



United States of America
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

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

April 22, 2016

Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

**Re: Expanding Consumers' Video Navigation Choices, MB Docket No. 16-42
Commercial Availability of Navigation Devices, CS Docket No. 97-80
Comment of the Director of the Bureau of Consumer Protection of the
Federal Trade Commission**

Dear Secretary Dortch:

As the Director of the Federal Trade Commission's Bureau of Consumer Protection, I submit this comment to assist the Federal Communications Commission ("FCC") in evaluating the consumer privacy implications of its proposed set-top box rulemaking.¹ The FCC proposes to require cable and satellite television service providers to obligate third-party manufacturers to certify that their set-top boxes comply with certain privacy requirements applicable to cable and satellite providers pursuant to the Communications Act. In this comment, I recommend that, if the FCC adopts the proposed rule, cable and satellite companies should require these certifications to be conveyed to consumers, in order to facilitate FTC enforcement against third-party set-top box manufacturers under the jurisdiction of the FTC.² The FTC's ability to enforce promises made by these entities serves as an important backstop to ensure that they are abiding by the required consumer privacy protections.

I. Background

On March 16, 2016, the FCC proposed a rule intended to make it easier for companies other than cable and satellite television providers (known as multichannel video programming distributors, or "MVPDs") to sell set-top boxes that can be used with consumers' cable and satellite television services. The vast majority of consumers currently get their set-top boxes through their MVPDs, such as Comcast and DirecTV, and not through third parties that operate

¹ Expanding Consumers' Video Navigation Choices; Commercial Availability of Navigation Devices, 81 Fed Reg. 14033 (March 16, 2016). The FCC's Notice of Proposed Rule Making ("NPRM") was adopted and released on February 18, 2016 and published in the Federal Register on March 16, 2016. On March 17, 2016, the FCC extended by seven days the period in which parties could submit initial comments.

² I understand that the goal of the NPRM is to enhance competition among set-top box providers. The FTC has a dual mission to protect consumers and promote competition. This comment, however, is limited to the NPRM's consumer protection implications as they relate to consumer privacy and to the FTC's authority to enforce privacy promises.

set-top boxes using the FCC’s current interoperability standard. The proposed rule seeks to make it easier for current set-top box manufacturers like TiVo, as well as other manufacturers that may seek to offer set-top boxes, such as Amazon, Apple, Google, and Roku, to create compatible devices.

In its Notice of Proposed Rulemaking (“NPRM”), the FCC observes that the consumer protection statutes that govern MVPD-provided set-top boxes do not apply to set-top boxes provided by third parties.³ The NPRM proposes to address this discrepancy by requiring MVPDs to provide television subscription information to those third-party set-top box manufacturers that “certify” to MVPDs that their devices comply with the consumer protection requirements that apply to MVPD-provided set-top boxes.⁴ MVPDs would be required to provide television service information to any set-top boxes sold by third parties that certify compliance, and would be prohibited from providing information to any set-top boxes sold by third parties that fail to certify compliance.⁵ The NPRM seeks comment on this proposal, including whether such a program could be effective and how it should be structured.⁶

In this comment, I propose that if the FCC adopts the rule, MVPDs should require that third-party set-top box manufacturers represent *to consumers*, as well as to MVPDs, that their products comply with the cable and satellite statutory privacy provisions.⁷ Such a representation would be analogous to manufacturers voluntarily committing to a privacy code of conduct. The FTC has long advocated for the use of meaningful codes of conduct, and the FTC has well-established authority to enforce such codes of conduct under the FTC’s Section 5 authority to prohibit deceptive practices.⁸ Section II provides background on the FTC’s enforcement and advocacy regarding industry codes of conduct. Section III offers suggestions on how to structure an obligation to commit to a code of conduct in a manner that would permit enforcement under the FTC Act.

II. The Federal Trade Commission’s Privacy Program

The FTC is an independent agency charged by Congress with promoting consumer protection and competition in the marketplace. As the primary federal agency protecting consumers from unfair and deceptive privacy and data security practices, the FTC engages in extensive enforcement, policy, and consumer and business education initiatives. Privacy has

³ Set-Top Box NPRM at 14045-6 (citing 47 U.S.C. §§ 338(i) (satellite privacy), 551 (cable privacy), 303a (children’s programing); 47 C.F.R. § 25.701(e) (children’s programming); 47 C.F.R. Pt. 11 (emergency alerts)). Although the focus of this comment is consumer privacy, its suggestions apply equally to enforcement of promises regarding emergency alerts and children’s programming.

⁴ *Id.* at 14045, 14051 (proposing Section 76.1200(l)).

⁵ *Id.* at 14051 (proposing Section 76.1211(a)).

⁶ *Id.* at 14045-6.

