifications on this disclosure prohibition raise questions. Disclosure is prohibited for communications maintained "solely for the purposes of providing storage or computer processing services, if the provider is not authorized to access the contents of the communication for purposes of providing any services other than storage or computer processing."[63] At least one observer reads this to mean that disclosure of the contents of information will not be prohibited unless the service provider may only access the data for the purposes of storage or data processing.[64] If this interpretation is correct, it could be that very few entities that collect and store data online would be subject to the disclosure prohibition. Many entities with which consumers share their data online for storage and other purposes require that consumers allow the companies to access their data in order to serve advertising, and for other purposes beyond mere storage or processing.[65]

As a result, it appears that the SCA as it relates to RCS may have a relatively limited application in today's online environment, despite the forecasted migration to cloud computing. As long as online companies condition their services on having access to the contents of a person's communications for some reason other than "storage or computer processing," it is possible that

[60] *See* Steve Jackson Games, Inc. v. United States Secret Service, 816 F. Supp. 432 (W.D. Tex. 1993)(provider of a bulletin board service was providing a remote computing service).

[61] *See, e.g.*, In Re Jetblue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299 (E.D.N.Y. 2005)(finding that the airline, though it complied and stored customer data through its website, such storage was incidental to its provision of reservation services, and the airline was not providing an RCS).

[62] 18 U.S.C. § 2702 (b).

[63] *Id.*

[64] William Jeremy Robison, Note: Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act, 98 GEO. L.J. 1195 (2010).

[65] *See e.g.*, Google Privacy Policy, http://www.google.com/intl/en/privacy/privacy-policy.html (October 3, 2010) ("We may combine the information you submit under your account with information from other Google services or third parties in order to provide you with a better experience and to improve the quality of our services. For certain services, we may give you the opportunity to opt out of combining such information."); Google Privacy Center, Advertising and Privacy, http://www.google.com/intl/en/privacy/ads/ visited April 1, 2011 ("Google scans the text of Gmail messages in order to filter spam and detect viruses. The Gmail filtering system also scans for keywords in users' emails which are then used to match and serve ads. The whole process is automated and involves no humans matching ads to Gmail content."); Twitter Privacy Policy, http://twitter.com/privacy (November 16, 2010) ("We engage certain trusted third parties to perform functions and provide services to us. We may share your personal information with these third parties, but only to the extent necessary to perform these functions and provide such services, and only pursuant to obligations mirroring the protections of this privacy policy."). This is presented under the assumption that Google and Twitter provide, at some point in time, an RCS. However, analysis by a reviewing court in a particular case would be necessary for a final determination to be made.

the prohibition on disclosure in the SCA would not apply. However, there has been very little case law on the subject, and future court interpretations may differ depending on the circumstances of individual cases. As in the case of court interpretations of the phrase "electronic storage," a split in interpretations may occur as well.

As with providers of ECS, the SCA requires that the service be offered to the public. Therefore, a company that allows remote storage for its employees only may not be providing the service to the public, and therefore would not be providing an RCS.[66]

Furthermore, even if the communication is covered by the disclosure prohibition, an exception may apply. The relevant exceptions from the prohibition on disclosure are the same as the exceptions discussed above for providers of ECS.[67] Disclosure is allowed to the intended recipient, with consent of the subscriber to the RCS, or as may be necessarily incident to the rendition of the service or the protection of the property of the service provider. RCS, like ECS, providers may disclose more freely non-content information to non-governmental third parties than content information. RCS providers may disclose "a record or other information pertaining to a subscriber of such service (not including the contents of communications)" to any person who is not a governmental entity.[68] Therefore, for non-content information, an RCS provider may disclose subscriber information relatively freely. It becomes important, therefore, to analyze what is "content" and what is "non-content" information.

Content vs. Non-Content

The prohibitions on disclosure in the SCA apply only to the contents of communications. The statute defines content as "any information concerning the substance, purport or meaning of that communication."[69] Content, therefore, is clearly the text within the body of an e-mail, or the voice-mail stored on a server.[70] Less clear, perhaps, is whether the addressees of particular messages, the subject lines of these messages, or other identifying aspects of communications, would be considered to be the "content" of the communication. The DOJ posits that subject lines are, in fact, "contents."[71] On the other hand, an analogy to the telephone context in which telephone numbers dialed are not considered to be "contents" of the communication would seem to indicate that the addressee information for an e-mail is not "contents," as the DOJ and interpreting courts agree.[72] Most information maintained by ECS and RCS providers that is not

[66] *See* Andersen Consulting LLP v. UOP, 991 F. Supp. 1041, 1043 (N.D. Ill. 1998) (finding that the requirement that the service be offered to the public precluded an internal e-mail system from being subject to the SCA's disclosure prohibitions); DOJ Manual, *supra* note 50.

