

THE COMMITTEE ON ENERGY AND COMMERCE
INTERNAL MEMORANDUM



TO: Subcommittee Members

FROM: Energy and Commerce Committee Staff

RE: Majority Memorandum for October 13, 2011, Subcommittee Hearing

I. Summary

On Thursday, October 13, 2011, the Commerce, Manufacturing, and Trade Subcommittee will hold a hearing entitled “Understanding Consumer Attitudes about Privacy” at 9:00 a.m. in room 2123 of the Rayburn House Office Building. Witnesses are by invitation only.

The purpose of this hearing is to examine consumers’ attitudes toward privacy as reflected by their utilization and manipulation of existing privacy controls.

II. Witnesses

Barbara Lawler
Chief Privacy Officer
Intuit

Scott Meyer
Chief Executive Officer
Evidon

Michael Hintze
Associate General Counsel
Microsoft

Linda Woolley
Executive Vice President
Direct Marketing Association
on behalf of the Digital Advertising Alliance

Alessandro Acquisti
Associate Professor of Information Systems and Public Policy
Carnegie Mellon University

Pam Dixon
Executive Director
World Privacy Forum

III. Background

Privacy laws

There is no single Federal law expressly governing all data collection in the United States, nor a single regulator to enforce existing privacy-related laws. Rather, an industry-specific approach has emerged whereby Congress has restricted consumer data collection and use by subject matter and provided the enforcement authority to the relevant Federal regulator. For example, the collection and use of medical information is handled primarily by the Secretary of Health and Human Services under the Health Insurance Portability and Accountability Act (HIPAA) and the collection and use of financial data is protected by the Gramm-Leach-Bliley Act and enforced by the financial regulators. Additionally, the Federal Trade Commission (FTC or Commission) enforces the Fair Credit Reporting Act, which regulates the collection and use of consumer information by credit reporting agencies and their practices related to consumer information.

The FTC arguably has the broadest jurisdiction of any Federal regulator to enforce general privacy violations under its section 5 authority defining unfair or deceptive acts or practices. The Commission has brought 34 cases under its section 5 authority since 2001 against companies that failed to protect consumer information, including when companies fail to adhere to their own stated privacy policy.

Consumer Attitudes and Expectations

Both policymakers and stakeholders have expressed increasing concern regarding the collection and availability of consumers' personal information online in recent years. Increased data collection and storage by such entities as websites, information brokers, direct marketers, ISPs, and advertisers have been driven in large part by the rapid decline of the associated costs of data processing and storage, while at the same time the value of consumer information has increased. For instance, data about consumers' online behavior can be used to target ads toward consumers whose preferences are aligned with a particular product or service, thereby increasing the likelihood of "conversion," or sale of the product. However, advocates have raised concerns regarding a lack of transparency and, in some cases, a lack of choice for the consumer to opt out of having their data collected and/or shared with unknown parties.

In 2010, the FTC staff and the Department of Commerce National Telecommunications and Information Administration (NTIA) separately issued reports on privacy and proposed regulatory frameworks.¹

¹ Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (2010) (available at <http://www.ftc.gov/os/2010/12/101201privacyreport.pdf>); Internet Policy Task Force, Department of Commerce, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework* (2010) (available at http://www.ntia.doc.gov/files/ntia/publications/iptf_privacy_greenpaper_12162010.pdf).

In the course of roundtable forums conducted to inform the staff report, the FTC received comments indicating a wide range of consumer attitudes and behavior regarding privacy. While the FTC received survey data indicating consumers care about privacy, there was little or no data about the level of discomfort or the percentage of consumers willing to forgo benefits to avoid tracking.² The FTC stressed that a lack of transparency and a lack of consumer understanding about data collection practices could be a problem affecting consumer attitudes and their ability to make informed choices.³ Similarly, the NTIA's report noted the lack of transparency as a problem weighing on consumer understanding and consumer trust.⁴

Industry Responses and Marketplace Developments

In response to growing concerns over online data collection and use, particularly regarding behavioral advertising, the online advertising community developed a self-regulatory model to provide consumers with notice and choice about advertisements delivered to them through behavioral targeting. The Digital Advertising Alliance, whose members include the Interactive Advertising Bureau, the Network Advertising Initiative, Direct Marketing Association, Association of National Advertisers, and the American Advertising Federation, developed and implemented the "About Ads" self-regulatory principles for online behavioral advertising program to provide consumers more information on why they are seeing a particular ad and to provide consumers a mechanism to opt out of future ads served to them based on behavioral advertising.

In its staff report, the FTC proposed a number of principles to enhance consumer choices regarding privacy. The Commission staff supported the concept of a mechanism whereby consumers could register their preference not to have their information collected, commonly referred to as a "Do-Not-Track" mechanism.

Since a Subcommittee hearing in the last Congress on "Do-Not-Track" legislation, the two most popular browser developers – Microsoft (Internet Explorer) and Mozilla (Firefox) - have designed a "Do-Not-Track" feature incorporated into their browsers.⁵ These features are user-controlled so consumers choose to turn on the feature to prevent tracking.⁶ Internet Explorer's tool blocks content from sites that are on tracking protection lists and that could otherwise use the content to collect information, while Mozilla's Firefox's "Do-Not-Track" feature broadcasts a signal to each website a consumer visits communicating the consumer's desire not to have his or her information collected. However, the effectiveness of this tool faces significant hurdles because every website that receives the signal from the consumer's browser

² "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework For Businesses and Policymakers" FTC Staff Report, (December 2010), p.29.

³ Id., p.25

⁴ "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework", The Department of Commerce Internet Policy Task Force, p.33.

⁵ Wingfield, Nick and Angwin, Julia "Microsoft Adds Do-Not-Track Tool to Browser" Wall Street Journal, available at <http://online.wsj.com/article/SB10001424052748703363904576200981919667762.html> (viewed October 4, 2011).

⁶ See <http://windows.microsoft.com/en-US/windows7/How-to-use-Tracking-Protection-and-ActiveX-Filtering> and <http://support.mozilla.com/en-US/kb/how-do-i-stop-websites-tracking-me>.

must choose to honor the request; there is no requirement that websites must honor the request. Additionally there is no current standard for the signal that is broadcast from the user's browser. Therefore, compliance by website operators has reportedly been extremely low.

In addition to the built-in features of the browsers, both offer consumers the ability to download "add-on" extension tools. In the case of Mozilla, many free add-ons have been developed to provide users greater control over their privacy and security (see <https://addons.mozilla.org/en-US/firefox/extensions/privacy-security/>).

* * *

Please do not hesitate to contact Gib Mullan, Shannon Weinberg, or Brian McCullough at (202) 225-2927 if you have any questions with respect to this hearing.