An Overview of the Federal Wiretap Act, Electronic Communications Privacy Act, and State Two-Party Consent Laws of Relevance to the NebuAd System and Other Uses of Internet Traffic Content from ISPs for Behavioral Advertising

July 8th, 2008

Much of the content on the Internet (just like content in newspapers, broadcast TV, radio and cable) is supported in whole or part by advertising revenue. The Internet offers special opportunities to target ads based on the expressed or inferred interests of the individual user. There are various models for delivering targeted ads online. These range from the purely contextual (everyone who visits a travel site sees the same airline ad) to models that involve compiling information about the online behavior of individual Internet users, to be used in serving them advertisements. For years, Web sites have entered into agreements with advertising networks to use "cookies" to track individual users across Web sites in order to compile profiles. This approach has always been, and remains, a source of privacy concern, in part because the conduct usually occurs unbeknownst to most Internet users. Recent developments, including the mergers between online service providers and some of the largest online advertising networks, have heightened these concerns. The Center for Democracy & Technology has been conducting a major project on behavioral advertising, in which we have been researching behavioral advertising practices, consulting with Internet companies and privacy advocates, developing policy proposals, filing extensive comments at the FTC, and analyzing industry self-regulatory guidelines.

This memo focuses on the implications of a specific approach to behavioral advertising being considered by Internet advertising networks and Internet Service Providers (ISPs). This new approach involves copying and inspecting the content of each individual's Internet activity with the cooperation of his or her ISP.[1] Under this new model, an advertising network strikes a deal with an ISP, and the ISP allows the network to copy the contents of the individual Web traffic streams of each of the ISP's customers. The advertising network analyzes

[1] *See, e.g.,* Peter Whoriskey, *Every Click You Make*, WASH. POST (Apr. 3, 2008), http://www.washingtonpost.com/wp-dyn/content/article/2008/04/03/AR2008040304052.html?nav=hcmodule; Saul Hansell, *I.S.P. Tracking: The Mother of All Privacy Battles*, N.Y. TIMES: BITS BLOG (Mar. 20, 2008), http://bits.blogs.nytimes.com/2008/03/20/isp-tracking-the-mother-of-all-privacy-battles/?scp=1-b&sq=the+mother+of+all+privacy+battles&st=nyt.

the content of these traffic streams in order to create a record of each individual's online behaviors and interests. Later, as customers of the ISP surf the Web and visit sites where the advertising network has purchased advertising space, they see ads targeted based on their previous Internet behavior.

NebuAd is one such advertising network company operating in the United States. In the past few months, it has come to light that NebuAd was planning to partner with Charter Communications, a cable broadband ISP, to conduct trials of the NebuAd behavioral advertising technology. Several other smaller ISPs, such as Wide Open West (WOW!), CenturyTel, Embarq, and Knology, have also announced plans with NebuAd to trial or deploy its behavioral advertising technology. In response to concerns raised by subscribers, privacy advocates, and policymakers, Charter, CenturyTel and Embarq have delayed these plans, but NebuAd and other similar companies are continuing to seek new ISP partners.

The use of Internet traffic content from ISPs for behavioral advertising is different from the "cookie"-based model in significant ways and raises unique concerns.[2] Among other differences, it copies all or substantially all Web transactions, including visits to sites that do not use cookies. Thus, it may capture not only commercial activity, but also visits to political, advocacy, or religious sites or other non-commercial sites that do not use cookies.

In this memo, we conclude that the use of Internet traffic content from ISPs may run afoul of federal wiretap laws unless the activity is conducted with the consent of the subscriber.[3] To be effective, such consent should not be buried in terms of service and should not be inferred from a mailed notice. We recommend prior, express consent, but we do not offer here any detailed recommendations on how to obtain such consent in an ISP context. Also, we note that that the California law requiring consent of all the parties to a communication has been applied by the state Supreme Court to the monitoring of telephone calls when the monitoring is done at a facility outside California. The California law so far has not been applied to Internet communications and it

---

[2] Privacy concerns also apply to advertising-based models that have been developed for services, such as email, that ride over ISP networks. *See* CDT Policy Post 10.6, *Google GMail Highlights General Privacy Concerns* (Apr. 12, 2004), http://www.cdt.org/publications/policyposts/2004/6 (recommending express prior opt-in for advertising-based email service).

