

BEFORE THE
NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION
Washington, DC 20590

In the Matter of)
Advance Notice of Proposed Rulemaking)
Regarding Federal Motor Vehicle Safety)
Standards: Vehicle-to-Vehicle (V2V)) Docket No. NHTSA-2014-0022
Communications Pursuant to Chapter)
301 of the Department of Transportation,)
Motor Vehicles and Driver Programs)

TO: The National Highway Traffic Safety Administration

Comment of the Federal Trade Commission

In its Advanced Notice of Proposed Rulemaking (“ANPRM”)¹ and accompanying report (“V2V Report”)² filed August 18, 2014, the National Highway Traffic Safety Administration (“NHTSA”) announced its intention to promulgate a rule that would (1) require vehicle-to-vehicle (“V2V”) communication capability for passenger cars and light truck vehicles by 2019 and (2) create minimum performance requirements for V2V devices and messages. As NHTSA has explained, the purpose of the V2V communications system is to enable devices on vehicles to transmit certain information such as the vehicle’s speed and bearing to surrounding vehicles. This information would then be processed and used to generate safety warnings for drivers.

¹ Federal Motor Vehicle Safety Standards: Vehicle-to-Vehicle (V2V) Communications, 79 Fed. Reg. 49,270 (ANPRM Aug. 20, 2014).

² Nat’l Highway Traffic Safety Admin., Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application (2014) (“V2V Report”), available at <http://www.nhtsa.gov/staticfiles/rulemaking/pdf/V2V/Readiness-of-V2V-Technology-for-Application-812014.pdf>.

NHTSA, as the agency charged with promoting vehicle safety, plans to mandate the inclusion of this V2V technology in future new cars at the conclusion of this process.

Among other issues, NHTSA asked for comment related to privacy and security issues raised in the V2V Report and the ANPRM. As the primary federal agency with authority over consumer privacy and data security, the Federal Trade Commission (“FTC” or “Commission”) appreciates the opportunity to provide comments limited to those issues.

I. FTC AUTHORITY AND ACTIVITY IN THE PRIVACY AND DATA SECURITY AREA

The FTC has served as the primary federal agency charged with protecting consumer privacy, dating back to the 1970 enactment of the Fair Credit Reporting Act (“FCRA”). The FTC has been the primary enforcer of this law, which protects sensitive data used for credit, employment, insurance, and other decisions from disclosure to unauthorized persons.

Beginning in the mid-1990s, with the development of the Internet as a commercial medium, the FTC expanded its focus on privacy to reflect the growing collection, use, and sharing of consumer data in the commercial marketplace. Since then, the Commission’s primary source of legal authority in the privacy area has been Section 5 of the FTC Act,³ which empowers the Commission to take action against deceptive or unfair commercial practices.⁴

To date, the FTC has brought more than fifty cases against businesses that allegedly failed to maintain reasonable security. The FTC has begun to address security of connected devices. Earlier this year, the Commission finalized an enforcement action and consent order against TRENDnet, a manufacturer of Internet-connected cameras that, we alleged, failed to

³ 15 U.S.C. § 45.

⁴ The Commission also enforces sector-specific statutes containing privacy and data security provisions, such as the Gramm-Leach-Bliley Act (“GLB Act”), Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 and 15 U.S.C.), and the Children’s Online Privacy Protection Act (“COPPA”), 15 U.S.C. §§ 6501-6506.

maintain reasonable security, in violation of Section 5 of the FTC Act.⁵ Among other things, the FTC charged TRENDnet with failing to test its products appropriately, resulting in hackers being able to post private video feeds of people's bedrooms and children's rooms on the Internet. The Commission's consent order requires TRENDnet to implement a comprehensive security program, obtain independent assessments of the program, and provide toll-free customer support to existing users.

The FTC has also brought numerous cases alleging privacy-related violations against social networking companies,⁶ mobile app developers,⁷ and companies that provide Internet-related services,⁸ among others. One recent example is the Commission's case against the mobile messaging service Snapchat, which the FTC alleged violated the FTC Act's prohibition against deceptive practices by representing to consumers that their text messages would disappear after a set period of time.