⁷ The comment does not offer an opinion on whether these public commitments would render the business-to-business certifications irrelevant, or whether that certification process could parallel the public commitments.

⁸ For example, in a 2012 report, the FTC committed to promote industry self-regulation through enforceable codes of conduct, which the FTC could enforce against companies that “fail[] to abide by the self-regulatory programs they join.” *See Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policy Makers* at 14 (Mar. 2012), available at <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>.

been a critical part of the FTC’s consumer protection mission for 45 years and continues to be central to its mission today.

A. Enforcement

The FTC is first and foremost a civil law enforcement agency. The FTC’s primary law enforcement tool, the FTC Act, prohibits unfair and deceptive acts or practices in or affecting commerce.⁹ A representation, omission, or practice is deceptive if it is material and likely to mislead consumers acting reasonably under the circumstances.¹⁰ An act or practice is unfair if it causes, or is likely to cause, substantial injury that is not reasonably avoidable by consumers or outweighed by countervailing benefits to consumers or competition.¹¹ The FTC also enforces sector-specific statutes that protect information relating to health, credit and other financial matters, and children’s online information, and has issued regulations implementing each of these statutes.

The FTC began its online privacy enforcement program nearly two decades ago.¹² In recent years, the FTC has brought enforcement actions against companies such as Microsoft, Facebook, Google, Equifax, HTC, Snapchat, and Wyndham.¹³ The FTC has also brought many cases enforcing privacy promises claiming compliance with industry codes of conduct. Specifically, when a company makes a representation to comply with a particular code or set of principles, but fails to do so, this could constitute a deceptive practice under Section 5 of the FTC Act.¹⁴ The following examples illustrate the FTC’s enforcement experience with privacy-related industry codes of conduct.

First, the FTC has brought cases against companies that offer “privacy seals” or certifications for other companies’ privacy practices. In 2014, the FTC settled charges that TRUSTe, a major provider of privacy certifications for online businesses, falsely represented that it conducted annual validations of websites with the TRUSTe seal.¹⁵ The FTC’s complaint alleged that for over six years and in over 1,000 instances, TRUSTe failed to conduct annual recertifications of companies holding TRUSTe privacy seals, despite providing information on its website that companies holding TRUSTe Certified Privacy Seals receive recertification every year. The order prohibits misrepresentations, requires monitoring, and mandated \$200,000 of disgorgement. In 2010, the FTC settled charges against ControlScan, a company that purported

⁹ *See id.*

¹⁰ *See* FTC Policy Statement on Deception at 1 (*appended to Cliffdale Assocs., Inc.*, 103 F.T.C. 110, 174 (1984)), available at <https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception>.

¹¹ 15 U.S.C. § 45(n).

¹² *Geocities*, No. C-3850 (FTC Feb. 12, 1999), available at <https://www.ftc.gov/enforcement/cases-proceedings/982-3015/geocities>.

¹³ *See generally* FTC, Privacy and Security Cases, https://www.ftc.gov/tips-advice/business-center/legal-resources?title=&type=case&field_consumer_protection_topics_tid=245.

¹⁴ The FTC’s privacy enforcement activity also has extended to the types of technologies implicated by the NPRM. In 2001, at the request of members of Congress, the FTC inquired into the data collection and sharing practices of TiVo, and ultimately decided to close the investigation. *See* Letter from FTC Chairman Robert Pitofsky regarding TiVo Investigation (May 11, 2001), available at https://www.ftc.gov/system/files/documents/public_statements/944143/010511tivoinvestigationltr.pdf.

¹⁵ *In the Matter of TRUSTe, Inc.*, Dkt. No. C-4512 (Nov. 17, 2014), available at <https://www.ftc.gov/enforcement/cases-proceedings/132-3219/true-ultimate-standards-everywhere-inc-truste-matter>.

to certify the privacy and security of online retailers and certain other websites.¹⁶ ControlScan offered a variety of privacy and security seals for display on websites. Consumers could click on the seals to discover exactly what assurances each seal conveyed. The FTC alleged that ControlScan deceived consumers about how often it actually monitored the sites that displayed its seals and the steps it took to verify the sites' privacy and security practices. The order bars such misrepresentations, required the company to take down its seals, and includes an over-\$850,000 judgment for disgorgement against the company and its founder.

Second, international data-transfer agreements permitting the global transfer of data – including the recently negotiated Privacy Shield Framework and its predecessor, the U.S.-EU Safe Harbor Framework – are also founded on the enforceability of promises to comply with codes of conduct. For example, the Privacy Shield, once finalized, will allow companies to export data collected in the EU to the United States if they commit to the code of conduct and certify compliance. These representations are enforceable under the FTC Act, pursuant to the prohibition on deceptive statements,¹⁷ and strengthen the privacy protections provided to EU citizens in the United States.¹⁸ The FTC has brought 39 cases involving alleged deceptive claims regarding a firm's compliance with the Safe Harbor Framework, and has committed to vigorously enforce the Privacy Shield Framework going forward.