[3] Additional questions have been raised under the Cable Communications Policy Act. *See* Rep. Edward Markey and Rep. Joe Barton, *Letter to Charter Communications CEO in Regards to the Charter-NebuAd Data Collection Scheme* (May 2008), http://markey.house.gov/docs/telecomm/letter_charter_comm_privacy.pdf. In this memo, we focus on issues arising under the federal Wiretap Act, as amended by the Electronic Communications Privacy Act.

is unclear whether it would apply specifically to the copying of communications as conducted for behavioral monitoring purposes, but if it or another state's all-party consent rule were applied to use of Internet traffic for behavioral profiling, it would seem to pose an insurmountable barrier to the practice.

Wiretap Act

A. Service Providers Cannot "Divulge" The Contents of Subscriber Communications, Except Pursuant to Limited Exceptions

The federal Wiretap Act, as amended by the Electronic Communications Privacy Act, protects the privacy of wire, oral, and electronic communications.[4] "[E]lectronic communication" is defined as "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 photooptical system . . . ."[5] Web browsing and other Internet communications are clearly electronic communications protected by the Wiretap Act.

In language pertinent to the model under consideration, § 2511(3) of the Act states that "a person or entity providing an electronic communication service to the pubic shall not intentionally divulge the contents of any communications . . . while in transmission on that service to any person or entity other than an addressee or intended recipient . . . ."[6]

There are exceptions to this prohibition on disclosure, two of which may be relevant here. One exception specifies that "[i]t shall not be unlawful under this chapter for an . . . electronic communication service, whose facilities are used in the transmission of a[n] . . . electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a *necessary incident to the rendition of his service* or to the protection of the rights or property of the provider of that service."[7] We will refer to this as the "necessary incident" exception. The second exception is for

[4] 18 U.S.C. §§ 2510-2522.

[5] *Id.* § 2510(12).

[6] *Id.* § 2511(3)(a). Lest there be any argument that the disclosure does not occur while the communications are "in transmission," we note that the Stored Communications Act (SCA) states that "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." *Id.* § 2702(a)(1). We do not comment further here on the SCA because, in our judgment, the approach that has been described so far clearly involves the divulging of communications "while in transmission."

[7] *Id.* § 2511(2)(a)(i) (emphasis added). This analysis focuses on the capture of electronic communications and definitions are abridged accordingly.

disclosures with the consent of one of the parties.[8] We will discuss both exceptions below. We conclude that only the consent exception applies to the disclosure of subscriber content for behavioral advertising, and we will discuss preliminarily what "consent" would mean in this context.

B. With Limited Exceptions, Interception Is Also Prohibited

The Wiretap Act regulates the "interception" of electronic communications. The Act defines "intercept" as the "acquisition of the contents of any … electronic … communication through the use of any electronic, mechanical, or other device."[9]

The Wiretap Act broadly bars all intentional interception of electronic communications.[10] The Act enumerates specific exceptions to this prohibition.[11] Law enforcement officers, for example, are authorized to conduct interceptions pursuant to a court order. For ISPs and other service providers, there are three exceptions that might be relevant. Two we have mentioned already: the "necessary incident" exception and a consent exception.[12]

A third exception, applicable to interception but not to disclosure, arises from the definition of "intercept," which is defined as acquisition by an "electronic, mechanical, or other device," which in turn is defined as "any device or apparatus which can be used to intercept a[n] . . . electronic communication *other than*—(a) any telephone or telegraph instrument, equipment or facility, or any component thereof . . . (ii) being used by a provider of . . . electronic communication service in the *ordinary course of its business* . . . ."[13] This provision thus serves to limit the definition of "intercept," providing what is sometimes called the "telephone extension" exception, but which we will call the "business use" exception.

---

[8] *Id.* § 2511(3)(b)(ii).

[9] *Id.* § 2510(4).

[10] *Id.* § 2511(1).

[11] *Id.* § 2511(2).

