

ONE HUNDRED ELEVENTH CONGRESS
Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115

Majority (202) 225-2927
Minority (202) 225-3641

MEMORANDUM

July 19, 2010

To: Members of the Subcommittee on Commerce, Trade, and Consumer Protection

Fr: Subcommittee on Commerce, Trade, and Consumer Protection Democratic Staff

Re: Legislative Hearing on H.R. ____, the BEST PRACTICES Act, and H.R. ____, a discussion draft to require notice to and consent of an individual prior to the collection and disclosure of certain personal information relating to that individual

On Thursday, July 22, 2010, at 2:00 pm in room 2123 of the Rayburn House Office Building, the Subcommittee on Commerce, Trade, and Consumer Protection will hold a legislative hearing on H.R. ____, the BEST PRACTICES Act, and H.R. ____, a discussion draft to require notice to and consent of an individual prior to the collection and disclosure of certain personal information relating to that individual.

I. Background

In today's global economy, information is critical and indispensable. Companies collect vast amounts of information about consumers through countless different methods, mechanisms, and media channels. Data is collected, aggregated, analyzed, used, and disseminated for a wide range of commercial practices. Over the past 15 months, the Subcommittee on Commerce, Trade, and Consumer Protection and the Subcommittee on Communications, Technology, and the Internet have held five hearings to examine the effects of these practices on consumer privacy. The hearings explored issues such as deep packet inspection, online behavioral advertising, merging consumer information collected offline with data collected online, location information, information brokers, and data security.¹ At the hearings, 34 witnesses testified

¹ Subcommittee on Communications, Technology, and the Internet, *Hearings on Communications Networks and Consumer Privacy: Recent Developments*, 111th Cong. (Apr. 23, 2009); Subcommittee on Commerce, Trade, and Consumer Protection, *Hearings on H.R. 2221, the Data Accountability and Protection Act, and H.R. 1319, the Informed P2P User Act*, 111th Cong. (May 5, 2009); Subcommittee on Communications, Technology, and the Internet and Subcommittee on Commerce, Trade, and Consumer Protection, *Hearings on Behavioral*

about the potential benefits and harms of rapidly-evolving business models that increasingly rely on the collection and use of consumer data.

There is no dispute that the reasonable collection and use of consumer information offer benefits to businesses, consumers, the marketplace, and society generally. Companies must collect information to process transactions and conduct day-to-day operations. Moreover, authentication, fraud prevention, and background checks are all activities that rely on consumer information. In addition, marketing databases help companies identify new sales leads, improve customer service, develop new lines of products, and make marketing more efficient.

However, numerous consumer groups, privacy advocates, academics, companies, and others have raised privacy concerns about the collection and use of consumer data. Most recently, 17 consumer groups outlined their concerns and renewed their call for a comprehensive consumer privacy law in a letter to the Federal Trade Commission (FTC) on July 14, 2010.² Privacy concerns range from being subjected to unwanted marketing to being denied goods or services based on a profile. In addition, the sale of targeted customer lists that characterize consumers as risk takers or gullible may expose consumers to increased risks of fraud.³ The use or misuse of sensitive information such as health information also could embarrass consumers, impact their employment, or lead to other problems. Other concerns have also been raised that consumers will unknowingly be “boxed” into categories based on past behavior and that their choices, and the information presented to them, will be limited as a result.⁴

Transparency is another issue raised by many stakeholders. Data collection practices are complex, varying from entity to entity. Even when choices are offered to consumers, they may be difficult to use, require the payment of fees, or only partially address the collection or use of information.

Over the past several months, a series of high-profile incidents involving consumer data has increased these privacy concerns. These incidents included Google’s launch of its social

Advertising: Industry Practices and Consumers’ Expectations, 111th Cong. (June 18, 2009); Subcommittee on Communications, Technology, and the Internet and Subcommittee on Commerce, Trade, and Consumer Protection, *Hearings on Exploring the Offline and Online Collection and Use of Consumer Information*, 111th Cong. (Nov. 19, 2009); Subcommittee on Communications, Technology, and the Internet and Subcommittee on Commerce, Trade, and Consumer Protection, *Hearings on the Collection and Use of Location Information for Commercial Purposes*, 111th Cong. (Feb. 24, 2010).

