PRIVATE ACTIONS CHALLENGING ONLINE DATA COLLECTION PRACTICES ARE INCREASING: ASSESSING THE LEGAL LANDSCAPE

Intellectual Property & Technology Law Journal

Eric C. Bosset
Simon J. Frankel
Mali B. Friedman
Stephen P. Satterfield

February 2011

The advent of the browser (or HTTP) cookie in the mid-1990s provided Web publishers and online advertisers with a new means of collecting information about consumer interests and for serving targeted advertisements on the basis of that information. This innovative technology also drew criticism from some circles and ultimately prompted several lawsuits against publishers, advertisers, and the ad networks that facilitate the relationship between them.[1] Although these suits largely were unsuccessful, the controversy over HTTP cookies led to modifications in browser privacy controls that gave users an increased ability to limit and delete cookies on their computers.

In the past decade, the number and quality of online data collection technologies have increased. At first, these technologies were subject to scrutiny principally by regulators, and industry responded by developing more robust privacy disclosures concerning their use. More recently, these next-generation technologies also have been a topic of heightened interest from the press—for example, an ongoing series in the *Wall Street Journal*[2]—and have inspired a spate of putative class action lawsuits relating to online data collection, alleging violations of various federal and state laws. Indeed, the past few years have witnessed the rise of a privacy plaintiffs' bar that has sought to transform statutes principally intended to criminally penalize wiretapping and computer hacking into vehicles for consumer protection litigation. For example:

- Recent suits have asserted class action claims against Internet service providers (ISPs) that allowed the online advertising company NebuAd to test a system using deep packet inspection (DPI) to profile subscribers' online activity anonymously for the purpose of serving targeted ads.[3]

- Several other suits allege that certain online marketing firms and their publisher affiliates improperly used "local shared objects," also known as "Flash cookies," to, for similar advertising reasons, track user activity and back up HTTP cookies for the purpose of restoring them later (also referred to as browser cookie re-spawning).[4]

- Still another recent suit asserts claims against an online marketing firm serving mobile devices, alleging that HTML5 software is used to install the mobile equivalent of browser cookies.[5]

The outcome of these suits may well depend on how far courts will extend the prohibitions in federal statutes such as the Electronic Communications Privacy Act (ECPA) and

the Computer Fraud and Abuse Act (CFAA). These statutes were drafted long before today's online environment could be envisioned, so their application to the technologies at issue in these suits poses interpretive difficulties for courts. As one federal court has observed, there is no "legislative or judicial history [for these statutes] to suggest that Congress intended to prohibit" Internet tracking activities.[6] "To the contrary," that court noted, "the histories of these statutes reveal specific Congressional goals—punishing destructive hacking, preventing wiretapping for criminal or tortious purposes, securing the operations of electronic communication service providers—that are carefully embodied in these criminal statutes and their corresponding civil rights of action."[7] The outcome of these lawsuits also may turn on whether traditional sources of commercial liability under state law, such as unfair competition and unjust enrichment, will be applied to electronic communications and digitally stored information.

An overview of the primary legal claims and defenses being asserted in these cases follows.

Electronic Communications Privacy Act

Title 1 of the Electronic Communications Privacy Act,[8] also known as the Wiretap Act, generally prohibits the interception, disclosure, or use of electronic communications. The Wiretap Act provides a private right of action and authorizes equitable relief, damages (including punitive damages), attorney's fees, and costs.[9] Compensatory damages consist of (1) actual damages and the profits made by the defendant from a violation or (2) statutory damages of $100 for each day of violation or $10,000, whichever is greater.[10]

In several suits, plaintiffs who subscribed to Internet service with companies that had allowed NebuAd to conduct a pilot test of its DPI technology have alleged that NebuAd intercepted and used ISP subscriber communications in violation of the Wiretap Act. The suits allege that NebuAd was permitted to test a device on the ISPs' networks that allowed NebuAd to intercept essentially all subscriber data transmitted over the networks. NebuAd allegedly used this data to construct anonymous interest category profiles on the basis of which it served targeted advertisements to subscribers. Although these lawsuits typically do not plead any quantifiable losses to individual subscribers resulting from the NebuAd test, the availability of a statutory damages alternative under the Wiretap Act could, if the cases are certified as class actions, impose on defendants a potential liability that is grossly disproportionate to any actual harm incurred by subscribers.

