



THE COMMITTEE ON ENERGY AND COMMERCE

INTERNAL MEMORANDUM

July 12, 2011

To: Members of the Subcommittee on Commerce, Manufacturing, and Trade
Members of the Subcommittee on Communications and Technology

From: Majority Staff

Re: Hearing on "Internet Privacy: The Views of the FTC, the FCC, and NTIA"

On Thursday, July 14, 2011, the Subcommittee on Commerce, Manufacturing, and Trade and the Subcommittee on Communications and Technology will hold a joint hearing entitled "Internet Privacy: The Views of the FTC, the FCC, and NTIA." The hearing will take place at 11:00 a.m. in 2123 Rayburn House Office Building. At the hearing, the Subcommittees will examine the views of several federal agencies regarding the regulation of Internet privacy. The following provides background on the hearing witnesses, as well as some general information on online privacy.

I. WITNESSES

The Honorable Edith Ramirez
Commissioner
Federal Trade Commission (FTC)

The Honorable Julius Genachowski
Chairman
Federal Communications Commission (FCC)

The Honorable Lawrence E. Strickling
Assistant Secretary for Communications and Information
National Telecommunications and Information Administration (NTIA)

II. INTERNET PRIVACY BACKGROUND

The Internet is a tool of incalculable value, both tangible and intangible. It has spurred many transformative innovations that affect the manner in which consumers act, including how they communicate, engage in commerce, obtain information, and entertain themselves. Companies collect vast amounts of information about consumers through these various Internet channels. Companies analyze, use, and disseminate the data in a wide range of commercial practices. Some, though not all, of this information is aggregated and anonymized. While it is well documented that the reasonable collection and use of consumer information offers benefits to businesses and consumers, concerns about individual privacy remain.

Once information takes a digital form, it can be copied, transferred, or accessed almost anywhere in the world where the Internet is available. Information is the currency of the Internet and a consumers' use of the information is the "cost" they pay under most business models for the free services and content they use (e.g., "pop-up" adds on a website). While applications providers continue to increase the variety of tools available to consumers to control their privacy settings, a lingering problem for most consumers is the lack of transparency and a basic understanding about how companies use this information. While surveys indicate that consumers harbor concerns about privacy, it is unproven whether more stringent laws and regulations on the collection and use of data will ameliorate these concerns in a manner that encourages innovation and electronic commerce.

As Congress takes a closer look at online privacy issues, industry has embarked on a self-regulatory campaign relating to the collection and use of consumer information. Industry-wide efforts include: (1) increased consumer education and site transparency to increase consumer comfort with how industry uses information, and (2) development of new preference profiles so consumers can personalize their browsing experience and control how much information to share.

Federal Trade Commission (FTC)

The Federal Trade Commission is the primary Federal regulatory body in the privacy realm, operating with a dual mission: competition and consumer protection. Through the Bureau of Consumer Protection (BCP), the FTC enforces a number of rules and regulations dealing with privacy: the Fair Credit Reporting Act (FCRA), the Fair and Accountable Transactions Act (FACTA), the implementing rules of the Gramm-Leach-Bliley Act (GLB) (regarding privacy policy requirements), the Safeguards Rule (requiring financial institutions to secure customers' sensitive information), and the very popular Do-Not Call-Registry (allowing consumers to block their telephone numbers from telemarketers). Where there are no specific rules, the Commission enforces other privacy-related violations under its Section 5 unfair or deceptive acts or practices authority (UDAP), such as a failure to abide by one's stated privacy or data security policy.¹

The Commission has taken a proactive role on privacy in the last decade, holding roundtable forum discussions, educational workshops, and issuing reports. Most recently, the Commission issued a preliminary staff report in December 2010 titled "Protecting Consumer Privacy in an Era of Rapid Change."² The Commission has collected extensive public comments on that report and plans to issue a final report by the end of 2011. Prior to the 2010 report, the Commission issued a staff report entitled "Self Regulatory Principles for Online Behavioral Advertising" in February 2009.³

¹ For a listing of the Commission's privacy-related enforcement actions, see <http://business.ftc.gov/legal-resources/8/35>.

² Available at <http://ftc.gov/os/2010/12/101201privacyreport.pdf>.

³ Available at <http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf>.