[67] 18 U.S.C. § 2702 (b).

[68] 18 U.S.C. § 2702 (c).

[69] 18 U.S.C. § 2510 (8).

[70] DOJ Manual, *supra* note 50.

[71] *Id.*

[72] *See* Hill v. MCI WorldCom Commc'ns, Inc. 120 F.Supp. 2d 1194 (S.D. Iowa 2000) (concluding that phone numbers of parties called are not the contents of the communication); DOJ Manual, *supra* note 50. Phone numbers and e-mail addresses are intuitively similar and it is likely that a reviewing court would find them to be equivalent and non-content information. However, as with all other aspects of the SCA, a fact specific inquiry would need to be done in each case to determine whether the information at issue is, indeed, the 'contents' of the communication." The answer may depend on which party in the process of the transmission and delivery of the communication is disclosing the information.

"contents" may fall under the category of customer records or other information pertaining to the subscriber.

The distinction between content and "non-content" information is important because, as noted above, the prohibitions on disclosure to non-governmental third parties in the SCA apply only to the contents of communications. Subscriber information can be freely disclosed to non-government entities.[73] According to the DOJ, "[common] examples of [customer records] include transactional records, such as account logs that record account usage; cell-site data for cellular telephone calls; and e-mail addresses of other individuals with whom an account holder has corresponded."[74] Also included in this category, when analyzing the permissibility of disclosure to non-government entities, is a customer's name, address, local and long distance telephone connection records, records of session times and durations, length and type of services, means and types of payments, etc.[75] As a result, there may be a wealth of identifiable information in customer records and subscriber records, but that information is not protected from disclosure to non-governmental entities by the SCA.

Section 631 of the Communications Act

It is also possible that privacy provisions of the Communications Act apply to agreements between cable operators acting as ISPs and online advertising providers.[76] Section 631 of the Communications Act provides basic privacy protections for personally identifiable information gathered by cable operators.[77] Specifically, cable operators must provide notice to subscribers, informing them of the types of personally identifiable information the cable operator collects, how it is disclosed, how long it is kept, etc.[78] Cable operators are prohibited from collecting personally identifiable information over the cable system without a subscriber's prior written or electronic consent.[79] Cable operators are also forbidden to disclose personally identifiable information without prior written or electronic consent of subscribers and must take action to prevent unauthorized access to personally identifiable information by anyone other than the

[73] *See* 18 U.S.C. § 2702.

[74] DOJ Manual, *supra* note 50.

[75] *Id.*

[76] Testimony of Ms. Leslie Harris, CEO of the Center for Democracy and Technology, *Privacy Implications of Online Advertising: Hearing Before the S. Comm. On Commerce, Science, and Transportation*, 110th Cong. (2008).

[77] Codified at 47 U.S.C. §551. It is important to note that those providing DSL Internet service over phone lines, such as Verizon or AT&T, would not be subject to the provisions of Section 631, because they are not cable operators. Testimony of Ms. Gigi B. Sohn, President, Public Knowledge, *Broadband Providers and Consumer Privacy: Hearing Before the S. Comm. On Commerce, Science, and Transportation*, 110th Cong. (2008)(hereinafter Public Knowledge Testimony), available at http://commerce.senate.gov/public/_files/SohnTestimony.pdf.

[78] 47 U.S.C. §551(a). The term cable operator "means any person or group of persons (A) who provides cable service over a cable system and directly or through one or more affiliates owns a significant interest in such cable system, or (B) who otherwise controls or is responsible for, through any arrangement, the management and operation of such a cable system." 47 U.S.C. § 552 (5). For the purposes of §551(a)-(g), the term cable operator also includes "any person who (i) is owned or controlled by, or under common ownership or control with, a cable operator, and (ii) provides any wire or radio communications service." 47 U.S.C. §551(a)(2).

