PREPARED STATEMENT OF

THE FEDERAL TRADE COMMISSION

on

Examining Ways to Improve Vehicle and Roadway Safety

Before the

COMMITTEE ON ENERGY AND COMMERCE

SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE

UNITED STATES HOUSE OF REPRESENTATIVES

Washington, D.C.

October 21, 2015

Doctor Burgess, Ranking Member Schakowsky, and members of the Subcommittee, I am Maneesha Mithal, Associate Director of the Division of Privacy and Identity Protection of the Bureau of Consumer Protection at the Federal Trade Commission ("FTC" or "Commission").[1] I appreciate the opportunity to present the Commission's testimony on the privacy- and security-related provisions of the discussion draft to provide greater transparency, accountability, and safety authority for the National Highway Traffic Safety Administration ("NHTSA"). While the Commission supports the Subcommittee's goal of protecting the privacy and security of consumers' information, we have concerns about the provisions as drafted.

I. BACKGROUND

The FTC has served as the primary federal agency charged with protecting consumer privacy and data security dating back to the 1970 enactment of the Fair Credit Reporting Act ("FCRA").[2] Beginning with the development of the Internet as a commercial medium in the mid-1990s, the FTC expanded its focus on privacy to reflect the growing collection, use, and sharing of consumer data in the commercial marketplace. Since then, using its enforcement authority, the Commission has brought hundreds of privacy and data security cases targeting violations of the Federal Trade Commission Act,[3] the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act,[4] the Do Not Call provisions of the Telemarketing Sales Rule,[5] the CAN

[1] This written statement presents the views of the Federal Trade Commission. My oral statements and responses to questions are my own and do not necessarily reflect the views of the Commission or of any Commissioner.

[2] 15 U.S.C. §§ 1681-1681x.

[3] 15 U.S.C. § 45(a).

[4] 16 C.F.R. Part 314, implementing 15 U.S.C. § 6801(b).

[5] 16 C.F.R. Part 310.

SPAM Act,[6] and the Children's Online Privacy Protection Act (COPPA).[7] These actions have addressed practices offline, online, and in the mobile and connected device environments.

In addition to enforcing a wide range of privacy and security laws, the FTC has distributed millions of copies of educational materials for consumers and businesses to improve their understanding of ongoing threats to security and privacy. Most recently, the FTC launched its "Start With Security" business education initiative that includes new guidance for businesses as well as a series of conferences across the country.[8] The business guidance lays out ten key steps to effective data security, drawn from the FTC's data security cases. It is designed to provide an easy way for companies to understand the lessons learned from our cases. It includes references to the cases, as well as plain-language explanations of the security principles that companies should implement.[9] In addition to the new guidance, the FTC also has introduced a one-stop website that consolidates the Commission's data security information for businesses.[10]

On the policy front, the Commission regularly holds seminars and workshops to examine the implications of new technologies and business models on consumer privacy and security. For example, at its Internet of Things workshop in November 2013, the Commission specifically examined privacy and security issues relating to the different technologies in connected cars, including Event Data Recorders ("EDRs") and other vehicle telematics.[11] Workshop participants

---

[6] 15 U.S.C. §§ 7701-7713.

[7] 15 U.S.C. §§ 6501-6506; *see also* 16 C.F.R. Part 312.

[8] *See* FTC Press Release, *FTC Kicks Off "Start With Security" Business Education Initiative* (June 30, 2015), *available at* https://www.ftc.gov/news-events/press-releases/2015/06/ftc-kicks-start-security-business-education-initiative.

[9] *See* FTC, *Start With Security: Lessons Learned From FTC Cases* (2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[10] *See* www.ftc.gov/datasecurity.

[11] FTC Workshop, *Internet of Things - Privacy and Security in a Connected World* (Nov. 19, 2013), *available at* https://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-security-connected-world. The workshop's panel on connected car technologies is on pages 235-291 of the workshop transcript *available at* http://www.ftc.gov/sites/default/files/documents/public_events/internet-

described the many safety and convenience benefits that connected cars offer. At the same time, participants described the potential privacy and security risks arising from this connectivity, including concerns about the ability of connected car technology to track consumers' precise geolocation over time; concerns that information about driving habits could be used to price insurance premiums or set prices for other auto-related products, without drivers' knowledge or consent; and concerns related to the security of connected cars. The Commission staff issued a report summarizing the workshop and outlining policy recommendations on the Internet of Things earlier this year.[12]

Finally, the FTC has provided advocacy statements to other government agencies considering regulatory actions in this area. In October 2014, the Commission filed a comment on NHTSA's advance notice of proposed rulemaking related to vehicle-to-vehicle (V2V) communications.[13] In its comment, the FTC expressed support for NHTSA's deliberative, process-based approach to addressing privacy and security risks and commended it for designing a V2V system to limit the data collected and stored to only that which serves its intended safety purpose. The Commission also has engaged in discussions with industry representatives and others on these very important issues.