Plaintiffs in these cases face a number of obstacles. First, courts consistently have refused to construe the Wiretap Act as providing a cause of action for secondary (or aiding and abetting) liability.[11] Only an entity that actually intercepted, disclosed, or used a protected communication may be held liable under the Wiretap Act. Thus, claims being made against ISPs simply for contracting with NebuAd presumably should fail. Second, the Wiretap Act applies only when the *content* of a communication has been acquired or used. It remains, at best, unsettled whether technologies that only register anonymous clickstream activity and retain no personally identifiable information about the user even trigger the statute. Third, several statutory exceptions permit conduct that is otherwise prohibited by the Wiretap Act. Among these is consent by "a party to the communication"[12]—here, the user or the Web site server with which the user communicated. As the court in one of these cases recently held,[13] consent may be

demonstrated through evidence of appropriate notice to users through service terms, privacy policies or similar disclosures that inform users of the potential for monitoring.. Other statutory exceptions include the business use exception, which permits interceptions in the ordinary course of business,[14] and the service provider exception, which allows conduct that is a "necessary incident" to rendering service or protecting the service provider's rights or property.[15] As worded, these exceptions should, under a range of varying circumstances, foreclose liability under the Wiretap Act for behavioral advertising of the kind that NebuAd allegedly practiced.

One recently settled suit concerning the use of Flash cookies included a Wiretap Act claim against the online marketing firm Quantcast and certain Web publishers with which it did business.[16] The plaintiffs asserted that the defendants used Flash cookies to facilitate surreptitious tracking of online activity by circumventing users' privacy preferences. Like HTTP cookies, Flash cookies can be used to track Web browsing activity, but such cookies are stored locally in Flash players, not in browsers, and so may not be affected by browser privacy controls. Although the installation of Flash cookies can be prevented by adjusting settings in the Flash player, the plaintiffs contended that Quantcast and the other defendants buried user disclosures and improperly used such cookies for tracking. Further, the plaintiffs alleged that the defendants used Flash cookies to back up and restore (or "re-spawn") deleted HTTP cookies and that, through such means, the defendants "acquir[ed] and/or intercept[ed] . . . [the plaintiffs'] electronic communications" in violation of the Wiretap Act.[17]

Other plaintiffs asserting that the use of Flash cookies or similar tracking devices violates the Wiretap Act will face many of the same obstacles as the plaintiffs in the ISP suits. Perhaps even more difficult than clearing those hurdles will be convincing courts that the use of cookies to collect user data constitutes "interception" within the meaning of the Act. Although the plaintiffs in litigation against Quantcast suggested that a defendant's acquisition of electronic communications *by any means* is sufficient for liability, many courts have refused to construe the statute so broadly. In the jurisdiction where all of the Flash cookies suits are pending, for example, it is well established that only a communication obtained *during transmission*, rather than from electronic storage, may implicate the Wiretap Act.[18] Under this analysis, the use of cookies—text files installed by a server on users' computers—would not appear to involve the acquisition of communications during transmission. After a cookie is installed, information about the user's activity may be accessed by the server whenever the user visits a Web site on which the server's code appears. However, such information is available only after the user already has communicated with the Web site. As such, this does not appear to be the type of communication that falls within the ambit of the Wiretap Act.

Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act (CFAA)[19] generally prohibits computer intrusions, most of which involve accessing computers "without authorization," or "exceed[ing] authorize[d]" access, coupled with some specified consequence, such as obtaining personal information or causing damage.[20] As conceived, the CFAA was directed principally at criminal computer hacking. Private persons who can show "damage or loss" from prohibited conduct may sue for civil damages if the alleged offense causes any of five enumerated results, the most common of which is "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value."[21] Remedies under the CFAA are "limited to economic damages" and equitable

relief.[22] All of the lawsuits mentioned above allege that online advertising technology was used to access individuals' computers without authorization, causing actionable loss and damage. But the allegations of computer intrusion and damage in these suits are vague and conclusory.

Many of the defenses available under the CFAA are analogous to those described with respect to the Wiretap Act. For example, the CFAA also does not authorize secondary liability for civil claims; a plaintiff must show that each defendant directly engaged in a prohibited intrusion.[23] Additionally, the CFAA element that access be "unauthorized" is comparable to the "consent" defense afforded under ECPA, and courts are likely to consider users' acceptance of privacy policies and other forms that disclosed the possibility of access as constituting authorization for purposes of the CFAA.

