



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

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

November 21, 2016

Nathaniel Beuse
Associate Administrator for Vehicle Safety Research
National Highway Traffic Safety Administration

Re: Request for Comment on “Federal Automated Vehicles Policy,” Docket No. NHTSA-2016-0090, Comment of the Director of the Bureau of Consumer Protection of the Federal Trade Commission¹

Dear Associate Administrator Beuse:

As the Director of the Federal Trade Commission’s Bureau of Consumer Protection, I submit this comment to express my support for the inclusion of consumer privacy and cybersecurity guidance in the National Highway Traffic Safety Administration (“NHTSA” or “Administration”) document, “Federal Automated Vehicles Policy: Accelerating the Next Revolution in Roadway Safety” (“Policy Report”).²

The FTC: Protecting Consumer Privacy and Security in the Internet of Things

The FTC is an independent agency charged by Congress with promoting consumer protection and competition in the marketplace. Privacy has been a critical part of the FTC’s consumer protection mission for forty-five years and continues to be central to its mission today. In recent years, in response to rapidly evolving technology markets, a chief focus of the FTC’s privacy and security efforts has been connected devices and the Internet of Things (“IoT”).

First, we have used our civil law enforcement authority under Section 5 of the FTC Act to take action against manufacturers of connected devices that have engaged in unfair or deceptive practices. Earlier this year, for example, the Commission settled allegations against device manufacturer ASUSTeK Computer (“ASUS”).³ The Commission alleged that critical security flaws in ASUS’s routers placed the home networks of hundreds of thousands of consumers at risk. Moreover, the Commission charged that the routers’ insecure “cloud” services led to the compromise of thousands of consumers’ connected storage devices, exposing

¹ Request for Comment on “Federal Automated Vehicles Policy,” 81 Fed. Reg. 65,703 (Sept. 23, 2016).

² Nat’l Highway Traffic Safety Admin., Federal Automated Vehicles Policy: Accelerating the Next Revolution in Road Safety, <https://www.transportation.gov/AV/federal-automated-vehicles-policy-september-2016>.

³ See Press Release, FTC, ASUS Settles FTC Charges That Insecure Home Routers and “Cloud” Services Put Consumers’ Privacy At Risk (Feb. 23, 2016), <https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put>.

their sensitive personal information on the internet. Among other things, the consent agreement required ASUS to establish a comprehensive security program and to notify consumers about software updates or other steps they can take to protect themselves from security flaws.

Second, the FTC has issued reports and hosted a variety of workshops to discuss policy solutions to address privacy and technological issues in the connected space. In January 2015, the FTC published a staff report on the IoT.⁴ This report synthesized and expanded upon our learning from a November 2013 workshop that addressed privacy and security issues in a variety of contexts, including connected cars. In October 2016, we held a workshop examining how the growing use of unmanned aerial drones may impact consumer privacy. And in December 2016, we will host a workshop on “smart” TVs, which will bring together industry, academic, government, and consumer protection experts to explore the privacy implications of this new technology, such as tracking of consumers’ media consumption and use of apps.⁵

Third, the FTC engages in extensive outreach efforts to provide business guidance and consumer education about privacy and data security. The Commission has distributed millions of copies of education materials for consumers and businesses to address security and privacy.⁶ The FTC also develops and maintains several popular web-based resources for consumers and businesses to learn more about privacy and security.⁷ For example, this summer, the FTC issued business and consumer guidance on protecting consumer privacy when renters connect their devices to their rental cars.⁸ Last year, we issued a security guidance document for companies designing and marketing IoT products.⁹

NHTSA’s Federal Automated Vehicles Policy

NHTSA’s Policy Report represents a significant step forward in adapting the current regulatory framework to the coming new age of autonomous vehicles. Although there are significant challenges in transitioning to fully autonomous vehicles, NHTSA’s thoughtful approach will help ease that transition and usher in a new era in transportation – a new era made possible by, among other things, innovative uses of information.

⁴ FED. TRADE COMM’N STAFF, INTERNET OF THINGS: PRIVACY AND SECURITY IN A CONNECTED WORLD 49 (2015) <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>; see also Fed. Trade Comm’n Workshop, *Internet of Things: Privacy & Security in a Connected World* (Nov. 19, 2013), <https://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-security-connected-world>.

