



# ELECTRONIC COMMERCE & LAW



## REPORT

Reproduced with permission from Electronic Commerce & Law Report, 14 ECLR 1597, 11/11/09, 11/11/2009. Copyright © 2009 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

### Privacy

#### **Privacy Advocates Urge FTC, Lawmakers To Scrutinize Data-Sharing in Web Privacy Probe**

**C**ompeting views of the direction the government should take on data privacy policy will be aired next month when the Federal Trade Commission convenes a day-long discussion of the issues among business leaders, government officials, and privacy policy advocates.

Privacy advocates are pressing for better notice to individuals, particularly with respect to the third-party transfers that take place among marketers and technology providers wielding new, sophisticated marketing and data analysis technologies. An official with the Washington-based policy group Electronic Privacy Information Center told BNA that the FTC should press businesses to comply with the Organization for Economic Cooperation and Development's 1980 fair information practices.

Fair information practices, in the OECD's formulation, provide robust notice and limitation protections, a right of access and transparency, along with obligations on the part of businesses to reasonably safeguard data under their control.

Representatives of the business community, however, would like the FTC to consider an alternative privacy framework that emphasizes the type of use planned for the consumer's information: For benign uses, notice requirements should be relaxed, while in the case of unexpected or intrusive data uses, notice would be more robust.

On the legislative front, the House Commerce Committee approved a bill (H.R. 3126) Oct. 29 that would give the Federal Trade Commission new rulemaking and enforcement authority (14 ECLR 1575, 11/4/09). The committee may also take up long-promised comprehensive privacy legislation, though no legislation has been introduced as yet.

One possible outcome of the ongoing policy development process is the creation of an entirely new regulatory framework that contains both notice-based and harm-based compliance obligations for business.

**FTC Revisiting Privacy Strategy.** FTC Chairman Jon Leibowitz has pledged to update the agency's approach to consumer protection online, and as early as next year the commission could issue new online privacy guidance (14 ECLR 1319, 9/16/09).

The commission requested information Sept. 15, ahead of a series of roundtable events about companies' data-collection, use, and sharing practices, and related benefits and risks (14 ECLR 1372, 9/23/09). The event is set for Dec. 7.

"We are taking a look at a number of technologies and business practices—including social networks, cloud computing, mobile, data broker relationships, and behavioral advertising—and will assess both the benefits and risks of those practices," Christopher Olsen, assistant director of the FTC's division of privacy and identity protection, told BNA. "We want to understand the implications."

**EPIC Urges Close Look at Current Practices.** Lillie Coney, associate director of the Electronic Privacy Information Center, told BNA that the FTC needs to focus more attention on major internet firms that are shaping business practices online, particularly surrounding how their privacy practices may change over time.

She said the commission should examine how companies are sharing consumer data across multiple online platforms, and take action if those sharing relationships are unfair or deceptive. If the FTC lacks the resources or statutory authority to do so, they should ask Congress for it, she said.

Coney said that EPIC wants the FTC to look carefully at how the largest online companies, especially Google, are approaching online privacy issues. Coney listed several concerns EPIC has regarding Google:

- consumer choice is not a realistic consideration with so many benefits and services now only available online;

- the online collection, retention, and use of personal information is not well known nor understood to inform policy makers and decision makers on how to best protect the public;

- new services are developed and deployed without consideration for the privacy consequences they may pose;

- the company has expressed support for policies that protect privacy by instituting programs that it deems appropriate; and

- there are no limitations that direct that once privacy measures are instituted by a private company, outside of the dictates of law or public policy that they cannot change that policy at their discretion.

EPIC has advocated that the FTC should focus more attention on the major Internet firms that are shaping business practices in the online environment. “Too much of the FTC’s privacy work focuses on activities that are inconsequential for most Internet users,” EPIC told the FTC in an Oct. 27 letter.

Coney told BNA that EPIC is particularly concerned about consumer rights in the cloud computing space, and data-sharing between social networks and third party sites such as search engines and feeds.

“All kinds of information is being stored on cloud services, and could be used to disadvantage consumers if marketers can get it,” Coney said. Consumers should have a right to regain that data, even if service is terminated, and to understand how that data may be used for other purposes, she added.

“This may not be a workable solution for much longer. Once the amount of information on the cloud exceeds the capacity of personal devices to hold that information then customer choice becomes constrained,” Coney said.

**Business Group Supports Privacy Principles.** The Business Forum for Consumer Privacy, which reportedly includes members from Microsoft Corp., Google Inc., eBay Inc., and Hewlett-Packard Co., published a whitepaper in March, calling for use- and category-based approaches to companies’ data practices (14 ECLR 383, 3/18/09).

