Privacy Law and Online Advertising

Kathleen Ann Ruane
Legislative Attorney

January 20, 2010

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

CRS Report for Congress
Prepared for Members and Committees of Congress

Summary

To produce revenue, websites have placed advertisements on their sites. Advertisers will pay a premium for greater assurance that the advertisement they are purchasing will be seen by users that are most likely to be interested in the product or service offered. As a result, technology has been developed which enables online advertisements to be targeted directly at individual users based on their web surfing activity. This practice is widely known as "behavioral" or "e-havioral" advertising.

This individual behavioral targeting has raised a number of privacy concerns. For instance, questions have been asked whether personally identifiable information is being collected; how the information collected is being protected; and whether current laws are being violated if data are being collected without the consent of the parties involved. It is often unclear whether current laws, such as the Electronic Communications Privacy Act and the Communications Act, apply to online advertising providers that are collecting data through click tracking, capturing search terms, and other methods. However, it is likely that in many cases these laws could be held to apply to such activities and that these methods of data collection would be forbidden unless consent is obtained from one of the parties to the communication. This report will examine the application of these statutes to online behavioral advertising in more detail.

There are no current federal regulations specific to online behavioral advertising. The FTC maintains that self-regulation is preferable to agency regulations, because the state of the industry is fluid and complex. To aid the industry in self-regulation of online behavioral advertising, in 2009, the FTC released a set of self-regulatory principles for the use of web sites and behavioral advertisers. The principles set forth guidance for the industry regarding the information that may be collected online and how companies should notify their customers about the collection. The FTC also applauded the efforts of industry groups to develop more detailed guidance on the issue. Organizations such as the Network Advertising Initiative, Interactive Advertising Bureau, and Privacy Group Coalition have created policies, similar to the FTC's recent release, which many online advertising providers have pledged to follow that represent industry best practices for protecting the privacy of web users.

For more information about the online advertising industry, see CRS Report R40908, *Advertising Industry in the Digital Age*, by Suzanne M. Kirchhoff.

Contents

Introduction and Technical Background 1
Electronic Communications Privacy Act 2
The Online Advertising Provider 2
The Internet Service Provider 3
The Consent Exception to ECPA 4
Data Collection Agreements Between Website Operators and Online Advertising Providers 5
Data Collection Agreements Between ISPs and Online Advertising Providers 6
Section 631 of the Communications Act 7
Federal Trade Commission Online Advertising Self-Regulatory Principles 10
Industry Self-Regulatory Principles 11

Contacts

Author Contact Information 12

Introduction and Technical Background

Many website operators produce income by selling advertising space on their sites. Advertisers will pay a premium for ads that are more likely to reach their target demographic. In other media, such as broadcasting, advertisers engage in targeting by purchasing advertising time during programs that those who buy their products are most likely to watch. The Internet presented new challenges and opportunities for advertisers to reach their target audiences. Technology has been developed that allows advertisers to target advertising to individual web users. This is seen as an advantage for advertisers, because, rather than aiming their ads at groups of people who visit a particular site, their ads are aimed at the individual user. This maximizes the odds that the user who sees the ad will be interested in the product or service it touts. Targeting advertising to individuals involves gathering information about that individual's web surfing habits. The collection of this information has raised concerns among some over the privacy of web activity, particularly if the data collected are personally identifiable. Some have alleged that online advertisers are violating privacy laws by collecting these data.

In online advertising's simplest form, a commercial website rents out "space" on its site to another website which places a hot link banner advertisement in that space.[1] The banner ad, when clicked, sends the user directly to the advertiser's website. In this scenario, no matter who visits a particular website, that user will see the same advertisement, regardless of whether he/she may be interested in that product or service. However, many advertisers will pay a premium for the increased likelihood that users viewing their advertisement would be interested in the product or service offered. As a result, technology has developed to more accurately target online ads to the desired audience.