---

things-privacy-security-connected-world/final_transcript.pdf.

[12] *See FTC Staff Report on the Workshop "Internet of Things: Privacy and Security in a Connected World"* (Jan. 27, 2015), *available at* https://www.ftc.gov/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things.

[13] *See Federal Trade Commission Comment Before the National Highway Traffic Safety Administration Regarding the NHTSA Proposed Rule Entitled "Federal Motor Vehicle Safety Standards: Vehicle-to-Vehicle (V2V) Communications," and the Accompanying Report, and Addressing Privacy and Security Issues Raised in the V2V Report and the Proposed Rule* (Oct. 20, 2014), *available at* https://www.ftc.gov/system/files/documents/advocacy_documents/federal-trade-commission-comment-national-highway-traffic-safety-administration-regarding-nhtsa/141020nhtsa-2014-0022.pdf.

II. Discussion Draft

The Commission is pleased to offer its views on Title III of the discussion draft, which focuses on privacy and security for connected vehicles. We appreciate that one of the goals of the discussion draft is to improve privacy protections for consumers and to provide incentives for vehicle manufacturers to adopt and implement best practices for vehicle security and safety. However, we have concerns about several aspects of the provisions of Title III.

A. Privacy Provisions

The draft would amend title 49 of the U.S. Code to add Section 32402(e), which grants a broad safe harbor from FTC law enforcement actions to any vehicle manufacturer who submits a privacy policy to the Secretary of Transportation that explains the notice, choices, and privacy-related commitments the manufacturer will make. Under this proposal, manufacturers can satisfy the requirements of this section without providing any substantive protections for consumer data. For example, a manufacturer's policy could qualify for a safe harbor even if it states that the manufacturer collects numerous types of personal information, sells the information to third parties, and offers no choices to opt out of such collection or sale. Moreover, because the safe harbor exempts a manufacturer from FTC oversight, and Section 32402(d)(2) provides a separate exemption from civil penalties, a manufacturer that submits a privacy policy that meets the requirements of Section 32402(b) but does not follow it would not be subject to any enforcement mechanism. Furthermore, although the privacy policy requirements only apply to information collected from vehicle "owners, renters, or lessees," the safe harbor would immunize manufacturers for privacy practices related to other types of consumers – such as collecting information from vehicle shoppers through manufacturers' websites. Thus, for example, the Commission could be precluded from bringing a Section 5

action[14] based on any privacy-related misrepresentation on a manufacturer's website, even if the misrepresentation is unrelated to vehicle data. Precluding the Commission from taking action against such misrepresentations goes well beyond Title III's focus on vehicle data, particularly in light of the Commission's extensive experience in consumer privacy enforcement.[15]

Section 32402(c) would authorize manufacturers to update privacy policies' terms simply by submitting an updated policy to the Secretary of Transportation. This provision would enable a manufacturer to make a material change to its privacy policy and then unilaterally apply the new policy to consumer data collected under its earlier policy. By contrast, the Commission has acted in a number of instances to ensure that consumers can rely on the terms of privacy policies in effect at the time information is collected by prohibiting a company from making material changes to those terms without first obtaining consumers' affirmative express consent.[16]

B. Hacking Provisions

Section 302 of the discussion draft would prohibit unauthorized access to an electronic control unit, critical system, or other system containing driving data. We support the goal of deterring criminals from accessing vehicle data. Security researchers have, however, uncovered security vulnerabilities in connected cars by accessing such systems.[17] Responsible researchers often contact companies to inform them of these vulnerabilities so that the companies can voluntarily make their cars safer. By prohibiting such access even for research purposes, this

---

[14] Section 5 of the FTC Act prohibits unfair or deceptive acts or practices in or affecting commerce. 15 U.S.C. § 45(a).

[15] *See supra* pp. 1-3.

[16] *See, .e.g., Facebook, Inc.*, No. C-4365 (F.T.C. July 27, 2012), *available at* https://www.ftc.gov/enforcement/cases-proceedings/092-3184/facebook-inc; *Gateway Learning Corp.*, No. C-4120 (F.T.C. Sept. 10, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/042-3047/gateway-learning-corp-matter.