[12] Separate from the consent provision for disclosure, the consent exception for interception is set forth in 18 U.S.C. § 2511(2)(d): "It shall not be unlawful under this chapter for a person not acting under color of law to intercept a[n] . . . electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception . . . ."

[13] *Id.* § 2510(5) (emphasis added).

C. The Copying of Internet Content for Disclosure to Advertising Networks Constitutes Interception

When an ISP copies a customer's communications or allows them to be copied by an advertising network, those communications have undoubtedly been "intercept[ed]."[14] Therefore, unless an exception applies, it seems likely that placing a device on an ISP's network and using it to copy communications for use in developing advertising profiles would constitute illegal interception under § 2511(1)(a); similarly, the disclosure or use of the intercepted communications would run afoul of § 2511(1)(c) or § 2511(1)(d), respectively.

D. The "Necessary Incident" Exception Probably Does Not Permit the Interception or Disclosure of Communications for Behavioral Advertising Purposes

The Wiretap Act permits interception of electronic communications when the activity takes place as "a necessary incident to the rendition of [the ISP's] service or to the protection of the rights or property of the provider of that service."[15] The latter prong covers anti-spam and anti-virus monitoring and filtering and various anti-fraud activities, but cannot be extended to advertising activities, which, while they may enhance the service provider's revenue, do not "protect" its rights. Courts have construed the "necessary incident" prong quite strictly, requiring a service provider to show that it *must* engage in the activity in order to carry out its business.[16] It is unlikely that the copying, diversion, or disclosure of Internet traffic content for behavioral advertising would be construed as a "necessary incident" to an ISP's business. Conceivably, an ISP could argue that its business included copying its subscribers communications and providing them to third parties for purposes of placing advertisements on Web sites unaffiliated with the ISP, but the ISP would probably have to state that that business existed and get the express agreement of its customers that they were

---

[14] *See, e.g.,* United States v. Rodriguez, 968 F.2d 130, 136 (2d Cir. 1992) (holding in context of telephone communications that "when the contents of a wire communication are captured or redirected in any way, an interception occurs at that time" and that "[r]edirection presupposes interception"); *In re* State Police Litig., 888 F. Supp. 1235, 1267 (D. Conn. 1995) (stating in context of telephone communications that "it is the act of diverting, and not the act of listening, that constitutes an 'interception'").

[15] 18 U.S.C. § 2511(2)(a)(i).

[16] *See* United States v. Councilman, 418 F.3d 67, 82 (1st Cir. 2005) (en banc) (holding that service provider's capture of emails to gain commercial advantage "clearly" was not within service provider exception); Berry v. Funk, 146 F.3d 1003, 1010 (D.C. Cir. 1998) (holding in context of telephone communications that switchboard operators' overhearing of a few moments of phone call to ensure call went through is a "necessary incident," but anything more is outside service provider exception).

subscribing to that business as well as the basic business of Internet access, which leads anyhow to the consent model that we conclude is necessary.

E. While It Is Unclear Whether the "Business Use" Exception Would Apply to the Use of a Device Installed or Controlled by a Party Other than the Service Provider, the Exception Does Not Apply to the Prohibition Against Divulging a Subscriber's Communications

The "business use" exception, § 2510(5)(a), constricts the definition of "device" and thereby narrows the definition of "intercept" in the Wiretap Act. There are two questions involved in assessing applicability of this exception to the use of Internet traffic content for behavioral advertising: (1) whether the device that copies the content for delivery to the advertising network constitutes a "telephone or telegraph instrument, equipment or facility, or any component thereof," and (2) whether an ISP's use of the device would be within the "ordinary course of its business."

We will discuss the "business use" exception at some length, because there has been considerable discussion already about whether copying of an ISP subscriber's communications for behavioral advertising is an "interception" under § 2511(1) of the Wiretap Act. However, even if the business use exception applied, an ISP would only avoid liability for the *interception* of electronic communications. It would still be prohibited from divulging the communications of its customers to an advertising network under the separate section of the Wiretap Act, § 2511(3), which states that a service provider "shall not intentionally divulge the contents of any communication . . . while in transmission on that service to any person or entity other than an addressee or intended recipient . . . ."[17] The business use exception does not apply to this prohibition against divulging.[18]

At first glance, it would seem that the business use exception is inapplicable to the facilities of an ISP because the exception applies only to a "telephone or telegraph instrument, equipment or facility, or any component thereof." However, the courts have recognized that ECPA was motivated in part by the

---

[17] 18 U.S.C. § 2511(3)(a).