“Data is the currency of the digital economy,” the group said. Information about consumers’ activities can assist businesses in advertising, product planning, fraud detection, customer service, enhancing the consumer experience, and maximizing sales, the group said.

They recommended that the focus should shift to data use, rather than data collection. Companies’ uses of data should define their obligations to protect it. “Rather than require individuals to police the use of their information, the use-and-obligation approach places obligations for responsible data use squarely on the organization.”

Martin Abrams, senior policy advisor and executive director of Hunton & Williams’ Centre for Information Policy Leadership, said that the Business Forum for Consumer Privacy will offer for the FTC’s consideration a new framework for approaching privacy concerns, one that focuses on the nature of the collecting entity’s use of personal information. Every class of use has as-

sociated obligations. Every company that uses the data must respect the obligations associated with the uses.

There are several different versions of fair information practices that have been published to date, including by the OECD and APEC. Abrams told BNA. The FTC should encourage the use of fair information practices, Abrams said, but companies should be able to apply them in a manner that makes the most sense in the context of a given situation.

“Requiring companies to ‘comply’ with OECD principles as EPIC recommended is somewhat problematic, because they were created as guidance—not as regulations,” Abrams said. “The commission should require organizations to protect individuals from risks, not simply comply with procedural disclosure requirements. Data is collected and used differently depending on the intended purposes. There are obligations to individuals that come with all uses, including transparency, that must be respected by the commercial users.”

As a baseline, Abrams said that companies that collect consumer data online should disclose that fact. “We agree that there should be no secret collection of data,” Abrams said. “But more notice isn’t always going to be a good thing because, in some cases, every pixel on a page might be controlled by a different entity, and if consumers were presented with notifications for each one they would be overwhelmed.”

Companies are working to create a workable just-in-time notice strategy for data transfers that consumers do not expect, Abrams said. “There are certain flows that consumers would find as an incredible surprise, and there should be some kind of just-in-time notice there. But, we—as an overall community—have not figured out how to make just-in-time work.”

**Policies Versus Practices.** Paul M. Schwartz, professor of law and director of Berkeley Center for Law & Technology, told BNA that although the FTC might expand its focus beyond notice considerations, it should not completely abandon its attention on privacy policies.

“In general, terms of use and privacy policies are always a good thing. Privacy notices make companies think about what their privacy practices are,” Schwartz said. “Policies also give privacy advocates an opportunity to examine business practices related to consumer information.”

One thing companies need to work on, Schwartz said, is keeping the lines of communication open between the lawyers who write the policies, and the tech-side employees who are involved in data-collection and use. “There can be a disjunction between the lawyers and the individuals who are responsible for what actually happens on the technical side. Policies need to reflect actual practices,” Schwartz said.

When it comes to data-sharing between online services, transparency gains additional importance, he added. “The big issue with the sharing with the third party sites is that transparency gets to be a big issue, because it’s hard to know as a consumer where the information is going.”

**New Hybrid Privacy Model Emerging.** D. Reed Freedman, a former FTC staff attorney and current partner with Morrison & Foerster LLP in Washington, D.C., said it seems almost inevitable that the commission will move towards a framework that encompasses both notice-based and harm-based approaches taken in years past. Discussion will likely center on which prac-

tices pose the greatest risks, and disclosure requirements will likely be posited accordingly.

“The commission will consider how consumers understand online business practices, and where practices are clear and risks are minimal fewer safeguards will be required,” Freeman said.

“But where consumers may be harmed, more protections may be needed and heightened notice or choice might apply. It might even ban truly egregious activities. The big debate will be over what practices will go into each bucket.”

BY AMY E. BIVINS

---

*More information about the Federal Trade Commission's Dec. 7, 2009, privacy roundtable event is available at the FTC website, <http://www.ftc.gov/bcp/workshops/privacyroundtables/index.shtml>*

*Full text of the Oct. 27 EPIC letter to the FTC available at <http://pub.bna.com/eclr/epicftcrequest.pdf>*

*Full text of the OECD's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data available at [http://www.oecd.org/document/18/0,3343,en\\_2649\\_34255\\_1815186\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html)*

*Full text of H.R. 3126 available at <http://pub.bna.com/eclr/hr3126.pdf>*

*Full text of letter to House Energy and Commerce about H.R. 3126 available at <http://pub.bna.com/eclr/ftcletter.doc>*

*The Business Forum for Consumer Privacy's "A New Approach to Protecting Privacy in the Evolving Digital Economy A Concept for Discussion" whitepaper available at the International Association of Privacy Professionals' Web site, <https://www.privacyassociation.org/images/stories/pdfs/a%20new%20approach%20to%20protecting%20privacy%20-%20final.pdf>*