Online advertising providers, such as DoubleClick and NebuAd, have developed the ability to target ads to individual Internet users who would be most interested in seeing those ads. These techniques are known generally as "behaviorally targeted advertising." Behaviorally targeted advertising delivers ads that are geared toward specific Internet users by tracking certain, though not necessarily all, web activity of each user and inferring each user's interests based on that activity. Most online advertising providers monitor individual Internet users by placing a "persistent cookie" on that user's computer. "Cookies" are small text files that can store information. "Persistent cookies" reside on a hard drive indefinitely, unlike most "cookies" which expire when a browser window is closed. Generally, online advertisers give the "cookies" they place on user computers a unique alphanumeric code that identifies that user to the advertising company purportedly without revealing any personally identifiable information. "Cookies" may be placed on an individual's computer when an individual visits a website affiliated with the online advertisement supplier; however, the exact moment of "cookie" placement may be different when the relevant advertising partnership is between a user's Internet Service Provider (ISP) and an online advertising provider.

[1] For a basic description of the technology involved in delivering behaviorally targeted advertising, please see the following source material: In re DoubleClick, Inc. Privacy Litigation, 154 F.Supp. 2d 497 (S.D.N.Y. 2001), In re Pharmatrak Privacy Litigation, 329 F.3d 9 (1st Cir. 2003), and Paul Lansing and Mark Halter, *Internet Advertising and Right to Privacy Issues*, 80 U. Det. Mercy L. Rev. 181 (2003). *See also*, Testimony of Mr. Robert R. Dykes, CEO of NebuAd Inc., *Privacy Implications of Online Advertising: Hearing Before the S. Comm. On Commerce, Science, and Transportation*, 110th Cong. (2008)(hereinafter NebuAd Testimony), available at http://commerce.senate.gov/public/_files/RobertDykesNebuAdOnlinePrivacyTestimony.pdf.

Once the cookie is in place, it gathers certain information related to that user's online activity on a continuous basis and relays that information to the online advertising provider. The advertising provider assembles that data into an individual profile that is then used to target advertising to that user's interests. This process is ongoing, but, in general, the user may opt out of continued monitoring at any point, assuming they are aware that it is occurring. In most types of behaviorally targeted advertising technology, the advertising firm gathers information about user activities on websites that are affiliated with the advertising firm. The behavioral advertiser DoubleClick, for instance, operates on this model. Information on individual users is transmitted to DoubleClick by DoubleClick's clients. In a newly emerging behavioral advertising model, the advertising provider is attempting to partner with the users' ISP. This partnership will presumably grant the advertising provider access to all web activity in which an ISP's subscribers engage. Both of these types of potential partnerships raise a number of questions regarding potential violations of existing privacy protections in federal law.

Electronic Communications Privacy Act

Concerns have been raised that online advertising providers, websites, and ISPs that agree to collect certain data generated by Internet traffic to behaviorally target advertising may be violating the Electronic Communications Privacy Act (ECPA)100 Stat. 1848, 18 U.S.C. 2510-2521.[2] 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.), which prohibits the interception of electronic communications unless an exception to the general prohibition applies.[3] ECPA also prohibits electronic communications service providers from intentionally divulging information while in transit to third parties, unless an exception applies. This section will discuss the potential application of ECPA to online advertising providers and the potential application of ECPA to ISPs.

The Online Advertising Provider

The first question that must be addressed is whether ECPA applies to the activities of online advertising providers. Online advertising providers are acquiring 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 they are acquiring that information while the communication is in transit.[4] Furthermore, these advertisers may acquire information, such as words entered into a search engine or answers to online forms, while it is in transit.[5] 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."[6] It is important to lay out the statutory definitions of each of

[2] 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.