[18] By adopting two different exceptions—"necessary incident" and "ordinary course"—Congress apparently meant them to have different meanings. Based on our reading of the cases, the necessary incident exception is narrower than the ordinary course exception. It is significant that the "necessary incident" exception applies to both interception and disclosure while the "ordinary course" exception is applicable only to interception. This suggests that Congress meant to allow service providers broader latitude in examining (that is, "intercepting" or "using") subscriber communications so long as they did not disclose the communications to third parties. This permits providers to conduct a range of in-house maintenance and service quality functions that do not involve disclosing communications to third parties.

"dramatic changes in new computer and telecommunications technologies"[19] and therefore was intended to make the Wiretap Act largely neutral with respect to its treatment of various communications technologies. The Second Circuit, for example, concluded in a related context that the term "telephone" should broadly include the "instruments, equipment and facilities that ISPs use to transmit e-mail."[20] Therefore, as a general matter, it should be assumed that the business use exception is available to ISPs.

However, it is not certain that the device used to copy and divert content for behavioral advertising would be considered to be a component of the service provider's equipment or facilities. In some of the behavioral advertising implementations that have been described, the monitoring device or process is not developed or controlled by the ISP but rather by the advertising network.

The second question is whether an ISP's use of a device to copy traffic content for behavioral advertising falls within the "ordinary course of its business." There are a number of cases interpreting this exception, but none of them clearly addresses a situation where a service provider is copying all of the communications of its customers. Many of the cases arise in situations where employers are monitoring the calls of their employees for purposes of supervision and quality assurance. "These cases have narrowly construed the phrase 'ordinary course of business.'"[21] Often such cases also involve notice to the employees and implied consent.[22] One court has stated that, even if an entity could satisfy the business use exception, notice to one of the parties being monitored would be required.[23] Other cases involve the monitoring of prisoners.

Some cases have interpreted "ordinary course" to mean anything that is used in "normal" operations. The D.C. Circuit, for instance, has suggested that monitoring "undertaken normally" qualifies as being within the "ordinary course of business."[24] In the context of law enforcement taping of the phone calls of prisoners, the Ninth and Tenth Circuits have concluded that something is in the "ordinary course" if it is done routinely and consistently.[25] It might be that

---

[19] S. Rep. No. 99-541, at 1 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3555.

[20] Hall v. Earthlink Network, Inc., 396 F.3d 500, 505 (2d Cir. 2005) (quoting S. Rep. No. 99-541 at 8).

[21] United States v. Murdock, 63 F.3d 1391. 1396 (6th Cir 1995).

[22] *E.g.,* James v. Newspaper Agency Corp., 591 F.2d 579 (10th Cir. 1979).

[23] *See, e.g.,* Adams v. City of Battle Creek, 250 F.3d 980, 984 (6th Cir. 2001).

[24] Berry v. Funk, 146 F.3d 1003, 1009 (D.C. Cir. 1998) (workplace monitoring).

[25] *See* United States v. Van Poyck, 77 F.3d 285, 292 (9th Cir. 1996); United States v. Gangi, 57 Fed. Appx. 809, 814 (10th Cir. 2003).

courts would give equal or greater latitude to service providers in monitoring their networks than they would give to mere subscribers or users.

Other circuit courts have used a more limited interpretation, concluding that "ordinary course" only applies if the device is being used to intercept communications for "legitimate business reasons."[26] Although the courts have not been entirely clear as to what that means, some have suggested that it is much closer to necessity than to mere profit motive.[27] One frequently-cited case explicitly holds that the business use exception does not broadly encompass a company's financial or other motivations: "The phrase 'in the ordinary course of business' cannot be expanded to mean anything that interests a company."[28]

Normal principles of statutory interpretation would require that some independent weight be given to the word "ordinary," so that the exception does not encompass anything done for business purposes. It is unclear, however, how much weight courts would give to the word "ordinary" in a rapidly changing market. It does not seem that the phrase "ordinary course of business" should preclude innovation, but courts might refer to past practices and normal expectations surrounding a line of business and specifically might look to what customers have come to expect.

