ConsumersUnion®

POLICY & ACTION FROM CONSUMER REPORTS

May 1, 2017

Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue N.W.
Suite CC-5610 (Annex A)
Washington, D.C. 20580

Submitted via www.ftc.gov.

Comments of Consumers Union to the
Federal Trade Commission and the National Highway Traffic Safety Administration on the
Notice of Workshop and Request for Public Comments on
"Connected Cars - Workshop, Project No. P175403"

Consumers Union, the policy and mobilization arm of Consumer Reports,[1] welcomes the opportunity to submit comments in advance of the June 28, 2017, public workshop hosted by the Federal Trade Commission (FTC) and the National Highway Traffic Safety Administration (NHTSA) on consumer privacy and security issues posed by motor vehicles with wireless connectivity. As cars become increasingly networked, including through advances in automation and communication technologies, companies and regulators alike should make the protection of consumers' data a top priority.

Consumers deserve to know what data their car is collecting and transmitting, and who has access to this information. They should be able to trust that companies are legally obligated to protect their privacy and the security of their data. This trust is important not just for consumers themselves, but also for the broader acceptance and successful deployment of advanced features—including lifesaving safety systems—across the marketplace.

Accordingly, Consumers Union supports requiring vehicle manufacturers and suppliers to meet baseline, enforceable standards to protect consumer privacy and data security, which are too important to be left to voluntary measures alone. These standards should, at a minimum, involve mandatory adherence to the Fair Information Practice Principles (FIPPs). As they develop the standards, we urge the FTC and NHTSA to work together, as well as with Congress and other federal agencies, to ensure that consumers have transparency, meaningful choice, control, and security with regard to personal data of theirs associated with a motor vehicle.

---

[1] Consumers Union is the policy and mobilization arm of Consumer Reports, an independent, nonprofit organization that works side by side with consumers to create a fairer, safer, and healthier world. As the world's largest independent product-testing organization, Consumer Reports uses its more than 50 labs, auto test center, and survey research center to rate thousands of products and services annually. Founded in 1936, Consumer Reports has over 7 million subscribers to its magazine, website, and other publications.

In previous submissions to NHTSA, Consumers Union has offered various comments on how the agency should address issues related to consumer privacy and data security. As we have noted, today's cars have upward of 70 to 100 electronic control units, and potentially contain as many as 100 million lines of software code—significantly more than a new passenger airplane.[2] These cars include several mechanisms through which they can collect substantial information about consumers and potentially compromise their privacy. We have urged NHTSA to work with the FTC and other stakeholders to meaningfully address issues such as de-identification and data minimization, and have encouraged limits on the retention of consumers' personal information.[3]

In addition, today's cars can have major security vulnerabilities just as a computer or a mobile device can, but unlike many connected products, a breach of safety-critical vehicle systems comes with serious risks that can be associated with life-or-death consequences.[4] Appropriately, NHTSA has recognized the protection of data security as a critical element of motor vehicle safety, including as a part of its September 2016 automated vehicles guidance and its December 2016 notice of proposed rulemaking for a safety standard related to vehicle-to-vehicle (V2V) communications.[5] For example, specific to the agency's proposed rule on V2V, the agency demonstrated that it is on the right track by recognizing that security requirements should be included in regulatory text, by proposing the use of at least 128-bit encryption, and by pledging additional research on the security of message authentication. While we have urged and continue to urge NHTSA to develop a mandatory safety standard for data security, we

---

[2] Government Accountability Office, "Vehicle Cybersecurity: DOT and Industry Have Efforts Under Way, but DOT Needs to Define Its Role in Responding to a Real-World Attack" at 7-8 (Mar. 2016) (online at www.gao.gov/assets/680/676064.pdf).

[3] We also urged the agency to base its views of appropriate privacy protection, as well as the definition of "personal data," on stronger measures than the White House Consumer Privacy Bill of Rights. We have serious concerns with this proposal, including that it: (1) does not adequately define what constitutes sensitive information, or provide consumers with meaningful choices about their data; (2) does not explicitly protect large categories of personal information, such as geolocation data, business records, and data "generally available to the public"; (3) gives companies broad leeway to determine the protections that consumers will receive; and (4) generally offers protections to consumers only if a company identifies a risk of harm, according to its own judgment. *See* Consumers Union, "Consumers Union statement on White House discussion draft of Consumer Privacy Bill of Rights Act" (Feb. 27, 2016) (online at consumersunion.org/news/consumers-union-statement-on-white-house-discussion-draft-of-consumer-privacy-bill-of-rights-act); Letter from 14 consumer and privacy advocates to President Barack Obama (Mar. 2, 2016) (online at consumerfed.org/pdfs/150302_consumerprivacyPresident_letter.pdf).