[79] 47 U.S.C. §551(b).

subscriber or cable operator.[80] NebuAd has argued that Section 631 does not apply to the activities of cable operators when cable operators are acting as cable modem service providers.[81]

Section 631 governs the protection of information about subscribers to "any cable service or other service" provided by a cable operator. "Other service" is defined as "any wire or radio communications service provided using any of the facilities of a cable operator that are used in the provision of cable service."[82] In its order classifying cable modem services as "information services," the FCC stated the belief that "cable modem service would be included in the category of 'other service' for the purposes of section 631."[83] Furthermore, in 1992, Congress added the term "other services" to Section 631 as part of the Cable Television and Consumer Protection and Competition Act.[84] The House Conference Report on the law clarified that provisions redefining the term "other services" were included in order "to ensure that new communications services provided by cable operators are covered by the privacy protections" of Section 631.[85]

Section 631 is judicially enforced, however, and it is for the courts to interpret the scope of its application absent more specific guidance from Congress.[86] It is unclear whether all of the provisions of Section 631 encompass Internet services. "Other services" have been interpreted by at least one district court to encompass Internet services.[87] On the other hand, in 2006, the Sixth Circuit Court of Appeals found that the plain language of Section 631(b) precluded its application to broadband Internet service.[88] Section 631(b) prohibits cable operators from using their cable systems to collect personally identifiable information without the consent of subscribers.[89] The court based its decision that Internet services were not covered by this prohibition on its interpretation of the definition of "cable systems."[90] The court found that the systems that deliver Internet services are not the systems that Section 631(b) addresses, and therefore, cable operators were not prohibited by Section 631(b) from collecting personally identifiable information over systems that delivered Internet access services. The Supreme Court has yet to rule on this issue.

Even if Section 631(b) does not prevent cable operators from collecting personally identifiable information over broadband Internet services, Section 631(c) may prohibit the disclosure of such information to third parties regardless of whether the information was collected over the cable system.[91] Section 631(c) of the Communications Act states that "a cable operator shall not

---

[80] 47 U.S.C. §551(c).

[81] Memorandum from NebuAd, Inc., Legal and Policy Issues Supporting NebuAd's Services at 6.

[82] 47 U.S.C. Sec. §551(a)(2)(B).

[83] *In the Matter of Inquiry Concerning High-Speed Access to the Internet Over Cable and Other Facilities; Internet Over Cable Declaratory Ruling; Appropriate Regulatory Treatment for Broadband Access to the Internet Over Cable Facilities*, 17 FCC Rcd at 4854, ¶ 112.

[84] Cable Television and Consumer Protection and Competition Act, P.L. 102-385.

[85] H.Rept. 102-862.

[86] *See* 47 U.S.C. 551(f).

[87] *See* Application of the United States of America for an Order Pursuant to 18 U.S.C. Sec. 2703(D), 157 F. Supp. 2d 286, 291 (SDNY 2001)(finding that the notice requirement for the disclosure of personally identifiable information under 47 U.S.C. §551 included Internet services, except under 47 U.S.C. §551(h), which was exempt specifically from the broad definition of "other services").

[88] Klimas v. Comcast Cable, Inc., 465 F.3d 271, 276 (6th Cir. 2006).

[89] 47 U.S.C. §551(b)(1).

[90] *Klimas*, 465 F.3d at 276.

[91] 47 U.S.C. §551(c)(1).

disclose personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned and shall take such actions as are necessary to prevent unauthorized access to such information by a person other than the subscriber or cable operator."[92] If a cable operator, as an ISP, agrees to allow an online advertising provider to inspect traffic over its cable system and to acquire some of that information, it seems that the cable operator/ISP is disclosing information to the online advertising provider. Such disclosure would apparently be a violation of the Communications Act if (1) the information disclosed is personally identifiable information and (2) the cable operator/ISP is disclosing it without the prior written or electronic consent of the subscribers to whom the information pertains.

Whether online advertising providers are gathering personally identifiable information in order to provide their services is a matter of much debate. Section 631 does not define what personally identifiable information is; it defines what personally identifiable information is not. According to 631, personally identifiable information (PII) does not include "any record of aggregate data which does not identify particular persons."[93] Online advertising providers claim that they do not collect any personally identifiable information.[94] Public interest groups and other commentators disagree, citing scenarios in which data which was not supposed to contain personally identifiable information was used to identify individuals.[95] Because Section 631 is judicially enforced, it is likely that whether online advertisers are acquiring personally identifiable information as opposed to aggregate data that do not identify particular persons will be a determination made by a federal trial court. To date, there have been no cases addressing this question.