In addition, the plaintiffs in these cases should have a difficult time making the required showing of tangible damage or economic loss associated with the alleged intrusion, as only specific types of damage and loss are cognizable under the CFAA. Loss is defined as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service."[24] "[D]amage" is any "impairment to the integrity or availability of data, a program, a system, or information."[25] Although precisely what type of harm is cognizable under the CFAA has varied under the case law, most courts look for quantifiable costs that are related to the functioning of the computer.[26] In contrast, claimed intangible harm, such as mental distress, typically is not cognizable.[27] At least one court has held that the transmission of a cookie, standing alone, is not actionable damage or loss under the statute.[28] Moreover, except under certain highly unusual circumstances,[29] the CFAA imposes a minimum $5,000 threshold of damages to maintain a civil lawsuit.[30] Because most courts have rejected attempts by plaintiffs to satisfy this requirement by aggregating many smaller, individual claims,[31] each individual plaintiff should have to show damage rising to this level in order to have standing to sue.

Significantly, the plaintiff in the *Green v. CableOne* ISP suit, which involves the NebuAd technology, recently dismissed the CFAA claim.

Video Privacy Protection Act

The Video Privacy Protection Act (VPPA),[32] which sometimes is referred to as the Bork Bill, was passed in response to a newspaper's publication of Judge Robert Bork's video rental records during his 1988 Supreme Court confirmation hearing. The statute prohibits "video tape service provider[s]" from disclosing information about any "consumer['s] . . . having requested or obtained specific video materials or services."[33] There is a private right of action for unlawful disclosure.[34] Remedies include actual damages, liquidated damages of $2,500, punitive damages, attorney's fees, costs, and equitable relief.[35] The plaintiffs in litigation against Quantcast asserted that the publisher defendants offering online video content violated the VPPA by disclosing user information to Quantcast. The statute appears inapplicable on its face to an online context. As a threshold matter, the definition of "consumer[s]," under the VPPA includes "renter[s], purchaser[s], or subscriber[s] of goods or services from a video tape service provider."[36] In cases such as those involving Quantcast, where the defendants generally make available their video

content for no charge, this statutory definition would not appear to be met. It is also doubtful that the publishers would be deemed "video tape service provider[s]" under the VPPA, as none is regularly engaged in the "rental, sale or delivery of prerecorded video cassette tapes or similar audio visual materials."[37] In short, it is difficult to imagine that courts will interpret this statute, which was explicitly written to cover a distinctly different media format, to regulate the kinds of activities being challenged in these lawsuits.

State Law Claims

Many of these suits also assert violations of state analogues to ECPA[38] and the CFAA[39] and of state common law prohibiting intrusion upon seclusion, trespass to chattels, and unjust enrichment. These state claims are based on the same conduct as the federal claims, and many of the defenses to the state counterparts will be similar. Moreover, at least one court has held that the federal Wiretap Act preempts comparable claims brought under state statutes.[40] Few courts have applied the various common law claims to the Internet in any context, but when they have done so, they have imposed similar requirements to those under the CFAA and ECPA, such as proof of scienter and tangible, quantifiable harm. For example, the Supreme Court of California has recognized the tort of trespass to chattels in the electronic communications context but has made it clear that a plaintiff must make a showing of harm similar to that required by the CFAA.[41]

Finally, some suits have asserted claims of deception under state consumer protection statutes.[42] Their applicability is unlikely because these claims do not involve any sale of goods or services, as such statutes typically require.

Class Certification

All of the suits cited in this article have been pleaded as class actions, but strong arguments militate against certification, including predominant questions in these cases relating to Internet access, computer damage, and user consent that may not be susceptible to class-wide resolution.

Conclusion

The wave of recent lawsuits against ISPs, publishers, and online advertising firms is likely to continue as more sophisticated technologies for tracking commercial Web browsing activity raise new concerns about consumer privacy. Current federal and state statutes are, at best, blunt tools to regulate the rapidly changing environment of the Internet. Courts are appropriately hesitant to impose potentially huge statutory damages authorized under existing statutes for conduct that provides demonstrable benefits to consumers—in the form of more relevant advertising or free Web content—while the corresponding risk to individual privacy is typically remote. It thus is not surprising that Congress is currently considering ECPA reform as well as comprehensive privacy legislation that would, in some circumstances, afford a private right of action to consumers whose personal information is collected without their consent. Similarly, the White House and federal agencies, such as the Federal Trade Commission and the Department of Commerce, are scrutinizing closely the data collection practices of entities operating online. These issues raise both important and competing public policy considerations

that will only be worked out over time. In the meantime, the courts are likely to remain an active forum for resolving these disputes.