The Federal Communications Commission (FCC) and The Communications Act

Telecommunications Services. Historically, the Federal Communications Commission has been the locus of electronic communications privacy regulation. The FCC's customer proprietary network information (CPNI) rules, which date back to the 1980s, regulate the way telephone companies may use and share subscriber information, such as what telecommunications services their customers have, whom they call and when, and for how long. Congress codified and expanded these rules in 1996 by adding Section 222 to the Communications Act. Congress defined CPNI as both the technical information a telephone company has about its customers as well as the information customers would typically see on their bill. Congress restricted the ability of telephone companies to use and share such information except when aggregated to prevent identifying data about individual subscribers.

To implement Section 222, the FCC revised its rules in the late 1990s, requiring carriers to obtain opt-in consent before using individually identifiable information for certain marketing purposes. The FCC reverted to an opt-out regime, however, after the U.S. Court of Appeals for the Tenth Circuit ruled that the Communications Act did not explicitly require opt-in and that an opt-out regime was a less restrictive interpretation that was more consistent with carriers' commercial free speech rights.

The FCC extended its CPNI rules in 2007 to providers of interconnected VoIP service, established safeguards for the unauthorized disclosure of individually identifiable information, and established oversight procedures to ensure industry compliance. The updated rules allow telephone companies and their affiliates to use individually identifiable private information for marketing purposes subject to opt-out, impose safeguards before such information may be shared with joint venture partners, and require opt-in approval before most other disclosures of an individual's private information. The D.C. Circuit upheld this new regime as consistent with the First Amendment given the increasing activity of data brokers using private information for marketing purposes. In 2009, the Commission announced enforcement actions against over 600 telephone companies that failed to comply with federal privacy protections.

Cable Services. Section 631 of the Communications Act governs cable privacy. Except to provide service or render a bill, cable operators may not use or share personally identifiable information collected over the cable system absent prior consent from the subscriber. It also requires operators to notify subscribers about the operators' data collection practices. Subscribers may bring suit in federal court for violations of Section 631.

Do-Not-Call and Phone and Fax Solicitations. The Telephone Consumer Protection Act of 1991 required the Commission to draft rules to protect residential telephone subscribers from unwanted telephone solicitations generally, including from the use of robo-dialing and other automated calls. The Do Not Call Implementation Act of 2003 required the Federal Communications Commission to complete its consideration of adopting a do-not-call registry and related telemarketing rules, authorized the Federal Trade Commission to collect fees to establish a national do-not-call registry, and required both the FCC and FTC to coordinate on reports to Congress on the effectiveness of these rules. The Junk Fax Prevention Act of 2005 supplemented the FCC's existing junk-fax regulations, allowing consumers to opt out of unwanted faxes and requiring annual reports on the Commission's enforcement efforts.

Mobile and Location-Based Services. Section 222(f) of the Communications Act prohibits wireline and wireless providers from using or disclosing customer location information absent opt-in consent. In the National Broadband Plan, the Commission identified the need for increased consumer awareness and potential privacy protections as consumers expand their use of mobile, location-based services. And just last month, in June 2011, the FCC and the FTC hosted a forum to help consumers understand how consumer information is collected and used for location-based services.

Online Privacy. Some of the recent round of debate regarding electronic communications privacy can be traced back to a July 2008 hearing in what was then called the Subcommittee on Telecommunications and the Internet on plans by NebuAd to provide targeted Internet advertising based on consumers' browsing habits. Since then, the FCC's National Broadband Plan concluded that the lack of online privacy protections is deterring consumers from adopting broadband. The FCC has also recently claimed in its "network neutrality" decision and other rulings that it has authority under Section 706 of the 1996 Telecommunications Act to regulate Internet-related services to promote broadband. If upheld, this claim could allow the FCC to adopt rules regarding Internet privacy. The FCC also commenced in 2010 a "Wi-Spy" investigation into whether Google violated the law when it collected consumer data over Wi-Fi transmissions without first getting permission.

The National Telecommunications and Information Administration (NTIA)

In 2010, the NTIA's Internet Policy Task Force launched a notice of inquiry regarding information privacy and innovation in the Internet economy and held an all-day forum on the interaction between privacy and innovation. In its subsequent report, the Task Force recommended building a general privacy framework based on an expanded set of Fair Information Practice Principles, the publication of privacy impact assessments by industry, the use of voluntary codes of conduct to address emerging technologies, and the establishment of a Privacy Policy Office within the Department of Commerce.

III. STAFF CONTACTS

Please contact Jim Barnette or Jeff Mortier at 5-2927 if you have any questions regarding the hearing.