



Jessica L. Rich
Office of the Director
Bureau of Consumer Protection

UNITED STATES OF AMERICA
Federal Trade Commission
WASHINGTON, D.C. 20580

October 29, 2014

By Email

Eric Lightner
Director, Federal Smart Grid Task Force, Office of Electricity Delivery
and Energy Reliability, U.S. Department of Energy
1000 Independence Avenue S.W.
Washington, DC 20585

Re: Comment: Voluntary Code of Conduct for Utilities and Third Parties Providing
Consumer Energy Use Services

Dear Mr. Lightner,

Federal Trade Commission staff has been following with interest your public multi-stakeholder process to consider, and ultimately develop, a voluntary code of conduct relating to privacy and security practices for data concerning consumer energy usage. As Director of the Federal Trade Commission's Bureau of Consumer Protection,¹ I welcome the opportunity to comment on the proposed Voluntary Code of Conduct (VCC) published in the Federal Register by the Office of Electricity Delivery and Energy Reliability, Department of Energy (DOE OE).²

¹ The views expressed in this letter are my own and do not necessarily reflect the views of the Federal Trade Commission or any particular Commissioner.

² Request for Public Comment, "Data Privacy and the Smart Grid: A Voluntary Code of Conduct," 79 Fed. Reg. 54695 (Sept. 12, 2014), available at www.gpo.gov/fdsys/pkg/FR-2014-09-12/html/2014-21838.htm.

Background on FTC's Role in Privacy and Data Security

The Federal Trade Commission (FTC) is an independent agency with a broad mission to protect consumers and promote competition in the commercial marketplace. The central purpose of our consumer protection mission is to protect consumers from deceptive and unfair practices – that is, false or misleading claims by companies or practices that subject consumers to unreasonable risk of injury.³ As part of this mission, the FTC has worked actively for decades to protect consumers' privacy and security through a multi-pronged approach that includes law enforcement, policy initiatives, and consumer and business education. For example, under the laws we enforce, the FTC has challenged as false dozens of companies' claims about what data they collect, whether they share it with third parties, what choices they offer to consumers, and the level of security they provide for consumers' personal data. These matters have involved businesses in a wide variety of industries, including companies that sell mobile and Internet-connected devices;⁴ companies that provide Internet-related services;⁵ social media companies;⁶ and mobile app developers.⁷

³ 15 U.S.C. § 45.

⁴ *HTC America, Inc.*, Docket No. C-4406 (F.T.C. June 25, 2013) (final decision and order), available at www.ftc.gov/sites/default/files/documents/cases/2013/07/130702htcdo.pdf; *TRENDnet, Inc.*, Docket No. C-4426 (F.T.C. Jan. 16, 2014) (final decision and order), available at www.ftc.gov/system/files/documents/cases/140207trendnetdo.pdf.

⁵ *Google, Inc.*, Docket No. C-4336 (F.T.C. Oct. 13, 2011) (final decision and order), available at www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzdo.pdf.

⁶ *Facebook, Inc.*, Docket No. C-4365 (F.T.C. Aug. 10, 2012) (final decision and order), available at www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf.

⁷ *Snapchat, Inc.*, Matter No. 132-3078 (F.T.C. May 14, 2014) (proposed consent agreement), available at www.ftc.gov/system/files/documents/cases/140508snapchatanalysis.pdf; *United States v. Path, Inc.*, No. C-13-0448 (N.D. Cal. Feb. 8, 2013) (Stipulated Final J.), available at www.ftc.gov/sites/default/files/documents/cases/2013/02/130201pathincdo.pdf.

The FTC has long supported self-regulation through codes of conduct such as the proposed VCC.⁸ For example, the Commission has issued a report recommending principles and a framework for addressing privacy across different industries,⁹ as well as reports proposing best practices for particular industries and contexts, such as data brokers, online behavioral advertising, facial recognition, and mobile privacy disclosures.¹⁰ The agency also has encouraged the development of strong and enforceable industry-specific codes of conduct for privacy through open, multi-stakeholder processes such as this one. For example, Commission staff participated in the National Telecommunications and Information Administration (“NTIA”)¹¹ process to develop a code of conduct for mobile devices, and is currently participating in the NTIA’s process to develop practices for facial recognition technologies.

Consumer Protection Issues Raised by Consumer Energy Data

As you well know, the energy industry is a complex one, involving numerous parties – utilities, electricity marketers, state and local regulators, companies that provide services to

⁸ The Commission staff has supported the development of industry codes of conduct in general, but with the caveat that they not be used to facilitate coordination that would reduce competition. *See, e.g.*, FTC Staff Advisory Opinion, From Bureau of Competition Staff to Council of Better Business Bureaus, Inc. (Aug. 15, 2011) (addressing whether staff was likely to recommend the agency challenge self-regulatory principles for online behavioral advertising as an anticompetitive restraint of trade) *available at* www.ftc.gov/sites/default/files/documents/advisory_opinions/council-better-business-bureaus-inc./100815cbbbletter.pdf.