Assuming even that online advertising providers are gathering personally identifiable information, cable operators are allowed to disclose personally identifiable information as long as they obtain the prior written or electronic consent of the relevant subscribers, essentially an "opt-in" standard.[96] In the event that online advertising companies are determined to be gathering personally identifiable information and that Section 631(c) applies to cable operators in their provision of cable modem services, cable operators would be required to obtain consent for such disclosure under an "opt-in" regime.

Proposed Privacy Frameworks

While the FTC has had success in enforcing companies' privacy policies, some believe that a more comprehensive and uniform system is needed to protect consumer privacy and to inform consumers about the usage of the data that companies collect from them. To that end, the FTC and the DOC have proposed new privacy frameworks and have sought comment from the public on the proposals.

---

[92] 47 U.S.C. §551(c)(1). Cable operators, however, may collect such information without consent for the purposes of obtaining information necessary to provide cable services or other services provided to the subscriber or to detect unauthorized reception of cable communications. Cable operators may disclose personally identifiable information without consent when it is necessary to render cable services or other services provided by the cable operator to the subscriber, pursuant to a valid court order, and in other limited circumstances. 47 U.S.C. 551 (c)(2). These exemptions do not appear to apply in this case.

[93] 47 U.S.C. §551(a)(2)(A).

[94] *See, e.g.*, NebuAd Testimony.

[95] *See, e.g.*, CDT Testimony.

[96] 47 U.S.C. §551(c).

Federal Trade Commission's Proposed Framework for Protecting Privacy Online and Offline

As mentioned earlier, no federal statute expressly governs online data gathering, nor does any particular federal agency. Nonetheless, the Federal Trade Commission (FTC) has been able to utilize its general powers under Section 5 of the Federal Trade Commission Act and some of the authority delegated to the agency by the Fair Credit Reporting Act to take steps to protect consumer privacy in individual circumstance where, for instance, consumer information was mishandled or company practices were deceptively represented.

Recently, the FTC proposed a new framework for protecting consumer data collected both on and offline.[97] The proposal drew from previous FTC guidance for industry self-regulation, discussed below, as well as numerous meetings with the public and industry participants. The most controversial aspect of the FTC's proposal was for a universal "Do Not Track" system; however there were a number of other important suggestions contained in the proposal. The FTC appears to be attempting to create a system of both government oversight (if not regulation) of online privacy along with binding, consistent industry self-regulation.

The FTC first suggests that companies adopt a system being referred to as "privacy by design."[98] It is meant to encourage the protection of data to be built into a company's everyday business, making unauthorized or unexpected disclosure of data the exception rather than the rule. This does not appear to be a suggestion for government regulation, but rather a suggestion for what might be best practices.

Second the FTC proposed simpler disclosures and choices for consumers about the use of their data.[99] This could be accomplished in a number of ways, but the FTC's primary suggestion is for "streamlining" communications with consumers, perhaps through simplifications of their information-dense privacy policies. The FTC's observation here is that some data usage by companies is inevitable and commonly accepted. For example, certain data is needed to fulfill services ordered, and most consumers are aware that companies will use data previously provided by the consumer to market other products or services the company might have to offer. For unusual uses of data, or data practices that are not "commonly accepted," the FTC proposed that choice regarding whether a consumer would allow that use of his or her data be presented to the consumer at the time the data was being collected or before the product or service is delivered. The FTC further proposed clarifying which data usage practices were commonly accepted and which were not.

It is in this context that the FTC proposed the institution of a "Do Not Track" system.[100] The FTC posits that a "Do Not Track" system could be created either through federal legislation, or through robust industry self-regulation. In either case, the FTC suggested that the system be universal, persistent, easy to use, and enforceable.

---

[97] Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change**:** A Proposed Framework For Businesses And Policymakers (2010) available at http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

[98] *Id.* at 43, citing *Privacy by Design*, Information and Privacy Commissioner of Ontario, http://www.privacybydesign.ca.

[99] *Id.* at 52.

[100] *Id.* at 66.