Finally, in a case against Google – which the FTC settled for \$22.5 million – the FTC alleged that Google provided deceptive instructions for opting out of third-party cookies on Apple's Safari browser.¹⁹ The complaint alleged that Google's deceptive opt-out instructions contradicted its promise to abide by the Network Advertising Initiative's ("NAI") code of conduct, which requires truthful disclosure of data practices. The FTC's complaint alleged, among other things, that Google's representation of compliance with the NAI code was deceptive.

B. Policy and Education

The FTC has long encouraged industry to establish strong, enforceable codes of conduct.²⁰ In addition, the FTC has written reports and hosted a variety of workshops to discuss policy solutions to address privacy and technological issues similar to those raised by the NPRM.

¹⁶ *FTC v. ControlScan*, Civ. No. 1:10-cv-0532 (N.D.Ga. Feb. 25, 2010), available at <https://www.ftc.gov/enforcement/cases-proceedings/072-3165/federal-trade-commission-plaintiff-v-controlscan-inc>.

¹⁷ See *supra* n.11.

¹⁸ See Letter from Chairwoman Edith Ramirez to Commissioner Věra Jourová, at 1-2 (Feb. 23, 2016).

¹⁹ The \$22.5 million penalty against Google arose from the fact that the complaint alleged violations of a prior consent decree. For initial violations of the FTC Act, the FTC lacks civil penalty authority, but is able to pursue equitable remedies, including disgorgement. A company that fails to comply with an FTC order is subject to a civil penalty of up to \$16,000 per violation, or \$16,000 per day for a continuing violation. See 15 U.S.C. § 45(l); 16 C.F.R. § 1.98(c).

²⁰ See, e.g., Prepared Statement of the FTC on Emerging Threats in the Online Advertising Industry, Before the Comm. on Homeland Security and Governmental Affairs, Permanent Subcomm. on Investigations, 113th Cong. at 2 (May 15, 2014), available at

https://www.ftc.gov/system/files/documents/public_statements/309891/140515emergingthreatsonline.pdf;

Testimony of the FTC on the Use of Facial Recognition Technology by Governments and the Private Sector Before the Senate Comm. on the Judiciary Subcomm. on Privacy, Technology, and the Law, 112th Cong. (July 18, 2012), available at https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-use-facial-recognition-technology-governments-and/120718facialrecognition.pdf.

In February 2013, for example, the FTC published a staff report encouraging clear and conspicuous privacy disclosures on mobile devices.²¹ In January 2015, the FTC published a staff report on the Internet of Things that encouraged the development of industry codes of conduct.²² In November 2015, the FTC held a workshop on cross-device tracking to examine how companies are able to link the activities of a single consumer across devices, including computers, smartphones, and televisions.²³ And later this year, the FTC will host a workshop on “smart” TVs, which will bring together industry, academic, government, and consumer protection experts to explore the privacy implications of pervasive tracking of consumers’ media consumption.²⁴

Finally, the FTC engages in extensive outreach efforts to provide business guidance and consumer education about privacy and data security. The FTC has distributed millions of copies of education materials for consumers and businesses to address security and privacy.²⁵ The FTC also develops and maintains several popular web-based resources for consumers and businesses to learn more about privacy and security.²⁶ For example, earlier this month, the FTC launched an online tool that health apps can use to determine what laws and regulations govern their activities, which the FTC developed in coordination with other federal agencies.²⁷

III. Suggestions Regarding the Proposed Certification Program

I support the FCC’s efforts to protect consumer privacy in connection with its proposal to expand the market for set-top boxes. The FCC’s proposal that cable and satellite companies require third-party set-top box manufacturers to certify compliance with the same protections applicable to cable and satellite companies will provide valuable privacy protections for

²¹ FTC Staff Report, *Mobile Privacy Disclosures: Building Trust Through Transparency* 15-16 (February 2013), available at <https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf>. See also FTC Workshop, *In Short: Advertising & Privacy Disclosures in a Digital World* (May 30, 2012), <https://www.ftc.gov/news-events/events-calendar/2012/05/short-advertising-privacy-disclosures-digital-world>.

²² FTC Staff Report, *Internet of Things: Privacy and Security in a Connected World* 49 (Jan. 2015) available at <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>; See also FTC Workshop, *Internet of Things: Privacy and Security in a Connected World* (Nov. 19, 2013), <https://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-security-connected-world>.

²³ FTC Workshop: *Cross-Device Tracking* (Nov. 16, 2015), <https://www.ftc.gov/news-events/events-calendar/2015/11/cross-device-tracking>.