Viewed one way, it is hard to see how the copying of content for behavioral advertising is part of the "ordinary course of business" of an ISP. After all, the ISP is not the one that will be using the content to develop profiles of its customers; the profiling is done by the advertising network, which does not even disclose to the ISP the profiles of its own subscribers. (The profiles are proprietary to the advertising network and it is careful not to disclose them to anyone.) Very few (if any) of the ads that are placed using the profiles will be ads for the ISP's services; they will be ads for products and services completely unrelated to the ISP's "ordinary course of business." Moreover, the ads will be placed on Web sites having no affiliation with the ISP. On the other hand, the

---

[26] *See* Arias v. Mutual Central Alarm Serv., Inc., 202 F.3d 553, 560 (2d Cir. 2000) (monitoring calls to an central alarm monitoring service).

[27] *See id.* (concluding that alarm company had legitimate reasons to tap all calls because such businesses "are the repositories of extremely sensitive security information, including information that could facilitate access to their customers' premises"); *see also* First v. Stark County Bd. of Comm'rs, 234 F.3d 1268, at *4 (6th Cir. 2000) (table disposition).

[28] Watkins v. L.M. Berry & Co., 704 F.2d 577, 582 (11th Cir. 1983). Watkins states: "We hold that a personal call may not be intercepted in the ordinary course of business under the exemption in section 2510(5)(a)(i), except to the extent necessary to guard against unauthorized use of the telephone or to determine whether a call is personal or not. In other words, a personal call may be intercepted in the ordinary course of business to determine its nature but never its contents." 704 F.2d at 583. This language supports the conclusion that the business use exception could not cover wholesale interception of ISP traffic, no more than switchboard operators can perform wholesale monitoring of telephone traffic.

ISP could argue that part of its business model—part of what keeps its rates low—is deriving revenue from its partnership with advertising networks.

The legislative histories of the Wiretap Act and ECPA weigh against a broad reading of the business use exception. Through these laws, Congress intended to create a statutory regime generally affording strong protection to electronic communications. Congress included limited, specific and detailed exceptions for law enforcement access to communications, and other limited, specific and detailed exceptions to allow companies providing electronic communications service to conduct ordinary system maintenance and operational activities. Congress gave especially high protection to communications content. If the business use exception can apply any time an ISP identifies a new revenue stream that can be tapped though use of its customers' communications, this careful statutory scheme would be seriously undermined.

F. The Consent Exception: The Context Weighs Heavily in Favor of Affirmative, Opt-In Consent from ISP Subscribers

Consent is an explicit exception both to the prohibition against intercepting electronic communications under the Wiretap Act and to the Act's prohibition against disclosing subscriber communications. The key question is: How should consent be obtained for use of Internet traffic content for behavioral advertising? Courts have held in telephone monitoring cases under the Wiretap Act that consent can be implied, but there are relatively few cases specifically addressing consent and electronic communications. However, in cases involving telephone monitoring, one circuit court has stated that consent under the Wiretap Act "is not to be cavalierly implied."[29] Another circuit court has noted that consent "should not casually be inferred"[30] and that consent must be "actual," not "constructive."[31] Yet another circuit court has stated: "Without actual notice, consent can only be implied when the surrounding circumstances *convincingly* show that the party knew about and consented to the interception."[32] Furthermore, "knowledge of the *capability* of monitoring alone cannot be

[29] Watkins. 704 F.2d at 581 ("Consent under title III is not to be cavalierly implied. Title III expresses a strong purpose to protect individual privacy by strictly limiting the occasions on which interception may lawfully take place.").

[30] Griggs-Ryan v. Smith, 904 F.2d 112, 117 (1st Cir. 1990).

[31] *In re* Pharmatrak, Inc. Privacy Litig., 329 F.3d 9, 20 (1st Cir. 2003); *see also* United States v. Corona-Chavez, 328 F.3d 974, 978 (8th Cir. 2003).

