Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

The Dawn Of Internet Privacy?

Law360, New York (April 22, 2011) -- Sens. John Kerry, D-Mass., and John McCain, R-Ariz., on April 12 submitted a bipartisan bill to the Senate called the Commercial Privacy Bill of Rights Act of 2011.

The act seeks to regulate, for the first time, the extent to which online companies can collect and use the personal data of users of their Web services — a controversial practice often referred to as "data-mining." Not surprisingly, reaction to the act has been mixed.

Regardless of whether the act provides much needed privacy protection for Web users or is a legislative overreaction, as some contend, it clearly reflects a trend toward heightened scrutiny of Internet data-mining activities and may increase the likelihood of privacy-related litigation against online companies and Internet providers.

What Is Data-Mining?

The process by which online companies track, aggregate and analyze user data is often referred to as "data-mining." This is done in a number of ways, the most common of which is through "cookies" — pieces of text stored on a user's computer by Web browsers such as Internet Explorer, Google Chrome and Firefox.

Mobile applications (apps) are also a growing source of this information. Cookies serve a variety of purposes, most of which are perfectly legitimate, such as storing Web site preferences, passwords and authentication information. Cookies can also be used, however, to track various Web sites visited by the user. In this fashion, online companies are able to gather information about users that is often used to facilitate targeted advertising.

For example, if a user were to visit a number of Web sites about fishing, the company tracking the information can create a user profile noting that the user is a fishing aficionado, which can then be sold to fishing equipment companies. Many companies are willing to pay for this information because it allows them to identify and specifically advertise to people they believe to be interested in their products.

While these uses are generally innocuous, critics of data-mining note that sensitive personal information can also be discovered through these processes, often without a user's knowledge. To complicate matters, while Internet users concerned about data-mining can easily remove cookies from their browser, advanced "super cookies" — which embed in programs such as Adobe Flash and Microsoft Silverlight — regenerate themselves even after a user has deleted them from their browser and are much harder to permanently remove.

Washington Takes Notice

Public awareness and concern over the practice of data-mining has grown over the last few years and has led to increased scrutiny by the federal government. Last year the FTC asked Web browser manufacturers to voluntarily implement features designed to prevent unauthorized Internet tracking, with mixed results.

While both Firefox and Internet Explorer have announced that they plan to introduce some form of "do not track" technology, their proposals are fairly limited in scope.

In the meantime, Congress — spurred by the executive branch — has not been idle. Two House bills proposed in February sought to regulate data-tracking activities by creating a "do not track" list and a baseline Internet privacy law — HIPAA for the Web. Both bills remain in committee.

Congress's latest attempt to protect Internet users from unwelcome data tracking activities is the Commercial Privacy Bill of Rights Act of 2011 proposed by Sens. Kerry and McCain.

The Commercial Privacy Bill of Rights Act of 2011: Key Provisions

The act attempts to regulate the gathering of personally identifiable information collected on and off the Internet in two ways. First, the act seeks to compel companies seeking to gather data to provide "transparent notice of practices and purposes" for which the information is being gathered. See The Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong. § 201 (2011).

To accomplish this goal, the act provides that, within 60 days of the enactment of the act, the Federal Trade Commission will initiate a rule-making proceeding to require each entity covered by the act "to provide clear, concise and timely notice to individuals of — a) the practices of the covered entity regarding the collection, use, transfer and storage of covered information; and b) the specific purposes of these practices." Id. at § 201(a)(1).

The act also requires that regulations be put in place to compel covered entities to provide notice before changing such practices. The FTC is empowered to provide sample notices and guidance as to how to comply with their regulations.

The second goal of the act is to force data gathering entities to provide a way for users to prevent disclosure of their personal information. Specifically, the bill provides that the FTC must, within 180 days of the passage of the act, initiate a rule-making procedure to "offer individuals a clear and conspicuous mechanism for opt-out consent for any use of their covered information that would otherwise be unauthorized use" and "to offer individuals a robust, clear and conspicuous mechanism for opt-out consent for the use by third parties of the individuals' covered information for behavioral advertising or marketing." Id. at § 202(a)(1)-(2).