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

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

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

[6] 18 U.S.C. §2511(1)(a).

the key terms in order to assess whether the ECPA prohibition and/or any of its exceptions applies 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.[7]
- "Contents" when used with respect to any wire, oral, or electronic communication includes any information concerning the substance, purport, or meaning of that communication.[8]
- "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.[9]

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 ECPA.[10]

Merely determining that this type of data acquisition by online advertisers is an interception for the purposes of ECPA does not end the analysis. ECPA excepts certain communication interceptions from its prohibition. The exception to ECPA 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.[11] The question of when and how consent to the interception may be given is addressed below.

The Internet Service Provider

The second question to be addressed is whether ECPA applies to ISP providers that would allow online advertising providers to gather data from traffic over the ISP's network. ECPA 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."[12] This section seems to apply to ISPs that would agree to allow

[7] 18 U.S.C. §2510(4).

[8] 18 U.S.C. §2510(8).

[9] 18 U.S.C. §2510(12).

[10] 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 Pharmatrk, 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).

[11] "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).

[12] 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 (continued...)

online advertising providers to acquire portions of the web traffic of ISP customers, because the ISP would be allowing the advertising providers to acquire the contents of communications while they are in transmission and 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 ECPA does not end the analysis. An ECPA 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."[13] 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 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.[14] 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."[15] If the ISPs obtain the consent of their customers to intercept some of their online activities, this exception to ECPA 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 ECPA

As noted above, interception of electronic communications is not prohibited by ECPA if one of the parties to the communications has consented to the interception. Consent is not defined by ECPA; nor do precise instructions of how and when consent may be obtained under ECPA appear in regulation. Therefore, it has been left largely to the courts to determine when consent to intercept a communication otherwise covered by ECPA's prohibitions has been granted.[16] There

(...continued)

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).

[13] 18 U.S.C. §2511(2)(a)(i).

[14] *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.

[15] 18 U.S.C. 2511(3)(b)(ii).

[16] *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 98-326, *Privacy: An Overview of Federal Statutes*
(continued...)

have been few cases dealing with ECPA's application to online advertising providers and none examining ECPA's application to agreements between ISP providers and online advertising providers. As a result, many open-ended questions exist regarding how to obtain adequate consent. This section first will examine whether the consent exception to ECPA applies to data collection agreements between online advertising providers and website operators. It will then examine whether and how the consent exception applies to data collection agreements between ISPs and online advertising providers.

Data Collection Agreements Between Website Operators and Online Advertising Providers

Agreements for online advertising providers to monitor certain web traffic may be between the online advertising provider and the website operators seeking to have ads placed on their sites. The advertising providers receive information about user activity on participating websites and aggregate that data to better target ads. In litigation against the online advertising provider DoubleClick for violations of ECPA, the court examined whether websites were "users" of electronic communications services under ECPA.[17] ECPA 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."[18] The court 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.[19] 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.[20]

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.[21] Consent for private interceptions of electronic communications cannot be granted if the purpose of the interception is the commission of criminal or tortious conduct.[22] The court noted that the focus of the determination of criminal or tortious purpose under ECPA 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."[23] 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

(...continued)

Governing Wiretapping and Electronic Eavesdropping, by Gina Stevens and Charles Doyle.

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

[18] 18 U.S.C. §2510(13).

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

[20] *Id.* at 514.

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

[22] 18 U.S.C. §2511(2)(d).

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

DoubleClick was motivated by tortious intent. As a result, the court found that the consent exception to ECPA was satisfied.[24]

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.[25] 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.[26] In collecting personally identifiable information by intercepting data without the consent of one of the parties, the online advertiser potentially had violated ECPA, but may have lacked the requisite intent to be found liable under the statute.[27] 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 generally are not violating ECPA, because the websites are "parties to the communication" with the ability to consent to interception. Based on these cases, the advertising providers will not be seen as running afoul of ECPA so long as the data the advertising providers collect do not fall outside the scope of the data the advertising providers' clients have 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."[28] 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.

---

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

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

[26] *Id.* at 20.

[27] *Id.* at 23.