⁹ FTC, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Mar. 2012) (“2012 Privacy Report”), *available at* www.ftc.gov/os/2012/03/120326privacyreport.pdf.

¹⁰ FTC, *Data Brokers: A Call for Transparency and Accountability* (May 2014), *available at* www.ftc.gov/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014; FTC Staff Report, *Self-Regulatory Principles For Online Behavioral Advertising: Tracking, Targeting, and Technology* (Feb. 2009), *available at* www.ftc.gov/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral; FTC Staff Report, *Facing Facts: Best Practices For Common Uses of Facial Recognition Technologies* (Oct. 2012), *available at* www.ftc.gov/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies; FTC Staff Report, *Mobile Privacy Disclosures: Building Trust Through Transparency* (Feb. 2013), *available at* www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf.

¹¹ *See* <http://www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-process-mobile-application-transparency>.

utilities, and third parties – that may seek access to consumer energy data, whether from utilities¹² or directly from consumers. For example, the “Green Button” initiative enables consumers to download their energy usage information and then use apps or other services to analyze their data, help them understand how their data usage compares to others’, or motivate them to reduce their energy use.¹³ With the introduction of smart meters, energy usage information is more granular than ever before.

There are many potential benefits to consumers from smart meters, chief among them giving consumers tools that increase energy efficiency and lower energy costs. At the same time, these developments raise new questions about what this energy data might reveal about consumers, and how it should be treated. For example, one employee of a company providing smart meter services noted that, with a live stream of smart meter data from a home, “we can infer how many people are in the house, what they do, whether they’re upstairs, downstairs, do you have a dog, when do you habitually get up, when did you get up this morning, when do you have a shower: masses of private data.”¹⁴ Very detailed energy usage data could lead to disclosure of information about “sleeping habits, vacation, health, affluence, or other lifestyle details.”¹⁵

¹² See, e.g., <http://www.opower.com> (providing energy usage data analysis and tools to utilities and their customers).

¹³ The Green Button is an initiative to facilitate sharing of energy data collected through smart meters, and a number of apps make use of the information. See “Welcome to the Green Button” at www.data.gov/energy/welcome-green-button; see also greenbuttondata.org. The Environmental Protection Agency’s Energy Star “Yardstick” tool allows consumers to input their energy usage data so that they can better understand how their energy usage compares with their neighbors’. See Brian Ng, EPA blog, “How Does Your Home Compare to Your Neighbor’s?” (May 12, 2012), available at blog.epa.gov/energystar/2014/05/how-does-your-home-compare-to-your-neighbors/. Electricity marketers and general retailers also offer various energy management devices and services.

¹⁴ NISTIR 7628, Guidelines for Smart Grid Cybersecurity: Vol. 2, Privacy and the Smart Grid, prepared by The Smart Grid Interoperability Panel – Smart Grid Cybersecurity Committee, at 25 n. 62 (Sept. 2014), available at dx.doi.org/10.6028/NIST.IR.7628r1 (citing a 2010 Reuters article quoting a representative from Siemens Energy).

¹⁵ See *id.* at 28-33.

In November 2013, FTC staff held a workshop to examine the privacy and security issues presented by the Internet of Things (“IoT”). The FTC invited speakers from consumer groups, industry, academia, and government – including DOE – to discuss the issues presented in different IoT settings, including smart energy technologies.¹⁶ The workshop addressed issues such as how to provide notice and choice for information practices for connected devices – like smart meters – that do not have a screen interface, and the importance of security, both from the standpoint of securing information transmitted by devices and about physical security and safety. Staff is currently developing a report recommending best practices for the IoT industry as a whole.

In addition, states and municipalities that regulate utilities have been following privacy issues associated with smart meters very closely. For example, California is among more than a half dozen states that have adopted regulations governing privacy and security of consumer energy data from smart meters and third party access to smart meter data.¹⁷ California Public Utility Commission regulations require companies, among other things, to specify the primary purpose for which covered information will be used; obtain consumers’ consent for use of the information for secondary purposes; limit data collection and retention to that reasonably necessary; and secure information and provide notice of breaches of unencrypted information.¹⁸

¹⁶ FTC Workshop, *The Internet of Things: Privacy and Security in a Connected World* (Nov. 19, 2013) (material available at www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-security-connected-world).

¹⁷ In 2005, Congress gave the Commission authority to make rules relating to consumer energy usage. *See* 42 U.S.C. § 16471. The Commission has not to date exercised this authority.

