Internet Privacy Concerns

Reignited in 2010

By Brian Balow and Tatiana Melnik

Fast Facts:

The top 50 websites installed, on average, 64 pieces of tracking technology.

Private litigation is increasing pertaining to the gathering and use of online data.

Federal agencies are again focusing on Internet privacy issues.

The issue of online privacy, or lack thereof, has been widely debated since people began sharing information on the Internet. In 1999, Scott McNealy, Sun Microsystems' chief executive officer, declared that people "have zero privacy" and they should "[g]et over it."[1] People's willingness to relinquish their privacy has fueled the growth of social networking websites such as MySpace and Facebook and, to a lesser extent, blogging websites such as Blogger and WordPress.[2] Mark Zuckerberg, Facebook's chief executive officer, has suggested that its users do not care about privacy and that Facebook's ever-changing privacy policy is simply a reflection of the "social norms."[3]

Internet Privacy is Making a Comeback

People are beginning to rethink their online activities as they become more educated about the ways in which companies use information and realize the impact of over-sharing. In mid-2010, the *Wall Street Journal* (WSJ), through its 2010 "What They Know" series, shined a bright light on the consequences of online information sharing.[4] The WSJ investigated, among other things, the extent to which website owners use technology to gather information about their users for advertising purposes. The WSJ found that the nation's top 50 websites—including dictionary.com, careerbuilder.com, and photobucket.com—"on average installed 64 pieces of tracking technology onto the computers of visitors, usually with no warning."[5] Moreover, current web technology can "scan in real time what people are doing on a Web page, then instantly assess location, income, shopping interests and even medical conditions."[6] In the December 2010 installment of the series, the WSJ found that iPhone and Android apps disclose an individual's username and password, contacts, age, gender, location, unique phone ID, and phone number to advertising companies,[7] likely without the individual's knowledge or consent. This information enables advertising companies to build comprehensive user profiles, forcing users to see ads that advertisers want them to see as they traverse the Internet.

Summary of Recently Settled Internet Privacy Litigation

This data gathering and sharing has not been well received by many consumers, who often feel they have been poorly informed regarding such activities and that their privacy was violated.

In 2008, Facebook, Blockbuster, Overstock, and a few other companies faced a class-action lawsuit over Facebook's Beacon program, which was designed to share purchases with friends by posting an update on a friend's "wall" when another friend made a purchase.[8] Plaintiffs claimed that Facebook violated consumers' privacy rights by failing to provide notice of Beacon's data-sharing activities and failing to obtain informed consent before disseminating personal information from Beacon-affiliated websites to Facebook.[9] Facebook settled the lawsuit by creating a $9.5 million fund to establish a nonprofit organization that will support projects and initiatives promoting online privacy, safety, and security.[10]

In July 2010, Google faced a similar complaint over its Google Buzz program, a social networking tool integrated into Gmail, Google's web-based e-mail program. Plaintiffs claimed that Google violated consumers' privacy rights because Gmail users were automatically enrolled in Google Buzz without their knowledge or consent, which caused the contacts with whom they e-mailed or chatted most frequently to be embedded in the users' Google Buzz profile.[11] Google Buzz then automatically retrieved and sent pictures, video, text, and other data that users posted to websites such as Picasa and YouTube to the e-mail accounts of the users' frequent contacts.[12] Google settled the lawsuit by creating an $8.5 million fund to support privacy organizations.[13]

Pending Internet Privacy Litigation

Several high-profile class-action lawsuits alleging Internet-based privacy violations were filed in 2010:

- *Valdez v Quantcast Corporation*[14]—In July, Edward Valdez and others filed a class-action lawsuit in California against Quantcast, ESPN, NBC, and a host of other defendants, alleging that their privacy, financial interests, and computer security were violated through a "pattern of covert online surveillance" because the defendants stored Flash cookies on the users' computers to respawn deleted browser cookies.[15]
- *Intzekostas v Fox Entertainment Group*[16]—In September, Erica Intzekostas, a Pennsylvania resident, filed a class-action lawsuit in California against Fox Entertainment Group and Clearspring Technologies, Inc., alleging that the defendants circumvented browser controls of individuals visiting the *American Idol* website and planted Flash cookies that respawned when users deleted the cookies.
- *Graf v Zynga Game Network, Inc*[17]—In October, Nancy Graf, a Minnesota resident, filed a class-action lawsuit in California against Zynga, a software company developing games such as "Farmville" for Facebook, alleging that Zynga violated game players' privacy by gathering and sharing personally identifiable information with third-party advertisers without players' consent.
- *Lalo v Apple Inc*[18] and *Freeman v Apple Inc*[19]—Both class-action lawsuits were filed in December in California. They stem from the WSJ article about Apple apps sharing consumers' information without their consent. The plaintiffs are also suing Dictionary.com, LLC; Pandora Media, Inc.; and The Weather Channel.