[4] *See, e.g.,* Government Accountability Office, "Vehicle Cybersecurity: DOT and Industry Have Efforts Under Way, but DOT Needs to Define Its Role in Responding to a Real-World Attack" at 12-19 (Mar. 2016) (online at www.gao.gov/assets/680/676064.pdf)*;* Federal Bureau of Investigation, Department of Transportation, and NHTSA, "Motor Vehicles Increasingly Vulnerable to Remote Exploits" (Mar. 17, 2016) (online at www.ic3.gov/media/2016/160317.aspx); Staff of U.S. Sen. Edward J. Markey, *Tracking & Hacking: Security and Privacy Gaps Put American Drivers at Risk* (Feb. 9, 2015) (online at www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf).; "One in Five Vehicle Vulnerabilities are 'Hair on Fire' Critical," Security Ledger (Aug. 11, 2016) (online at securityledger.com/2016/08/one-in-five-vehicle-vulnerabilities-are-hair-on-fire-critical).

[5] *See* Comments of Consumer Reports and Consumers Union to the National Highway Traffic Safety Administration on the Federal Automated Vehicles Policy (Nov. 22, 2016) (online at www.regulations.gov/document?D=NHTSA-2016-0090-1069); Comments of Consumers Union to the National Highway Traffic Safety Administration on the Notice of Proposed Rulemaking: Federal Motor Vehicle Safety Standards; V2V Communications (Apr. 12, 2017) (online at www.regulations.gov/document?D=NHTSA-2016-0126-0463).

nevertheless appreciate the agency's other work to ensure that companies put the safety and security of consumers first. The agency should be supported in this endeavor by Congress, which should provide NHTSA with adequate resources to carry out its important work and pass clarifying legislation, if needed, to confirm the agency's authority.[6]

We also appreciate NHTSA's work to complete guidelines outlining best practices for data security, which it released in October 2016. In our comments on these best practices, we agreed with most of the agency's recommendations for companies, and suggested certain enhancements in the interest of bolstering the document. Specifically, we asked that NHTSA, among other things:

- Require rigorous and independent third-party auditing in addition to companies' self-audits, to ensure that a car's systems are evaluated by entities without a financial self-interest in the conclusion;

- Ensure that security researchers have broad access to incident and risk data, so that experts that may have a perspective and expertise that a company lacks can serve as an important resource for identifying and addressing security risks;

- Continue encouraging information sharing among companies, and take all necessary steps to ensure that it receives the information it needs to reliably assess the safety of a vehicle with regard to potential security issues;

- Apply the best practices to all individuals and organizations manufacturing and designing vehicle systems and software as planned, not just motor vehicle and equipment manufacturers;

- Maintain its support for the layered approach to data security that it outlined in the best practices, and require the company documentation it had recommended; and

- Account for aftermarket devices designed to improve vehicle data security.

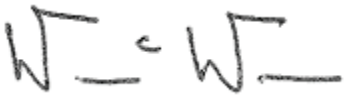
In conclusion, the work of the FTC and NHTSA is highly important toward ensuring that consumers have transparency, meaningful choice, control, and security with regard to their personal data associated with a motor vehicle. However, additional steps should be taken to ensure that consumers are protected in their cars, and that regulators receive the information and resources they need to adequately oversee companies and protect safety, security, and privacy on

---

[6] *See* "Short-staffed NHTSA struggles to handle car-hacking threats," AutoBlog (Oct. 2, 2015) (online at www.autoblog.com/2015/10/02/short-staffed-nhtsa-struggles-to-handle-car-hacking-threats); *see also, e.g.,* Sen. Edward J. Markey and Sen. Richard Blumenthal, "Sens. Markey, Blumenthal Introduce Legislation to Protect Drivers from Auto Security, Privacy Risks with Standards & 'Cyber Dashboard' Rating System," press release (July 21, 2015) (online at www.markey.senate.gov/news/press-releases/sens-markey-blumenthal-introduce-legislation-to-protect-drivers-from-auto-security-privacy-risks-with-standards-and-cyber-dashboard-rating-system).

the roads. We appreciate the agencies' attention to these issues, and look forward to the workshop on June 28.[7]

Respectfully submitted,



William C. Wallace
Policy Analyst
Consumers Union

[7] *See* Comments of Consumer Reports and Consumers Union to the National Highway Traffic Safety Administration on the Request for Comment on Cybersecurity Best Practices for Modern Vehicles (Nov. 28, 2016) (online at www.regulations.gov/document?D=NHTSA-2016-0104-0995).