Notes

[1] *See, e.g.*, In re Pharmatrak, Inc. Privacy Litig., 329 F.3d 9 (1st Cir. 2003), *claim dismissed on remand*, 292 F. Supp. 2d 263 (D. Mass. 2003); In re DoubleClick, Inc., Privacy Litig., 154 F. Supp. 2d 497 (S.D.N.Y. 2001).

[2] Articles in the series, entitled "What They Know," are available online at *http://online.wsj.com/public/page/what-they-know-digital-privacy.html* (last viewed 12/16/10).

[3] *See* Mortensen v. Bresnan Commc'ns LLC, No. 1:10-cv-0013-RFC (D. Mon.) (filed Feb. 16, 2010); Deering v. CenturyTel, Inc., No. 10-cv-00063-RFC (D. Mon.) (filed Feb. 11, 2010); Green v. Cable One, Inc., No. 1:10-cv-0259 (RBP) (N.D. Ala.) (filed Feb. 3, 2010); Manard v. Knology, Inc., No. 4:10-cv-15 (CDL) (M.D. Ga.) (filed Feb. 2, 2010); Kirch v. Embarq Mgmt. Co., No. 2:10-cv-02047-JAR-GLR (D. Kan.) (filed Jan. 26, 2010); Valentine v. WideOpen West, Fin., LLC, No. 1:09-cv-07653 (N.D. Ill.) (filed Dec. 9, 2009). Covington & Burling LLP represents the defendant in one of these cases, Green v. Cable One, Inc.

[4] *See* Rona v. Clearspring Techs., Inc., No. 2:10-cv-07786-GW-JCG (C.D. Cal.) (filed Oct. 18, 2010); Godoy v. Quantcast Corp., No. 2:10-cv-07662 (C.D. Cal.) (filed Oct. 13, 2010); Davis v. VideoEgg, Inc., No. 2:10-cv-07112-GW-JCG (C.D. Cal.) (filed Sept. 23, 2010); Intzekostas v. Fox Entm't Group, No. 2:10-cv-06586-GW-JCG (C.D. Cal.) (filed Sept. 2, 2010); La Court v. Specific Media, Inc., No. 8:10-cv-01256-JVS-VBK (C.D. Cal.) (filed Aug. 19, 2010); White v. Clearspring Techs., Inc., No. 2:10-cv-05948-GW-JCG (C.D. Cal.) (filed Aug. 10, 2010); Aguirre v. Quantcast Corp., No. 2:10-cv-05716-GW-JCG (C.D. Cal.) (filed July 30, 2010); Valdez v. Quantcast Corp., No. 2:10-cv-05484-GW-JCG (C.D. Cal.) (filed July 23, 2010). On September 21, 2010, *Aguirre* was consolidated with *Valdez* under the caption In re: Quantcast Adver. Cookie Litig.

[5] *See* Aughenbaugh v. Ringleader Digital, Inc., No. 8:10-cv-01407-CJC-RNB (C.D. Cal.) (filed Sept. 16, 2010).

[6] In re DoubleClick Privacy Litig., 154 F. Supp. 2d 497, 526 (S.D.N.Y. 2001).

[7] *In re DoubleClick*, 154 F. Supp. 2d 497, 526

[8] 18 U.S.C §§ 2510-2522.

[9] 18 U.S.C. § 2520(a)-(b).

[10] 18 U.S.C. § 2520(c).

[11] *See, e.g.*, Reynolds v. Spears, 93 F.3d 428, 432-33 (8th Cir. 1996); Perkins-Carrillo v. Systemax, Inc., No. 03-cv-2836, 2006 WL 1553957, at *15 (N.D. Ga. May 26, 2006).

[12] 18 U.S.C. § 2511(2)(d).

[13] *See Mortensen v. Bresnan Commc'ns LLC*, No. 1:10-cv-0013-RFC, 2010 WL 5140454, at *3-5 (D. Mont. Dec. 13, 2010).

[14] The business use exception is structured as a carve-out from the statutory definition of "intercept." *See* 18 U.S.C. §§ 2510(4), (5).

[15] *See* 18 U.S.C. § 2511(2)(a)(i).

[16] On December 3, 2010, a proposed settlement agreement was filed in the Central District of California that would resolve all claims in the suits against Quantcast, Clearspring, and their publisher partners. The settlement agreement does not contain any admission of wrongdoing or that Flash cookies were used in the manner alleged.