[32] Berry v. Funk, 146 F.3d 1003, 1011 (D.C. Cir. 1998) (internal quotation omitted).

considered implied consent."[33] The cases where consent has been implied involve very explicit notice; many of them involve the monitoring of prisoners' phone calls.[34]

Consent is context-based. It is one thing to imply consent in the context of a prison or a workplace, where notice may be presented as part of the daily log-in process. It is quite another to imply it in the context of ordinary Internet usage by residential subscribers, who, by definition, are using the service for personal and often highly sensitive communications. Continued use of a service after a mailed notice might not be enough to constitute consent. Certainly, mailing notification to the bill payer is probably insufficient to put all members of the household who share the Internet connection on notice.

Thus, it seems that an assertion of implied consent, whether or not users are provided an opportunity to opt out of the system, would most likely not satisfy the consent exception for the type of interception or disclosure under consideration here. Express prior consent (opt-in consent) is clearly preferable and may be required. While meaningful opt-in consent would be sufficient, courts would likely be skeptical of an opt-in consisting merely of a click-through agreement—i.e., a set of terms that a user agrees to by clicking an on-screen button—if it displays characteristics typical of such agreements, such as a large amount of text displayed in a small box, no requirement that the user scroll through the entire agreement, or the opt-in provision buried among other terms of service.[35]

In regards to consent, the model under discussion here is distinguishable from the use of "cookies," which were found to be permissible by a federal district court in a 2001 case involving DoubleClick.[36] In that case, the Web sites participating in the DoubleClick advertising network were found to be parties to the communications of the Internet users who visited those sites. As parties to

---

[33] Watkins, 704 F.2d at 581; *see also* Deal v. Spears, 980 F.2d 1153, 1157 (8th Cir. 1992) (holding that consent not implied when individual is aware only that monitoring might occur, rather than knowing monitoring is occurring).

[34] "The circumstances relevant to an implication of consent will vary from case to case, but the compendium will ordinarily include language or acts which tend to prove (or disprove) that a party knows of, or assents to, encroachments on the routine expectation that conversations are private. And the ultimate determination must proceed in light of the prophylactic purpose of Title III-a purpose which suggests that consent should not casually be inferred." Griggs-Ryan, 904 F.2d at 117.

[35] *See, e.g.,* Specht v. Netscape Commc'ns Corp., 306 F.3d 17 (2d Cir. 2002) (rejecting online arbitration agreement because, among other things, site permitted customer to download product without having scrolled down to arbitration clause and agreement button said only "Download"); United States v. Lanoue, 71 F.3d 966, 981 (1st Cir. 1995) ("Deficient notice will almost always defeat a claim of implied consent.").

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

the communications, the Web sites could consent to the use of the cookies to collect information about those communications. Here, of course, the ISPs are not parties to the communications being monitored and the interception or disclosure encompasses communications with sites that are not members of the advertising network. Therefore, the source of consent must be the IPS's individual subscribers, as it would be impossible to obtain consent from every single Web site that every subscriber may conceivably visit.

State Laws Requiring Two-Party Consent to Interception

A. Summary

In addition to the federal Wiretap Act, a majority of states have their own wiretap laws, which can be more stringent than the federal law. Most significantly, twelve states[37] require all parties to consent to the interception or recording of certain types of communications when such interception is done by a private party not under the color of law.

In several of these states—for example, Connecticut—the all-party consent requirement applies only to the recording of oral conversations. In others, the all-party consent rule extends to both voice and data communications. For example, Florida's Security of Communications Act makes it a felony for any individual to intercept, disclose, or use any wire, oral, or electronic communication, unless that person has obtained the prior consent of all parties.[38] Similarly, the Illinois statute on criminal eavesdropping prohibits a person from "intercept[ing], retain[ing], or transcrib[ing an] electronic communication unless he does so . . . with the consent of all of the parties to such . . . electronic communication."[39]

The most important all-party consent law may be California's, because the California Supreme Court held in 2006 that the law can be applied to activity occurring outside the state.

B. California

The 1967 California Invasion of Privacy Act makes criminally liable any individual who "intentionally taps, or makes any unauthorized connection . . .