Third, the FTC proposed improvements to transparency by improving their privacy policies.[101] One of the primary suggestions here is for some degree of privacy policy standardization in order to make it easier for consumers and the FTC to compare privacy practices at different companies. Lastly, the FTC proposed a consumer education effort.[102]

Comments were due on the proposed framework in January of 2011. The FTC expects to issue its final report by the end of 2011.

Department of Commerce Privacy Policy Framework

The Department of Commerce also recently released its own proposal for the creation of a national privacy framework.[103] Like the FTC, the DOC appears to aim for a system of government oversight combined with enforceable industry self-regulation. The DOC did not include a recommendation for a Do Not Track system in its proposal, however.

First, the DOC suggested the creation of universal Fair Information Practice Principles.[104] The principles would serve as a foundation for companies to tailor their information gathering and disclosure policies and would be designed to aid consumers in understanding what data was being collected and how it would be used. Second, the DOC suggested the development of "voluntary, enforceable codes of conduct in specific industries."[105] These codes would be developed by the FTC in conjunction with the Department of Commerce (DOC). The DOC also recommended the creation within the DOC of a Privacy Policy Office (PPO) which would work with the FTC to develop voluntary and enforceable codes of conduct. The DOC further encouraged efforts to create global interoperability. Lastly, the DOC recommended the creation of a national standard for security breach notifications.[106] Such rules would require an act of Congress to be created.

Self-Regulation

Currently, privacy on the Internet is governed primarily by self-regulatory regimes. The FTC has published its recommendations for industry best practices. Furthermore, other online service providers have created self-regulatory groups designed to develop privacy policies and, in some cases, enforce these policies. Some of these self-regulatory regimes are discussed below.

[101] *Id.* at 69.

[102] *Id.* at 78.

[103] Dept. of Commerce Internet Pol. Task Force, Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework, (2010), available at http://www.ntia.doc.gov/reports/2010/IPTF_Privacy_GreenPaper_12162010.pdf.

[104] *Id.* at 23.

[105] *Id.* at 41.

[106] *Id.* at 57.

Federal Trade Commission Online Advertising Self-Regulatory Principles

In February of 2009, the FTC released a set of Self Regulatory Principles for Online Behavioral Advertising.[107] Among other things, the principles clarified the types of advertising to which they should be applied and discussed what types of Non-PII should be included when notifying a consumer about what types of data the site or advertiser is collecting about him/her. A brief sketch of the principles follows.[108]

- The FTC's principles cover only online behavioral advertising. Online behavioral advertising means "the tracking of a consumer's online activities ***over time***." The principles make clear that so-called "first party" advertising (where no information is shared with a third party) and contextual advertising (where the ad is based on a single page visit or search) are not covered by the principles.
- According to the principles, websites engaged in online behavioral advertising should provide clear notification to consumers regarding the types of data being collected on the site and why, as well as the opportunity for consumers to choose whether their data may be collected for such purposes.
- Companies collecting the data should provide reasonable security for the data. The security measures should be concomitant with the sensitivity of the data (the more sensitive the data, the more protected it should be). The data should be retained only so long as necessary to fulfill a legitimate business purpose or as required by law.
- Companies must keep the promises they make to their customers. If the company decides to use *previously* collected data for purposes that differ materially from the uses the company described to the customer at the time data collection began, the company should obtain the affirmative express consent of affected customers.
- Companies should collect sensitive data (e.g., social security number, medical information, financial account information, etc.) for behavioral advertising only after obtaining affirmative express consent from the consumer.

The FTC noted that the release of these principles is a step in the ongoing process of evaluating the online behavioral advertising industry. The principles do not absolve the companies of their responsibilities under other governing laws (i.e., Section 5 of the Federal Trade Commission Act).

Industry Self-Regulatory Principles

The principles announced by the FTC were intended to aid self-regulatory organizations in designing privacy, data gathering, and consent guidelines for their members. There are at least three separate industry guidelines for online behavioral advertising, each of which takes a different approach to complying with the FTC's self-regulatory principles. The Interactive

[107] FTC Staff, *Self-Regulatory Principles for Online Behavioral Advertising* (Feb. 12, 2009), *available at* http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf.

[108] FTC Staff, *Self-Regulatory Principles for Online Behavioral Advertising*, at 46-47 (Feb. 12, 2009), *available at* http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf.