In addition to enforcing the law, 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. On the policy front, the Commission regularly holds seminars and workshops to examine the implications of new technologies and business models on consumer privacy. These workshops have addressed key trends in today's changing technology landscape

⁵ TRENDnet, Inc., No. C-4426 (F.T.C. Jan. 16, 2014) (final decision and order), *available at* <http://www.ftc.gov/system/files/documents/cases/140207trendnetdo.pdf>.

⁶ Facebook, Inc., No. C-4365 (F.T.C. Aug. 10, 2012) (final decision and order), *available at* <http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf>.

⁷ Snapchat, Inc., File No. 132-3078 (F.T.C. May 14, 2014) (proposed consent agreement), *available at* <http://www.ftc.gov/system/files/documents/cases/140508snapchatorder.pdf>; *United States v. Path, Inc.*, No. 3:13-cv-00448-RS (N.D. Cal. Feb. 8, 2013) (consent), *available at* <http://www.ftc.gov/sites/default/files/documents/cases/2013/02/130201pathincdo.pdf>.

⁸ Google, Inc., No. C-4336 (F.T.C. Oct. 13, 2011) (final decision and order), *available at* <http://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzdo.pdf>.

and their impact on consumer data, including topics such as Big Data,⁹ mobile technology,¹⁰ and the Internet of Things.¹¹

II. CONNECTED VEHICLES AND V2V TECHNOLOGY

At its Internet of Things workshop in November 2013, the Commission specifically examined privacy and security issues relating to the different technologies involved with connected cars, including Event Data Recorders (“EDRs”) and other vehicle telematics.¹² Workshop participants described the many safety and convenience benefits that connected cars offer. For example, one participant pointed to beneficial uses such as detecting (and automatically correcting) skidding; providing navigation, weather, and traffic information; alerting first responders when airbags are deployed; and allowing consumers to control aspects of the vehicle’s functionality through their smartphone.¹³ At the same time, participants described three general types of potential privacy and security risks arising from this connectivity.

First, participants expressed concern about the ability of connected car technology to track consumers’ precise geolocation over time. Such information may divulge personal details

⁹ Fed. Trade Comm’n Workshop, *Big Data: A Tool for Inclusion or Exclusion?* (Sept. 19, 2014), available at <http://www.ftc.gov/news-events/events-calendar/2014/09/big-data-tool-inclusion-or-exclusion>.

¹⁰ Fed. Trade Comm’n Workshop, *In Short: Advertising and Privacy Disclosures in a Digital World* (May 30, 2012), available at <http://www.ftc.gov/news-events/press-releases/2012/05/ftc-announces-final-agenda-panelists-workshop-about-advertising>; Spring Privacy Series, *Mobile Device Tracking* (Feb. 19, 2014), available at <http://www.ftc.gov/news-events/events-calendar/2014/02/spring-privacy-series-mobile-device-tracking>.

¹¹ Fed. Trade Comm’n Workshop, *Internet of Things: Privacy & Security in a Connected World* (Nov. 19, 2013), available at <http://www.ftc.gov/bcp/workshops/internet-of-things>.

¹² *Id.* 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-things-privacy-security-connected-world/final_transcript.pdf.

¹³ Comment of Consumer Electronics Ass’n, #484 cmt. #00027 at 13, available at <http://www.ftc.gov/policy/public-comments/initiative-484>. Additional comments submitted after the workshop are available at <http://www.ftc.gov/policy/public-comments/initiative-510>.

about an individual.¹⁴ Did Consumer A visit an AIDS clinic last Tuesday? What place of worship does he attend? Was he at a psychiatrist's office last week? Did he meet with a prospective business customer? By collecting geolocation information from motor vehicles, businesses could build profiles of a driver's activities over time and use the information for purposes unanticipated by the driver. For example, a business could sell the information to a data broker, which might, in turn, tag the consumer with reference to his medical conditions and sell it to other businesses. Indeed, many consumers are concerned about the privacy of their geolocation data. One recent study found that nearly three quarters of consumers surveyed were reluctant to enable location tracking on their phones due to privacy concerns.¹⁵ Consistent with this generalized concern about geolocation data, NHTSA's own survey discussed in the V2V Report reflects consumer discomfort about businesses having access to additional driving-related geolocation information.¹⁶