To See Who is Tracking You Using Flash Cookies:

- **If using Windows XP:** Click on the My Computer icon, go to your C drive, select Documents and Settings, select [Your Profile], select Application Data, select Macromedia, select Flash Player, click in each of the #SharedObjects and the macromedia.com folders, and click through until you see the Flash cookies.
- **If using Windows 7 or Vista:** Click on the My Computer icon, go to your C drive, select Users, select [Your Profile], select AppData, select Roaming, select Macromedia, select Flash Player, click in each of the #SharedObjects and the macromedia.com folders, and click through until you see the Flash cookies.
- **If using Mac OS X:** Go to your Library, select Preferences, select Macromedia, select Flash Player, click in each of the #SharedObjects and the macromedia.com folders, and click through until you see the Flash cookies.

Flash cookie files are saved with a .sol extension. You would need to use a specialized editor to view their contents because they are stored in binary format.

Action at the Federal Level

Several federal agencies have also expressed a renewed interest in Internet privacy issues. Both the Federal Trade Commission (FTC) and the Department of Commerce issued reports in December 2010 addressing these concerns.

The Federal Trade Commission Report

On December 1, 2010, the FTC, the nation's chief privacy policy and enforcement agency for 40 years, issued the long-awaited draft staff privacy report, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (FTC Report).[20] This preliminary report provides insight into the FTC staff's current views on best practices in the privacy area, particularly as they relate to online privacy and the use of consumer data.[21] The FTC advises that "[f]or every business, privacy should be a basic consideration—similar to keeping track of costs and revenues, or strategic planning."[22] Moreover, while the FTC recognizes the efforts made by industry, it concludes that such self-regulation efforts "have been too slow, and up to now have failed to provide adequate and meaningful protection."[23]

"New devices and applications allow the collection and use of personal information in ways that, at times, can be contrary to many consumers' privacy expectations."

The FTC Report sets forth a framework that "would apply broadly to *online* and *offline* commercial entities that collect, maintain, share, or otherwise use consumer data that can be reasonably linked to a specific consumer, computer, or device."[24] Such entities would include online and brick-and-mortar stores that use loyalty cards, apps installed on smartphones, and websites that collect consumer information such as Google Analytics. The FTC's framework has three components:

(1) **Privacy by design—**Companies should adopt a *privacy by design* approach to incorporate privacy protections into the everyday life of their business.[25] Such protections would include assigning personnel to oversee business privacy practices, having policies and procedures in place to govern privacy, collecting the minimum data necessary to fulfill their business function, and providing security for consumer data.

(2) **Simplified choice—**Companies should state the terms and conditions governing their privacy practices in a more concise manner than currently stated. The FTC advocates that consumer consent would be *implied* for a limited set of "commonly accepted practices" such as purchase order fulfillment, fraud prevention, legal compliance, first-party marketing, and internal operations (for example, consumer satisfaction surveys).[26] For other practices, companies should provide consumers with a choice. For behavioral advertising, the FTC endorses a "do not track" option that "could be accomplished by legislation or potentially through robust, enforceable self-regulation."[27]

(3) **Greater transparency—**Companies should provide consumers with greater transparency regarding how their data is used. The FTC concludes that "[i]n general, privacy policies do a poor job of informing consumers about companies' data practices or disclosing changes to their practices."[28] Moreover, "the aggregation of consumer data by information brokers and other non-consumer-facing entities raises significant policy issues."[29] Companies provide such transparency by drafting simpler privacy policies, providing consumers with choice on data sharing, and obtaining informed consent when making privacy policy changes.

The comment period for the FTC Report closed on January 31, 2011. A final report is expected later this year.

The U.S. Department of Commerce Green Paper

On December 16, 2010, the Commerce Department's Internet Policy Task Force issued its "green paper" on privacy, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*.[30] Commerce Secretary Gary Locke notes in his opening that "[n]ew devices and applications allow the collection and use of personal information in ways that, at times, can be contrary to many consumers' privacy expectations."[31]

Similar to the FTC Report, the green paper outlines the Commerce Department's privacy recommendations and proposed

initiatives. The task force, for example, contemplates establishing enforceable codes of conduct to be designed by industry and encouraged through increased FTC enforcement and legislation as well as collaboration among privacy stakeholders. Additionally, the task force advocates for the creation of a Privacy Policy Office (PPO) in the Department of Commerce which "would have the authority to convene multi-stakeholder discussions of commercial data privacy implementation models, best practices, [and] codes of conduct,…[as well as working] in concert with the Executive Office of the President as the Administration's lead on international outreach for commercial data privacy policy."[32] While the PPO would "serve as a center of commercial data privacy policy expertise,"[33] the task force recommends that the FTC remain the lead consumer privacy enforcement agency for the U.S. government.