In addition to the two opt-out procedures, the act requires that individuals also be offered an opt-in mechanism for "the collection, use or transfer of sensitive personally identifiable information" Id. at §202(a)(3) — such as health-related information.[1]

Significantly, third parties to whom user data is lawfully transmitted also must comply with the scope of the authorization granted by the user. Id. at §202(b). The act forbids companies from gathering data that is unnecessary to deliver or improve a service or make a transaction absent authorization. See id. at §§301–303.

The act's enforcement provisions are a mixed bag for online companies. The FTC has primary jurisdiction to enforce the act, although state attorneys general are also empowered to bring a civil action under the act, under certain conditions. Id. at 403. In a victory for online companies, however, the act does not create a private right of action. Id. at § 406.

Civil penalties are available under the act. Covered entities that violate the act are subject to "a civil penalty equal to the amount calculated by multiplying the number of days that the entity is not in compliance with such title by an amount not to exceed $16,500." See id. at § 404(a). Maximum liability for any related series of violations is capped at $3 million. Id. at § 404(c).

Public Reaction to the Act

Initial reaction to the bill has been mixed. Some privacy advocates are pleased that legislative action has been taken to address the practice of data-mining, but others have criticized the bill for not going far enough.

More specifically, privacy advocates have argued that the act relies too much on opt-out and opt-in mechanisms on individual sites which users may ignore or find too cumbersome to use — rather than simply allowing users to register on a federal "do not track" list and thereby preclude all use of their personal data online.

On the flip side, providing users with discretion to allow tracking activities by particular sites permits certain kind of data-mining that may benefit the user, such as benign targeted advertising.

Legal Impact of the Act

If passed, the act would apply to any entity that "collects, uses, transfers or stores covered information concerning more than 5,000 individuals during any consecutive 12-month period" and which is within the authority of the FTC.[2]

As a result, even organizations that use the data only for internal purposes are within the act's purview and should be aware that modifications to their data-collecting procedures may soon be necessary. Online companies that fail to take necessary steps under the act could face significant civil penalties.

Increased legislative scrutiny of data-mining activities is mirrored by a rise in civil litigation over privacy violations. For example, in the recently filed class action lawsuit In re Zynga Privacy Litig., No. 10-cv-04680 (N.D. Cal.), the creators of the popular online app FarmVille, accessible through Facebook, have been sued for allegedly transmitting users' real names and other information to third parties for profit without prior authorization in violation of Facebook's privacy policy.

Facebook itself has been sued for similar sale of data, allegedly in violation of California's Unfair Competition Law among others. See In re: Facebook Privacy Litig., 5:10-cv-02389-JW (2010). While these lawsuits are in their early stages and the likelihood of success is unknown, the potential liability is significant, with each class numbering in the millions.

Regulation of the Internet remains a hot button issue and one in which the landscape is likely to continue to change in the near future. While it is uncertain that the Commercial Privacy Bill of Rights Act of 2011 will pass through Congress and be signed into law, there is a reasonable likelihood that some form of regulation will be passed in the near future.

Until the law in this field is more fully developed, companies that gather or make use of data gathered through online tracking should continue to evaluate their processes and carefully consider how user data is tracked and shared.

--By Timothy C. Blank, Steven G. Bradbury, Philip N. Yannella and Christopher R. Boisvert, Dechert LLP

Timothy Blank is managing partner of Dechert's Boston office. Steven Bradbury is a partner in the firm's Washington, D.C., office. Philip Yannella is a partner in the firm's Philadelphia office. Christopher Boisvert is an associate in the firm's Philadelphia office.

[1] Certain uses, such as transaction processing and fraud prevention, are exempted from this procedure by the Act.

[2] Common carriers subject to the Communications Act of 1934 certain non-profit organizations are also subject to the provisions of the proposed Act.