[37] The twelve states are California, Connecticut, Florida, Illinois, Maryland, Massachusetts, Michigan, Montana, Nevada, New Hampshire, Pennsylvania, and Washington.

[38] Fla. Stat. § 934.03(1).

[39] Ill. Comp Stat. 5/14-1(a)(1).

or who willfully and without the consent of all parties to the communication . . . reads, or attempts to read, or to learn the contents or meaning of any message . . . or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place" in California.[40] It also establishes liability for any individual "who uses, or attempts to use, in any manner . . . any information so obtained" or who aids any person in doing the same.[41] The law has a separate section creating liability for any person eavesdropping upon or recording a confidential communication "intentionally and without the consent of all parties," whether the parties are present in the same location or communicating over telegraph, telephone, or other device (except a radio).[42]

Consent can be implied only in very limited circumstances. The California state Court of Appeals held in *People v. Garber* that a subscriber to a telephone system is deemed to have consented to the telephone company's monitoring of his calls if he uses the system in a manner that reasonably justifies the company's belief that he is violating his subscription rights, and even then the company may only monitor his calls to the extent necessary for the investigation.[43] An individual can maintain an objectively reasonable expectation of privacy by explicitly withholding consent for a tape recording, even if the other party has indicated an intention to record the communication.[44]

In *Kearney v. Salomon Smith Barney, Inc.*, the state Supreme Court addressed the conflict between the California all-party consent standard and Georgia's wiretap law, which is modeled after the federal one-party standard.[45] It held that, where a Georgia firm recorded calls made from its Georgia office to residents in California, the California law applied. The court said that it would be unfair to impose damages on the Georgia firm, but prospectively the case effectively required out-of-state firms having telephone communications with people in California to announce to all parties at the outset their intent to record a communication. Clear notice and implied consent are sufficient. "If, after being so advised, another party does not wish to participate in the conversation, he or she simply may decline to continue the communication."[46]

---

[40] Cal. Pen. Code § 631(a).

[41] *Id.*

[42] *Id.* § 632(a). The statute explicitly excludes radio communications from the category of confidential communications.

[43] 275 Cal. App. 2d 119 (Cal. App. 1st Dist. 1969).

[44] Nissan Motor Co. v. Nissan Computer Corp., 180 F. Supp. 2d 1089 (C.D. Cal. 2002).

[45] 39 Cal. 4th 95 (2006).

[46] Id. at 118.

C. The Implications of *Kearney*

The Kearney case arose in the context of telephone monitoring, and there is a remarkable lack of case law addressing whether the California statute applies to Internet communications. If it does, or if there is one other state that applies its all-party consent rule to conduct affecting Internet communications across state lines, then no practical form of opt-in, no matter how robust, would save the practice of copying Internet content for behavioral advertising. That is, even if the ISP only copies the communications of those subscribers that consent, and the monitoring occurs only inside a one-party consent state, as soon as one of those customers has a communication with a non-consenting person (or Web site) in an all-party consent state that applies its rule to interceptions occurring outside the state, the ISP would seem to be in jeopardy. The ISP could not conceivably obtain consent from every person and Web site in the all-party consent state. Nor could it identify (for the purpose of obtaining consent) which people or Web sites its opted-in subscribers would want to communicate with in advance of those communications occurring.

A countervailing argument could be made that an all-party consent rule is not applicable to the behavioral advertising model, since the process only copies or divulges one half of the communication, namely the half from the consenting subscriber.

Conclusion

The practice that has been described to us, whereby an ISP may enter into an agreement with an advertising network to copy and analyze the traffic content of the ISP's customers, poses serious questions under the federal Wiretap Act. It seems that the disclosure of a subscriber's communications is prohibited without consent. In addition, especially where the copying is achieved by a device owned or controlled by the advertising network, the copying of the contents of subscriber communications seems to be, in the absence of consent, a prohibited interception. Affirmative express consent, and a cessation of copying upon withdrawal of consent, would probably save such practices under federal law, but there may be state laws requiring all-party consent that would be more difficult to satisfy.

FOR MORE INFORMATION

Please contact: Jim Dempsey, Ari Schwartz, or Alissa Cooper
202-637-9800