¹⁸ *See* Public Utilities Commission of the State of California, *Decision Adopting Rules to Protect the Privacy and Security of the Electricity Usage Data of the Customers of Pacific Gas and Electric Company, Southern California Edison Company, and San Diego Gas & Electric Company, Order Instituting Rulemaking to Consumer Smart Grid Technologies Pursuant to Federal Legislation and on the Commission’s own Motion to Actively Guide Policy in California’s Development of a Smart Grid System*, Rulemaking 08-12-009 (July 29, 2011), available at

The Voluntary Code of Conduct on Privacy and Smart Grid

The proposed VCC addresses many of these consumer protection issues in a thoughtful and forward-thinking manner. Among other things, DOE OE has been careful to establish a process that is open and transparent. DOE convened an initial workshop with a variety of stakeholders in January 2012 for moderated group discussions about Smart Grid privacy.¹⁹ After issuing a report summarizing the points raised in those discussions, it convened a series of public discussions run by stakeholders to discuss the possibility of a voluntary code of conduct and what that might entail. The drafts of the VCC and proceedings have been available online, and DOE OE solicited public comment on the most recent draft through a federal register notice. A variety of parties have participated, from state regulators and consumer advocates to utilities and third party product developers who make use – or plan to make use – of consumer energy data.

In addition, the code addresses many of the key privacy issues at stake in the smart grid and would apply to the entire breadth of entities that could access consumer energy data, including third parties. For example, the code covers important issues such as providing notice and getting consent for particular uses. The code distinguishes between primary and secondary uses and requires opt-in consent for such secondary uses. The code also requires that companies secure consumer data. Importantly, it requires that before a company can share consumer data with a third party for purposes other than that for which the information was originally collected, it must obtain a customer's specific and affirmative express consent. Overall, the code, if adopted, would provide meaningful protections for consumer data.

docs.cpuc.ca.gov/WORD_PDF/FINAL_DECISION/140369.pdf; *see generally* www.cpuc.ca.gov/PUC/energy/smartgrid.htm.

¹⁹ 2012 Privacy Report, *supra* note 9, at 48-50.

I have three suggestions that I believe would make the code even stronger. First, the code requires companies to provide a significant amount of information about data practices in a notice to consumers. This type of notice is, and should be, comprehensive so that consumers and others have a designated place that they can go to obtain accurate and complete information about a company's privacy practices. However, I recommend that you also include in the code a requirement that companies provide "just-in-time" disclosures to consumers at the time and place that they have the ability to exercise choices under the code. For example, when a consumer downloads a company's mobile app to check energy usage remotely, the company could alert the consumer – through push notifications or other clear and conspicuous disclosures on the phone – that the company sells consumer information to third parties for advertising. Such notices would call consumers' attention to the key information needed for those choices without forcing them to find and read the longer, more comprehensive notice at that very moment or, alternatively, skip reading the notice altogether.²⁰ Consumers that are interested in more detailed information will still be able to find it in the comprehensive notice.

Second, and relatedly, the code should require that all applicable consumer disclosures be made "clearly and conspicuously," so that consumers will see them and read them. The agency has produced guidance for businesses on providing clear and conspicuous notices.²¹

Third, the proposed code allows parties to adopt the code with deviations to accommodate conflicts in "laws, regulatory guidance, governing documents, and/or prevailing state/local business practices," as long as the party makes clear that it is not committing to that

²⁰ 2012 Privacy Report, *supra* note 9, at 48-50.

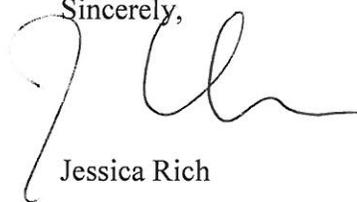
²¹ See FTC, *.com Disclosures: How to Make Effective Disclosures in Digital Advertising* (March 2013), available at www.ftc.gov/sites/default/files/attachments/press-releases/ftc-staff-revises-online-advertising-disclosure-guidelines/130312dotcomdisclosures.pdf.

aspect of the code. As I understand it, one purpose of this provision is to address the complex nature of commerce in this area and the variation among state and local regulations. For example, one locality might require a utility to make certain data public, while another might place restrictions on disclosure of the same data. However, by also allowing exceptions based on “prevailing state/local business practices,” the code may inadvertently signal that any particular business could choose not to adopt any portion of the code for any reason. This flexibility could undermine the value of a universal code, making it harder for consumers to understand and rely on the protections the code provides. I therefore recommend that you consider narrowing this provision, perhaps only to conflicts created by variations in existing laws and regulations.

Conclusion

I commend the DOE OE and stakeholders participating in the VCC process for developing this code. The FTC, as noted, supports industry self-regulation through strong and meaningful codes of conduct, provided they do not dampen the incentives of industry participants to compete. The data practices proposed in the code should give consumers important information and choices about how their data is handled. Thank you for this opportunity to respond to the request for comment.

Sincerely,

A handwritten signature in black ink, appearing to read 'Jessica Rich', written in a cursive style.

Jessica Rich

Director
Bureau of Consumer Protection