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 Navi gation Choices, MB Docket No. 16-42
Commercial Availability of Navigation Devices, CS Docket No. 97-80
Comment of the Director of the Bu reau 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

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 (NP RM), 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. S

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 V ra Jourov Æ, 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*

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 Prop osed 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

[redacted]

tfully submitted,

Respec

L. Rich, Director
ad of Consumer Protection

Jessica
Bureau