[17] Compl. ¶ 308, Valdez v. Quantcast Corp., No. 2:10-cv-05484-GW-JCG (C.D. Cal.).

[18] *See* Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878 (9th Cir. 2002).
[19] 18 U.S.C. § 1030.
[20] *See* 18 U.S.C. § 1030(a)(1)-(7).
[21] 18 U.S.C. § 1030(c)(4)(A)(i)(I).
[22] 18 U.S.C. § 1030(g).
[23] Although Congress recently amended § 1030(b) of the CFAA to impose *criminal* liability for conspiracy, *see* Pub. L. 110-326, Title II, § 206, 122 Stat. 3561, 3563 (2008), it made no change in the civil remedy provisions, which continue to provide a remedy only against "the violator." 18 U.S.C. § 1030(g); *see also* Smartix Int'l Corp. v. Mastercard Int'l LLC, No. 06-cv-5174, 2008 WL 4444554, at *1 n.2 (S.D.N.Y. Sept. 30, 2008); Garland-Sash v. Lewis, No. 05 Civ. 6827 (WHP), 2007 WL 935013, at *4 (S.D.N.Y. Mar. 26, 2007), *affirmed in relevant part by* Garland-Sash v. Lewis, No. 08-0740, 2009 WL 3227297 (2d Cir. Oct. 8, 2009).
[24] 18 U.S.C. § 1030(e)(11).
[25] 18 U.S.C. § 1030(e)(8).
[26] *See, e.g.*, Creative Computing v. Getloaded.com LLC, 386 F.3d 930 (9th Cir. 2004); Wilson v. Moreau, 440 F. Supp. 2d 81 (D.R.I. 2006), *affirmed*, 492 F.3d 50 (1st Cir. 2007); Czech v. Wall St. on Demand, Inc., 674 F. Supp.2d 1102, 1115-1118 (D. Minn. 2009).; Lyons v. Coxcom, Inc., No. 08-cv-02047-H-CAB, 2009 WL 347285, at * 8 (S.D. Cal. Feb. 6, 2009), *vacated on other grounds by* Lyons v. Coxcom, Inc., 2009 WL 6606941 (S.D. Cal. June 8, 2009).
[27] *See, e.g., Creative Computing*, 386 F.3d at 935.
[28] *See* Chance v. Avenue A, Inc., 165 F. Supp. 2d 1153, 1159 (W.D. Wash. 2001) (disapproved on other grounds by Creative Computing v. Getloaded.com LLC, 386 F.3d 930 (9th Cir. 2004)).
[29] *See* 18 U.S.C. § 1030(c)(4)(A)(i)(II-V).
[30] *See* 18 U.S.C. § 1030(c)(4)(A)(i)(I).
[31] *Lyons*, 2009 WL 347285, at * 8; Hayes v. Packard Bell, Nec. Inc., 193 F. Supp. 2d 910, 912 (E.D. Tex. 2001); Thurmond v. Compaq Computer Corp., 171 F. Supp. 2d 667 (E.D. Tex. 2001); *In re DoubleClick*, 154 F. Supp. 2d at 524. *But see* In re Apple & AT & TM Antitrust Litig., 596 F. Supp. 2d 1288, 1308 (N.D. Cal. 2008).
[32] 18 U.S.C. § 2710.
[33] *See* 18 U.S.C. § 2710(a)-(b).
[34] 18 U.S.C. § 2710(c).
[35] 18 U.S.C. § 2710(c).
[36] 18 U.S.C. § 2710(a)(1).
[37] 18 U.S.C. § 2710(a)(4).
[38] *See, e.g.*, Cal. Penal Code §§ 630, *et seq*. (California Invasion of Privacy Act).
[39] *See, e.g.*, Cal. Penal Code § 502 (California Computer Crime Law).
[40] Bunnell v. Motion Picture Ass'n of Am., 567 F. Supp. 2d 1148 (C.D. Cal. 2007).
[41] *See* Intel Corp. v. Hamidi, 71 P.3d 296, 302-304 (Sup. Ct. Cal. 2003).
[42] *See* Cal. Civil Code § 1750 (California Consumer Legal Remedies Act); Cal. Bus. & Profs. Code § 17200 (California Unfair Competition Law).

Reprinted with permission from the February 2011 issue of the *Intellectual Property & Technology Law Journal*, pages 3-8; © Wolters Kluwer.