² Letter from ACLU et al. to Jon Leibowitz, Chairman, Federal Trade Commission (July 14, 2010) (online at www.democraticmedia.org/files/CoalitionFTCletter71410_3.pdf)

³ See, e.g., Comments of the World Privacy Forum, Federal Trade Commission Privacy Roundtables, Project No. P095416 (Nov. 6, 2009) (online at www.worldprivacyforum.org/pdf/WPF_Comments_FTC_110609fs.pdf)

⁴ Martin Abrams, *Boxing and Concepts of Harm*, Privacy and Data Security Law Journal (Sept. 2009) (online at www.hunton.com/files/tbl_s47Details/FileUpload265/2692/Boxing_and_Concepts_of_Harm_Abrams_9.09.pdf)

network service Google Buzz;⁵ changes to Facebook users' privacy settings;⁶ the collection of payload data from open WiFi networks by Google's Street View cars;⁷ and Sears' collection of highly-sensitive personal information via a downloadable software application.⁸ Moreover, data breaches of sensitive information continue at an alarming pace. According to the Privacy Rights Clearinghouse, 494 million records containing sensitive personal information have been involved in security breaches since January 2005.⁹

II. Current Law

Many of the information collection practices discussed above are not subject to any federal laws or regulation. Specific federal laws address certain categories of personal information or specific entities. For example, the Fair Credit Reporting Act (FCRA) governs consumer report information,¹⁰ Title V of the Gramm-Leach-Bliley Act addresses the sharing of certain nonpublic personally identifiable information by financial institutions,¹¹ and rules promulgated pursuant to the Health Insurance Portability and Accountability Act apply to the privacy of medical records.¹² In addition, FTC may bring actions for unfair or deceptive acts or practices under the FTC Act, which includes the authority to bring actions related to a company's information collection and use.¹³ There are no federal laws, however, that comprehensively govern the collection, use, and dissemination of consumer information across the board.¹⁴

III. H.R. ____, the BEST PRACTICES Act

⁵ Letter from the Electronic Privacy Information Center to Federal Trade Commission (Mar. 2, 2010) (online at epic.org/privacy/ftc/googlebuzz/Google_Buzz_Supp_Complaint.pdf).

⁶ Letter from the Electronic Privacy Information Center to Federal Trade Commission (May 5, 2010) (online at epic.org/privacy/facebook/EPIC_FTC_FB_Complaint.pdf).

⁷ The Official Google Blog, *WiFi data collection*, (online at googleblog.blogspot.com/2010/05/wifi-data-collection-update.html) (accessed July 14, 2010).

⁸ Federal Trade Commission, *Sears Settles FTC Charges Regarding Tracking Software* (June 4, 2009) (online at www.ftc.gov/opa/2009/06/sears.shtm).

⁹ Privacy Rights Clearinghouse, *A Chronology of Data Breaches* (online at www.privacyrights.org/data-breach#1) (accessed July 14, 2010).

¹⁰ 15 U.S.C. §1681 *et seq.*

¹¹ 15 U.S.C. §§ 6801-6809.

¹² 45 C.F.R. Part 164.

¹³ 15 U.S.C. § 45(a)(2).

¹⁴ *See generally* Congressional Research Service, *Information Brokers: Federal and State Laws* (May 5, 2006) (RL-33005); Congressional Research Service, *Privacy Law and Online Advertising: Legal Analysis of Data Gathering By Online Advertisers Such as Double Click and NebuAd* (Feb. 20, 2009) (RL-34693).

On July 19, 2010, Rep. Bobby L. Rush introduced H.R. ___, the BEST PRACTICES Act. The purpose of this bill is to foster transparency about the commercial use of personal information and provide consumers with meaningful choice about the collection, use, and disclosure of such information.

The bill requires a covered entity to make available to individuals information about the covered entity's privacy practices, including a description of the information collected and the specific purposes for such collection. The FTC is directed to determine the means and timing of notices, may allow for or require shorter notices, and may issue model notices. A covered entity must provide an individual with the ability to opt out of the collection and use of covered information and must obtain express affirmative consent before collecting, using, or disclosing sensitive information. A covered entity that participates in a Safe Harbor Self-Regulatory Choice Program approved by FTC is not subject to certain requirements.

The bill also includes data security, access, data minimization, accountability, and accuracy requirements. The bill grants enforcement authority to FTC and the states, including civil penalty authority, and grants FTC streamlined rulemaking authority to implement the bill. Finally, the bill authorizes a limited private right of action and contains a preemption provision of certain state laws that expressly require covered entities to implement requirements with respect to the collection, use, or disclosure of covered information. The preemption provision does not apply to State laws that address health information or financial information, data breach laws, trespass, contract, or tort laws, and other laws that relate to acts of fraud. A section-by-section analysis of the bill is attached as Appendix A.