⁵ Fed. Trade Comm’n Fall Technology Series, *Smart TV* (Dec. 7, 2016), <https://www.ftc.gov/news-events/events-calendar/2016/12/fall-technology-series-smart-tv>.

⁶ See FED. TRADE COMM’N, PRIVACY & DATA SECURITY UPDATE: 2015, https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2015/privacy_and_security_data_update_2015-web_0.pdf.

⁷ See, e.g., IdentifyTheft.gov, <http://www.identitythefit.gov>; OnguardOnline.gov, <http://www.onguardonline.gov>; FED. TRADE COMM’N, START WITH SECURITY: A GUIDE FOR BUSINESS (2015), <https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business>.

⁸ FED. TRADE COMM’N, LEAVING INFO BEHIND, IN (RENTAL) CARS (2016), <https://www.ftc.gov/news-events/blogs/business-blog/2016/08/leaving-info-behind-rental-cars>; FED. TRADE COMM’N, WHAT IS YOUR PHONE TELLING YOUR RENTAL CAR (2016), <https://www.consumer.ftc.gov/blog/what-your-phone-telling-your-rental-car>.

⁹ FED. TRADE COMM’N, CAREFUL CONNECTIONS: BUILDING SECURITY IN THE INTERNET OF THINGS (2015), <https://www.ftc.gov/tips-advice/business-center/guidance/careful-connections-building-security-internet-things>.

Information collection, transmission, storage, and analysis are integral to realizing a vision of vehicles that are significantly safer and more efficient than the cars we drive today. Therefore, it is appropriate that the Policy Report, in addition to emphasizing vehicle safety, includes recommendations designed to ensure that privacy and security issues are considered throughout the vehicle lifecycle, particularly in the design phase.

As vehicles grow ever more connected – with the inclusion of apps, hands-free calling, and other functions integrated in the vehicle or enabled through platform interfaces such as Apple CarPlay, Google Android Auto and Windows Embedded Automotive – it is crucial that vehicle manufacturers (or “OEMs”) and other entities ensure that consumer privacy protections are built in from the start. The guidance outlined in the Policy Report addresses key issues such as transparency, choice, and security. For example, Section I(E)(1) on Data Recording and Sharing first notes that highly automated vehicles (“HAVs”) “have great potential to use data sharing to enhance and extend safety benefits.... Such shared data would help to accelerate knowledge and understanding of HAV performance, and could be used to enhance the safety of HAV systems and to establish consumer confidence in HAV technologies.” The Section further notes that the benefits from sharing this data can be realized without including personally identifiable information: “Generally, data shared with third parties should be de-identified (i.e., stripped of elements that make the data directly or reasonably linkable to a specific HAV owner or user).” Alternatively, OEMs and other entities can share the data with owner/user consent. This Section highlights the challenge in striking an appropriate balance that permits uses of data for important safety purposes, while protecting the privacy of that data,¹⁰ and I applaud NHTSA for explicitly grappling with this challenge.¹¹

Section I(E)(2) states that OEMs’ privacy policies and practices should follow the protections outlined in FTC guidance and the Consumer Privacy Bill of Rights – protections based on the Fair Information Practice Principles, such as choice, respect for context, and data security. I applaud NHTSA for encouraging compliance with these strong principles. In particular, the transparency principle, which requires OEMs to have public-facing privacy policies, is an important one because it would permit the FTC to take action against companies that misstate their information collection and use practices. By requiring companies to consciously think about their privacy practices, clearly and publicly articulate them, and ensure that their statement matches their practices, the transparency principle also provides an important accountability function.

¹⁰ I recognize that Section I(E)(1) will not be finalized until NHTSA completes the Paperwork Reduction Act process for its data collection and reporting requirements.

¹¹ To the extent OEMs share “de-identified” data, it is important that they take reasonable steps to ensure that the data cannot be re-identified. As technology improves, there is always a possibility that purportedly de-identified data could be re-identified. This is why it is important for OEMs to also have accountability mechanisms in place. For example, they should include contractual provisions with third parties with whom they share the data, requiring the third parties to commit not to re-identify the data.