²⁴ Fall Technology Series: *Smart TV* (Dec. 7, 2016), <https://www.ftc.gov/news-events/events-calendar/2016/12/fall-technology-series-smart-tv>.

²⁵ See *Privacy & Data Security Update* (2015), available at <https://www.ftc.gov/reports/privacy-data-security-update-2015>.

²⁶ See, e.g., *IdentifyTheft.gov* (<http://www.identitytheft.gov>); *OnguardOnline.gov* (<http://www.onguardonline.gov>); *Start with Security: A Guide for Business* (<https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business>).

²⁷ FTC, *Mobile Health Apps Interactive Tool*, available at <https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool>. The FTC developed the guidance tool in conjunction with the Department of Health and Human Service’s Office of the National Coordinator for Health Information Technology, the Office for Civil Rights, and the Food and Drug Administration.

consumers.²⁸ The FTC’s experience in supporting and enforcing privacy codes of conduct provides valuable guidance about how the certification approach proposed by the FCC can be effective. Requiring third-party set-top box manufacturers to promise that they will comply with cable and satellite statutory privacy provisions will be effective only if such promises are enforceable. The FTC can enforce manufacturers’ promises by using its Section 5 authority to prohibit deceptive practices, as it has done in the types of cases described in Section II.²⁹

The FCC’s final rule on set-top boxes should require that MVPDs provide access only to those third-party set-top boxes that have provided *consumer-facing* statements promising to comply with the privacy obligations that apply to MVPDs.³⁰ The FTC’s deception authority is clearly implicated by certifications to consumers. Examples of enforceable statements to consumers could include statements within privacy policies, on other portions of a consumer-facing website, on a retail box, on the device itself, or in the user interface of the device. In any scenario, the third-party set-top box manufacturers should make a representation to consumers that their set-top boxes will offer the same privacy protections that the cable and satellite privacy statutes require.

To help consumers better understand these privacy promises, third-party set-top box manufacturers should provide clear and prominent disclosures. The FTC has published several reports that provide suggestions for effective disclosure of data practices, all of which emphasize the importance of short, easy-to-understand, and just-in-time disclosures.³¹ Such disclosures could include a set-top box privacy “pledge” that would appear on the product package, the product specification page, and/or other prominent locations. The pledge could include a link to a consumer-friendly website explaining the manufacturers’ obligations under the pledge.³² MVPDs and third parties could then commit to this pledge. Section 5 liability would be triggered if any of the set-top box manufacturers’ practices were inconsistent with any material obligations of the pledge. Consumers that are only interested in determining whether a set-top box would honor the standard privacy protections could look for the pledge on the box or the website. Those consumers with greater interest in understanding the content of the pledge would be able to review the terms of the pledge on the consumer-friendly website.

IV. Conclusion

If the FCC proceeds with the proposed set-top box rule, the final rule would mandate that MVPDs provide data access only to third-party set-top box manufacturers that have certified

²⁸ Because the privacy protections implicated by the proposed certification requirement are the same protections that Congress enacted under Cable Communications Policy Act of 1984, the FTC is not commenting on the substance of these protections.

²⁹ The FTC also can enforce the promises that cable and satellite providers make to consumers, including promises regarding their data collection, use, and disclosure practices.

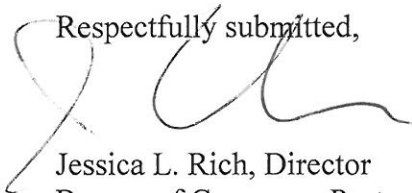
³⁰ The NPRM asks who should be responsible for maintaining a record of certifications, and suggests as possibilities a standards body or the FCC itself. For the purpose of FTC Act liability, a repository of certifications would not be necessary, provided that the statements are consumer-facing.

³¹ See *supra* n.8 at 15-16; n.24 at 39-43.

³² I encourage consumer testing of disclosures, to the extent feasible. The FTC has found testing to be a useful tool for developing effective consumer privacy disclosures. See, e.g., Financial Privacy Rule: Interagency Notice Research Project (Mar. 2011), available at <https://www.ftc.gov/tips-advice/business-center/guidance/financial-privacy-rule-interagency-notice-research-project> (describing eight-agency research project to develop privacy disclosures related to the Gramm-Leach-Bliley Act).

compliance with the privacy statutes that apply to cable and satellite companies. I encourage the FCC to require that cable and satellite companies limit access only to those third-party set-top box manufacturers that also have made public promises about these certifications to consumers, so that the FTC can provide an effective enforcement backstop.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'J. Rich', is written over the text 'Respectfully submitted,'.

Jessica L. Rich, Director
Bureau of Consumer Protection