[17] *See, e.g.*, Remarks of Professor Tadayoshi Kohno, Transcript of Internet of Things Workshop at 245-47, *supra* n.7; Charlie Miller & Chris Valasek, *Remote Exploitation of an Unaltered Passenger Vehicle* (2015), *available at* http://illmatics.com/Remote%20Car%20Hacking.pdf.

provision would likely disincentivize such research, to the detriment of consumers' privacy, security, and safety.[18]

C. Security Provisions

Section 303 of the draft amends title 49 of the U.S. Code Section 30701 to establish an "Automotive Cybersecurity Advisory Council" to "develop best practices for cybersecurity for manufacturers of automobiles offered for sale in the United States." Section 30701(a)(4)(B). Manufacturers that implement these best practices will be immunized from liability under Section 5 of the FTC Act with respect to any unfair or deceptive conduct "relating to" these best practices. Section 30701(g). We appreciate that the drafters intend to spur the development of best practices in security. However, we are concerned that the current draft will not encourage best practices robust enough to protect consumers.

First, at least fifty percent of the Council's membership must consist of representatives of automobile manufacturers. Although NHTSA, the Department of Defense, and the National Institute of Standards and Technology would have seats on the Council, it appears that all other stakeholders, including consumer advocates, security researchers, other automotive industry members, and others would be limited to one member.[19] Because any best practices approved by the Council will be "by a simple majority of members," manufacturers alone could decide what best practices would be adopted.

---

[18] Arguably, such a move would be out of step with direction of other industries, in which many companies pay "bug bounties" to researchers who discover software vulnerabilities, to encourage researchers to report the vulnerabilities in a manner that allows companies to fix them. *See, e.g.*, AT&T, AT&T Bug Bounty Program, *available at* https://bugbounty.att.com/ (last visited Oct. 18, 2015); Microsoft TechNext, Microsoft Bounty Programs, *available at* https://technet.microsoft.com/en-us/library/dn425036.aspx (last visited Oct. 18, 2015); Mozilla, Bug Bounty Program, *available at* https://www.mozilla.org/en-US/security/bug-bounty/ (last visited Oct. 18, 2015); United, United Airlines Bug Bounty Program, *available at* https://www.united.com/web/en-US/content/Contact/bugbounty.aspx (last visited Oct. 18, 2015).

[19] Notably, despite the fact that a company will enjoy immunity from FTC Act liability if its plan is approved by the NHTSA Administrator, the FTC does not have a seat on the Council.

Second, the discussion draft contains eight areas the best practices *"may"* – not must – cover. If the discussion draft required each of the eight areas to be addressed, it would at least create a minimum standard that the best practices would have to meet. However, the discussion draft does not do that. The Council – the majority of members of which are auto manufacturers – will decide the appropriate areas for best practices.

Third, a key component of data security is the need to update practices in light of emerging risks and technologies. The discussion draft requires the Council to meet annually to review the best practices, but leaves it up to the Council to adopt additional best practices "as necessary" in subsequent years, which could mean that risks are not addressed in a timely fashion. The discussion draft allows, but does not require, manufacturers to submit updated plans if they choose to modify their plans.

Fourth, although the statute requires NHTSA Administrator approval of a plan submitted by a manufacturer, NHTSA has little discretion in this regard. The Administrator may only reject a plan if he or she "demonstrates by clear and convincing evidence" that the plan is not consistent with the best practices adopted by the Council. This is too high a review standard, and would likely result in the approval of plans that may meet the bare minimum best practices on paper, but are in practice not appropriately tailored to foreseeable, evolving threats.

Finally, the proposed safe harbor is so broad that it would immunize manufacturers from liability even as to deceptive statements made by manufacturers relating to the best practices that they implement and maintain. For example, false claims on a manufacturer's website about its use of firewalls, encryption, or other specific security features would not be actionable if these subjects were also covered by the best practices.

In sum, the Commission understands the desire to provide businesses with certainty and incentives, in the form of safe harbors, to implement best practices. However, the security provisions of the discussion draft would allow manufacturers to receive substantial liability protections in exchange for potentially weak best practices instituted by a Council that they control. The proposed legislation, as drafted, could substantially weaken the security and privacy protections that consumers have today.

III. CONCLUSION

Thank you for the opportunity to provide the Commission's views on the privacy and cybersecurity provisions of the discussion draft. We look forward to continuing to work with the Subcommittee and Congress on this critical issue.