I also commend NHTSA for its inclusion of cybersecurity recommendations in the Policy Report.¹² In recent years, a number of security researchers have demonstrated that they are able to access and control key vehicle functions.¹³ NHTSA is already well aware that cybersecurity risks are real, and the potential for harm, enormous.¹⁴ To address these risks, the Policy Report emphasizes that “manufacturers and other entities should follow a robust product development process based on a systems-engineering approach to minimize risks to safety, including those due to cybersecurity threats and vulnerabilities.”¹⁵ This message is vitally important, and one that the Commission has emphasized consistently, such as in the agency’s “Start with Security” business education materials¹⁶ and the Commission’s report, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers*.¹⁷

Finally, I support the recommendation that companies share their experiences throughout the industry so that every company does not “have to experience the same cyber vulnerabilities in order to learn from them.”¹⁸ Although information sharing is not a panacea, robust information sharing can help industry members identify threats and act to prevent or mitigate security incidents. The FTC has supported industry efforts to share cybersecurity-related information in ways that do not run afoul of the antitrust laws. For example, in a policy statement issued jointly with the Department of Justice regarding the antitrust implications of legitimate cybersecurity information sharing, the Commission noted that one way to improve the nation’s “resilience to cyber incidents and to reduce and defend against cyber threats” is “by increasing cyber threat information sharing between the government and industry, and among industry participants,”¹⁹ and explained that “properly designed sharing of cybersecurity threat information is not likely to raise antitrust concerns.”²⁰

¹² I note that NHTSA separately issued a cybersecurity-focused guidance document, *Cybersecurity Best Practices for Modern Vehicles*, with best practices applicable to all types of vehicles, not just autonomous vehicles. See http://www.nhtsa.gov/About-NHTSA/Press-Releases/nhtsa_cybersecurity_best_practices_10242016. This document emphasized and reinforced key themes in the Policy Report, including the importance of cybersecurity throughout the product lifecycle. See, e.g., *Cybersecurity Best Practices for Modern Vehicles* at 12 (“Companies should make cybersecurity a priority by using a systematic and ongoing process to evaluate risks. This process should give explicit considerations [sic] to privacy and cybersecurity risks through the entire life-cycle of the vehicle.”).

¹³ See, e.g., Press Release, NY Univ., Tandon Sch. of Eng’g, *Researchers Find Vulnerabilities in Cars Connected to Smartphones* (Aug. 31, 2016), <http://engineering.nyu.edu/press-releases/2016/08/31/researchers-find-vulnerabilities-cars-connected-smartphones>; CHARLIE MILLER & CHRIS VALASEK, REMOTE EXPLOITATION OF AN UNALTERED PASSENGER VEHICLE (2015), [illmatics.com/Remote Car Hacking.pdf](http://illmatics.com/Remote%20Car%20Hacking.pdf).

¹⁴ See NHTSA Action Number EQ15005, <http://www-odi.nhtsa.dot.gov/owners/SearchResults>; NHTSA Campaign Number 15V508000, <http://www-odi.nhtsa.dot.gov/owners/SearchResultsByUrlCode.action?referenceSearch.requestId=84074&referenceSearch.urlCode=PYBUMLTQNYBCPHC>.

¹⁵ Policy Report at 21.

¹⁶ See <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>.

¹⁷ *Supra* note 15 at 3.

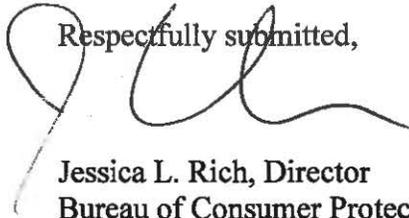
¹⁸ Policy Report at 21-22.

¹⁹ Department of Justice and Federal Trade Commission: Antitrust Policy Statement on Sharing of Cybersecurity Information, <https://www.ftc.gov/public-statements/2014/04/departement-justice-federal-trade-commission-antitrust-policy-statement>, at 2.

²⁰ *Id.* at 9.

In short, I support NHTSA's thoughtful consideration of the emerging issues presented by innovative technologies in vehicles, and the agency's strong commitment to protect consumer privacy and vehicle cybersecurity in the HAV area. I appreciate the opportunity to provide comments on the Policy Report and would be happy to provide further assistance to NHTSA as it moves forward on this important initiative.

Respectfully submitted,

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

Jessica L. Rich, Director
Bureau of Consumer Protection