Advertising Bureau (IAB) has published their "Self-Regulatory Program for Online Behavioral Advertising" with which their member organizations must comply.[109] The Network Advertising Initiative (NAI) has released its "Self-Regulatory Code of Conduct."[110] A collection of ten advocacy organizations, known collectively as the Privacy Group Coalition, has recommended that regulation be built around a framework of Fair Information Practices (FIPs).[111]

Each of these sets of guidelines and principles share broad similarities, but have many important differences as well. For instance, they disagree on the definition of online behavioral advertising.[112] The definition of such advertising is broader under the IAB's guidelines than the NAI's Guidelines. Consequently, the IAB's requirements apply to a broader range of ad-delivery techniques than the NAI's. There are also differences among the levels of protection accorded to different types of data. Sensitive Data, for example, receives the highest level of protection from each regulatory framework. However, no single regulatory framework defines sensitive data in the same way.[113] There are also differences in enforcement mechanisms, notification and consent practices, data retention policies, etc.

Currently, if a consumer wishes to opt-out of online behavioral advertising data collection practices or even to find out what sites are collecting their data and how, the consumer must first figure out which companies are collecting their data and then determine to which industry self-regulatory organization the companies belong. If they belong to differing industry organizations, then different rules may apply to the same data sets that are being collected. As noted above, different definitions may apply to similar or identical terms, different methods of rescinding consent for the collection of data may also be applied depending upon the self-regulatory organization, and different methods of enforcement for companies that fail to comply with the agreed upon principles may apply as well.

In December of 2009, the Center for Democracy and Technology (CDT) issued a report entitled "Online Behavioral Advertising: Industry's Current Self-Regulatory Framework is Necessary, But

---

[109] Interactive Advertising Bureau, Self-Regulatory Program for Online Behavioral Advertising, July, 2009, available at http://www.iab.net/media/file/ven-principles-07-01-09.pdf (hereinafter IAB Guidelines).

[110] Network Advertising Initiative, Self-Regulatory Code of Conduct (2008), available at http://www.networkadvertising.org/networks/2008%20NAI%20Principles_final%20for%20Website.pdf (hereinafter NAI Guidelines).

[111] Privacy Group Coalition, Online Behavioral Tracking and Targeting, Legislative Primer, September 2009, available at http://www.uspirg.org/uploads/nE/27/nE27slalKXMxhjOdnoYLEA/Online-Privacy—Legislative-Primer.pdf.

[112] NAI defines Third-Party Online Behavioral advertising as "any process used whereby data are collected across multiple web domains owned or operated by different entities to categorize likely consumer interest segments for use in advertising online." NAI Guidelines, *supra* note 105. IAB defines online behavioral advertising more broadly as "the collection of data from a particular computer or device regarding web-viewing behaviors over time and across non-affiliate websites for the purpose of using such data to predict user preferences or interests to deliver advertising to that computer or device based on the preferences or interests inferred from such web viewing behaviors. Online Behavioral Advertising does not include the activities of First Parties, Ad Delivery or Ad-Reporting, or contextual advertising (i.e., advertising based upon the content of a web page being visited, a consumer's current visit to a web page, or a search query). IAB Guidelines, *supra* note 104.

[113] IAB defines sensitive data as "financial account numbers, Social Security numbers, pharmaceutical prescriptions, or medical records about a specific individual." IAB Guidelines, *supra* note 104. NAI defines sensitive data more broadly as "Social Security numbers or other government identifiers, insurance plan numbers, financial account numbers, information that describes the precise real time geographic location of an individual derived through location based services such as through GPS enabled services, and precise information about past, present, or potential future health or medical conditions or treatments, including genetic, genomic, and family medical history." NAI Guidelines, *supra* note 105.

Still Insufficient on its Own to Protect Consumers."[114] The report analyzes the current self-regulatory framework and provides recommendations for strengthening consumer protection in this rapidly growing industry. Among their recommendations to the self-regulatory organizations themselves, CDT calls upon Congress to enact a comprehensive privacy bill and to grant the FTC broader rulemaking authority to regulate in this area.

Author Contact Information

Kathleen Ann Ruane
Legislative Attorney
kruane@crs.loc.gov, 7-9135

[114] Center for Democracy and Technology, Online Behavioral Advertising: Industry's Current Self-Regulatory Framework is Necessary, But Still Insufficient on its Own to Protect Consumers, December 2009, available at http://www.cdt.org/files/pdfs/CDT%20Online%20Behavioral%20Advertising%20Report.pdf.