Finally, the task force recommends that the federal government create a "comprehensive commercial data security breach framework for electronic records that includes notification provisions, encourages companies to implement strict data security protocols, and allows States to build upon the framework in limited ways."[34] Nearly all the comments received by the task force advocated, understandably, for a preemption of the current state breach-notification laws.[35]

Conclusion

Concerns over online privacy have increased in the last few years as privacy breaches and misuses of data believed to be private have come to light. Congress is also taking notice. In July 2010, Senator Thomas Carper and former Senator Robert Bennett introduced the Data Security Act of 2010 (S. 3579), which was referred to committee. Contrary to the assertions of several high-profile industry executives, as recognized by attorneys, the FTC, and the Department of Commerce, consumers do expect privacy in their online dealings. ■

Brian Balow is a member of Dickinson Wright and chairs the firm's IT Law Group. Mr. Balow was the firm's Business Technology and Telecommunications practice department manager from 2003 to 2008. He has nearly 20 years of experience in IT law-related matters, including counseling and advising on data security and privacy issues.

Tatiana Melnik is an associate with Dickinson Wright. Ms. Melnik sits on the SBM Information Technology Law Section Council and the Automation Alley Healthcare IT Committee. She is also a managing editor of the Nanotechnology Law & Business Journal. *She is a graduate of the University of Michigan Law School and the University of North Florida (BSc, information systems and BBA, international business).*

FOOTNOTES

1. PC World, Full Disclosure Blog, *Private Lives? Not Ours!* <http://www.pcworld.com/article/16331/private_lives_not_ours.html>. All websites cited in this article were accessed June 14, 2011.
2. But see Pew Research Center, *Pew Internet & American Life Project: Generations 2010* <http://pewinternet.org/~/media//Files/Reports/2010/PIP_Generations_and_Tech10.pdf > (finding that only 14 percent of teens aged 12–17 worked on their blogs compared with 28 percent in 2006, and speculating that this decrease is due, at least in part, to time being spent on social networking websites).
3. Arrington, *TechCrunch Crunchie Awards: Interview of Mark Zuckerberg* <http://www.ustream.tv/recorded/3848950>.
4. Wall Street Journal, *What They Know* <http://online.wsj.com/public/page/what-they-know-digital-privacy.html>.
5. Angwin, *The Web's New Gold Mine: Your Secrets* <http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html>.
6. *Id.*
7. Thurm & Kane, *Your Apps Are Watching You* <http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html>.
8. See *Lane v Facebook, Inc,* No 5:08-CV-03845-RS (ND Cal filed August 12, 2008).
9. *Id.*
10. See Settlement Agreement, *Lane v Facebook, Inc,* No 5:08-CV-03845-RS (September 18, 2009), available at <http://www.beaconclasssettlement.com/Files/SettlementAgreement.pdf>.
11. *In re Google Buzz User Privacy Litigation,* No 5:10-CV-00672-JW (ND Cal filed July 29, 2010).
12. *Id.* at 2.
13. Siegler, *Google Emails All U.S. Gmail Users About the Buzz Settlement—And to Say They're Not Getting a Dime* <http://techcrunch.com/2010/11/02/google-buzz-email>.
14. *Valdez v Quantcast Corporation,* No 2:2010-CV-05484 (CD Cal filed July 23, 2010).
15. A cookie is a small string of text stored in a user's computer by a web browser. These browser cookies can store website preferences, shopping-cart contents, and authentication information. Text cookies are not executable code and thus cannot respawn or replicate themselves. Flash cookies are commonly used because they are not deleted when people clear their browser cookies and they can be used to respawn deleted cookies. See generally Singel, *You Deleted Your Cookies? Think Again* <http://www.wired.com/epicenter/2009/08/you-deleted-your-cookies-think-again/>.
16. *Intzekostas v Fox Entertainment Group,* No 2:2010-CV-06586 (CD Cal filed September 2, 2010).
17. *Graf v Zynga Game Network Inc,* No 3:2010-CV-04680 (ND Cal filed October 18, 2010).
18. *Lalo v Apple Inc,* No 5:2010-CV-05878 (CD Cal filed December 23, 2010).
19. *Freeman v Apple Inc,* No 5:2010-CV-05881 (CD Cal filed December 23, 2010).
20. Federal Trade Commission, *FTC Staff Issues Privacy Report, Offers Framework for Consumers, Businesses, and Policymakers* <http://www.ftc.gov/opa/2010/12/privacyreport.shtm>.
21. Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* <http://www.ftc.gov/os/2010/12/101201privacyreport.pdf>.
22. *Id.* at i.
23. *Id.* at iii.
24. *Id.* at v (emphasis added).
25. *Id.* at 41.
26. *Id.* at 53–54.
27. *Id.* at 66.
28. *Id.* at 69.
29. *Id.* Data aggregation is generally the process of combining multiple sources of data for a specific purpose. Advertising companies aggregate data from various websites to create targeted advertising in an effort to increase sales.
30. U.S. Dept. of Commerce, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework* <http://www.ntia.doc.gov/reports/2010/IPTF_Privacy_GreenPaper_12162010.pdf>.
31. *Id.* at i.
32. *Id.* at 45.
33. *Id.*
34. *Id.* at 57.
35. *Id.*