IV. H.R. ___, a discussion draft to require notice to and consent of an individual prior to the collection and disclosure of certain personal information relating to that individual

On May 4, 2010, Reps. Boucher and Stearns released to the public a discussion draft to require notice to and consent of an individual prior to the collection and disclosure of certain personal information relating to that individual. More specifically, under this bill, a covered entity must provide individuals with a notice prior to collection of information that includes disclosures about the covered entity's privacy practices. A covered entity must provide an individual with the ability to opt out of the collection and use of covered information and must obtain express affirmative consent before collecting or disclosing sensitive information. The bill includes several exemptions from the consent requirements, including an exemption for covered entities or advertising networks engaged in online behavioral advertising. To qualify for the exemption, a covered entity must have a readily accessible opt-out mechanism, retain data for less than 18 months, and provides consumers with the ability to review or modify their profile, among other obligations.

The bill also includes data security and accuracy requirements. The provisions of the bill are enforced by FTC and the states and FTC is provided with streamlined rulemaking authority to implement the bill. Finally, the bill prohibits any private right of action and preempts any state law that includes requirements for the collection, use, or disclosure of covered information. A section-by-section analysis of the bill is attached as Appendix B.

V. WITNESSES

The following witnesses have been invited to testify:

David Vladeck

Director
Bureau of Consumer Protection
Federal Trade Commission

Ed Mierzwinski

Consumer Program Director
U.S. Public Interest Research Group

Leslie Harris

President and Chief Executive Officer
Center for Democracy and Technology

David Hoffman

Global Privacy Officer
Intel Corporation

Ira Rubinstein

Adjunct Professor of Law
New York University School of Law

Appendix A

Section-by-Section: The BEST PRACTICES Act

Section 1 of the bill states the title and includes the table of contents.

Section 2 sets forth definitions under the bill. Section 2(3) defines a “covered entity” as a person engaged in interstate commerce that collects or stores data containing covered information or sensitive information and excludes the government and certain small businesses. Section 2(4) defines “covered information” as certain information about an individual, such as a name, postal address, passport number, or financial account number. The definition excludes certain business and employment information. Section 2(8) defines “sensitive information” as certain information about an individual, such as medical history or financial information, race or ethnicity, biometric information, and Social Security numbers. FTC may modify the definition. Section 2(10) defines a “third party” based on the reasonable expectation of the consumer and requires FTC to clarify or modify the definition.

Section 101 requires a covered entity to make information about the covered entity’s privacy practices available to individuals, including a description of the information collected and the specific purposes for which the information was collected.

Section 102 requires a covered entity to provide individuals with concise, meaningful, timely, prominent, and easy-to-understand notice or notices. Section 102 directs FTC to promulgate rules to determine the means and timing of notices while taking into account the different media, devices, or methods through which a covered entity collects information. FTC can allow for or require shorter notices and may issue model notices.

Section 103 requires a covered entity to provide an individual with the ability to opt out of the collection and use of covered information. A covered entity may require, as a condition of receipt of a service or benefit, the collection and use of covered information about the individual, subject to a series of limitations. Opt-out consent is not required for the collection and use of covered information for certain operational purposes.

Section 104 requires a covered entity to obtain express affirmative consent before: disclosing covered information to third parties; collecting, using, or disclosing sensitive information; or engaging in comprehensive online data collection through hardware or software such as deep packet inspection.

Section 105 requires a covered entity to obtain express affirmative consent for the retroactive application of a privacy policy to previously collected information and to offer notice for prospective changes and opt-out consent for certain prospective changes.

Section 106 establishes that a covered entity is exempt from complying with sections 103 and 104 for the disclosure of covered information to service providers or for the collection or disclosure of publicly available information.

Section 201 requires a covered entity to establish procedures to ensure the accuracy of covered information and sensitive information, with exceptions for fraud databases and publicly available information.

Section 202 requires a covered entity to provide consumers with reasonable access to, and the ability to correct or amend, certain information held about that individual.

Section 301 requires a covered entity to have safeguards to secure information.

Section 302 requires a covered entity to conduct a privacy risk assessment for certain commercial projects and conduct periodic assessments of its information practices.