[28] 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).

"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.[29] A similar debate is occurring now involving how ISPs should obtain consent from their customers to share data about their 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.[30] If the individual never responds, interception can never begin. "Opt-out" consent, by contrast, 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 and the advertising provider will begin such tracking *unless* the individual notifies the ISP or the advertiser that he or she does not grant permission for such activity.[31] 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.[32] The present question is whether "opt-out" consent is sufficient to satisfy the ECPA consent requirement. This question has yet to be addressed by a federal court or clarified by legislation or regulation. However, as discussed below, if Section 631 of the Communications Act applies to this type of data collection, "opt-in" consent may already be required for cable companies acting as ISPs (though this may not be required of telco companies such as Verizon or AT&T that operate as ISPs).

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.[33] Section 631 of the Communications Act provides basic privacy protections for personally identifiable information

---

[29] *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.

[30] *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).

[31] *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).

[32] NebuAd Testimony at 4.

[33] 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).

gathered by cable operators.[34] 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.[35] Cable operators are prohibited from collecting personally identifiable information over the cable system without a subscriber's prior written or electronic consent.[36] 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 subscriber or cable operator.[37] 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.[38]

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."[39] 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."[40] Furthermore, in 1992, Congress added the term "other services" to Section 631 as part of the Cable Television and Consumer Protection and Competition Act.[41] 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.[42]

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.[43] 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.[44] 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.[45] Section 631(b) prohibits cable operators from using their cable

[34] 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.

[35] 47 U.S.C. §551(a).

[36] 47 U.S.C. §551(b).

[37] 47 U.S.C. §551(c).

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

[39] 47 U.S.C. Sec. §551(a)(2)(B).

[40] *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.

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

[42] H.Rept. 102-862.

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

[44] *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").

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

systems to collect personally identifiable information without the consent of subscribers.[46] The court based its decision that Internet services were not covered by this prohibition on its interpretation of the definition of "cable systems."[47] 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.[48] Section 631(c) of the Communications Act states that "a cable operator shall not 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."[49] 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."[50] Online advertising providers claim that they do not collect any personally identifiable information.[51] 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.[52] 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-

[46] 47 U.S.C. §551(b)(1).

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

[48] 47 U.S.C. §551(c)(1).

[49] 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.

[50] 47 U.S.C. §551(a)(2)(A).

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

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

in" standard.[53] 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.

Federal Trade Commission Online Advertising Self-Regulatory Principles

In February of 2009, the FTC released a new set of Self Regulatory Principles for Online Behavioral Advertising.[54] These principles represent the most recent step in the FTC's ongoing examination of behavioral advertising practices, which began with the release of proposed self-regulatory principles for public comment in December of 2007.[55] Among other things, the finalized 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.[56]

- 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.

[53] 47 U.S.C. §551(c).

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

[55] FTC Staff, *Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles* (Dec. 20, 2007), *available at* http://www.ftc.gov/os/2007/12/P859900stmt.pdf.

[56] 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.

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). the FTC pledged to continue to monitor online behavioral advertising issues and its affect on consumer privacy.

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 Advertising Bureau (IAB) has published their "Self-Regulatory Program for Online Behavioral Advertising" with which their member organizations must comply.[57] The Network Advertising Initiative (NAI) has released its "Self-Regulatory Code of Conduct."[58] And 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).[59]

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.[60] 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.[61] There are also differences in enforcement mechanisms, notification and consent practices, data retention policies, etc.

---

[57] 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)

[58] 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).

[59] 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.

[60] 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 58. 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 web sites 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 57.

[61] IAB defines sensitive data as "financial account numbers, Social Security numbers, pharmaceutical prescriptions, or medical records about a specific individual." IAB Guidelines, *supra* note 57. 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 (continued...)

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 Still Insufficient on its Own to Protect Consumers.[62] 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 space.

Author Contact Information

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

(...continued)

58.

[62] 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.