Section 303 mandates that a covered entity shall only retain covered information or sensitive information as long as necessary to fulfill a legitimate business purpose or comply with a legal requirement.

Sections 401-404 set out the requirements of a Safe Harbor Self-Regulatory Choice Program (Choice Program), establish that a covered entity that participates in Choice Program is not subject to certain sections, and require FTC to approve or decline to approve a Choice Program.

Section 501 authorizes a covered entity to collect or disclose aggregate information or de-identified information. A covered entity must take steps to protect that information. It is unlawful to re-identify or reconstruct such information, subject to FTC regulations.

Section 502 mandates that the Act shall have no effect on activities covered by other federal privacy laws.

Sections 601-605 grant enforcement authority to FTC and establish that a violation of titles I, II, or III of the bill is as an “unfair or deceptive act or practice” as established by regulation promulgated by FTC under Section 18 of the FTC Act. These sections grant enforcement authority to state attorneys general, subject to notification to and optional intervention by FTC, establish civil penalties for such violations, and authorize a limited private right of action.

Section 605 is a preemption provision of State laws that expressly require a covered entity to implement requirements with respect to the collection, use, or disclosure of covered information. The preemption provision does not apply to: laws that address health information or financial information; data breach laws; trespass, contract, or tort laws; and other laws that relate to acts of fraud.

Section 701 requires FTC to review the implementation of the Act and submit a report to Congress within 5 years of the Act’s enactment on its findings.

Section 702 requires FTC to conduct a consumer and business education campaign.

Section 703 establishes the effective date as 2 years after enactment.

Appendix B

Section-by-Section: a discussion draft to require notice to and consent of an individual prior to the collection and disclosure of certain personal information relating to that individual

Section 1 of the bill states the title.

Section 2 sets forth definitions under the bill. Section 2(4) defines a “covered entity” as a person engaged in interstate commerce that collects data containing covered information and excludes the government and certain small businesses. Section 2(5) defines “covered information” as certain information about an individual, such as a name, postal address, or passport number, as well as biometric information and a Social Security number. Section 2(10) defines “sensitive information” as certain information about an individual, such as medical or financial records. Section 2(13) defines an “unaffiliated party” as an entity that is not related by common ownership to or affiliated with a covered entity.

Section 3 requires a covered entity to provide individuals with a notice prior to collection of information that includes disclosures about the covered entity’s privacy practices. It must be posted on a Web site if information is collected via the Internet or made available in writing if information is collected by any means that does not utilize the Internet. A covered entity must provide an individual with the ability to opt out of the collection and use of covered information, except for the collection and use for operational purposes and for certain disclosures to a service provider.

Section 3 also requires a covered entity to obtain express affirmative consent for: the disclosure of covered information to unaffiliated parties; application of retroactive changes of a privacy policy to previously collected information; the collection or disclosure of sensitive information; or the use of hardware or software such as deep packet inspection to engage in comprehensive online data collection.

Finally, pursuant to an exception for individual managed preference profiles, a covered entity may disclose covered information to unaffiliated third parties without express affirmative consent if the covered entity (1) has a readily accessible opt-out mechanism; (2) retains data for less than 18 months; and (3) provides consumers with the ability to review or modify a preference profile.

Section 4 requires a covered entity to establish procedures to ensure the accuracy of covered information and to have safeguards to secure information. In addition, FTC is required to conduct a consumer education campaign.

Section 5 allows a covered entity to collect or disclose aggregate information or information that has been rendered anonymous.

Section 6 sets forth that location-based information is “call location information” under the Communications Act and cannot be disclosed without express affirmative consent.

Section 7 requires the Federal Communications Commission to submit a report to Congress within a year of enactment detailing all provisions of U.S. law that address subscriber privacy and how those provisions may be harmonized with this Act.

Section 8 grants enforcement authority to FTC and establishes that a violation of the Act is as an “unfair or deceptive act or practice” as established by regulation promulgated by FTC under Section 18 of the FTC Act. Under the bill, State attorneys general have the authority to seek injunctions and obtain damages, restitution, or other compensation.

Section 9 prohibits any private right of action.

Section 10 establishes that the Act preempts any State law or regulation that includes requirements for the collection, use, or disclosure of covered information.

Section 11 mandates that the Act shall have no effect on activities covered by other federal privacy laws.

Section 12 establishes the effective date as 1 year after enactment.