Second, FTC workshop participants expressed a concern 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. This kind of collection can fall outside the FCRA, which

¹⁴ See, e.g., *The Location Privacy Protection Act of 2014: Hearing on S. 2171 Before the Subcomm. for Privacy, Tech. and the Law of the S. Comm. on the Judiciary*, 113th Cong. (2014) (Statement of the Fed. Trade Comm'n) available at http://www.ftc.gov/system/files/documents/public_statements/313671/140604locationprivacyact.pdf.

¹⁵ TRUSTe, *2014 U.S. Consumer Confidence Privacy Report* (Jan. 28, 2014), available at http://www.truste.com/about-TRUSTe/press-room/news_us_truste_reveals_consumers_more_concerned_about_data_collection; see also NielsenWire, *Privacy Please! U.S. Smartphone App Users Concerned with Privacy When It Comes to Location* (Apr. 21, 2011), available at <http://www.nielsen.com/us/en/newswire/2011/privacy-please-u-s-smartphone-app-users-concerned-with-privacy-when-it-comes-to-location.html> (finding a majority of smartphone app users worry about their privacy when it comes to sharing their location through a mobile device). But see Matt Patronzio, *The 10 Most Popular Smartphone Apps in the U.S.* (April 3, 2014), available at <http://mashable.com/2014/04/03/popular-apps-chart/> (of the ten most popular mobile device apps downloaded, two are apps that use geolocation for mapping.)

¹⁶ See generally V2V Report, *supra* note 2 at 144-157.

generally governs data supplied by and furnished to credit reporting agencies for certain eligibility decisions.¹⁷

A third concern relates to the security of connected cars. At the Commission's Internet of Things workshop, one participant discussed his successful efforts to remotely access a car's internal computer network; he reported that he was able to control the vehicle's brakes and other critical functionality by hacking into the telematics unit.¹⁸

Although FTC workshop participants did not directly address V2V communications, many of the same questions and concerns apply: Who has access to the data, and for what purpose? What type(s) of information is collected? How long is the data stored, and with whom is it shared? What are the benefits of collecting and using the information? What security measures are in place to protect the data? What are the risks if the data is not reasonably secured?

III. THE V2V REPORT AND ANPRM

The Commission commends NHTSA's ANPRM and the V2V Report for taking into account the privacy and security concerns discussed above. In particular, the FTC highlights three elements of the proposal that appear designed to address these concerns.

First, the Commission supports NHTSA's implementation of a deliberative, process-based approach to address privacy and security risks. It appears that NHTSA has collaborated with numerous stakeholders to undertake a thorough privacy risk assessment. This risk assessment included a multi-step process of evaluating the needs served by V2V technology,

¹⁷ Scott R. Peppet, *Regulating the Internet of Things: First Steps Towards Managing Discrimination, Privacy, Security & Consent* (forthcoming TEX. L. REV. 2014) (manuscript at 17-20), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2409074&download=yes.

¹⁸ Remarks of Professor Tadayoshi Kohno, Transcript of Internet of Things Workshop at 245-47.

identifying system functions to serve those needs, identifying the data that must be collected to serve the needs, describing and quantifying privacy risks, and identifying ways to control these risks. It also appears that NHTSA is prepared to ensure that the V2V system will contain multiple technical, physical, and organizational controls to minimize privacy risks, including the likelihood of vehicle tracking by commercial entities. The Commission appreciates NHTSA's explanation of the substantial steps it took as part of its interim privacy impact assessment, and looks forward to reviewing the results of the final assessment.

Second, the Commission commends NHTSA for designing the V2V system in a way that limits the amount of data collected and stored to that which serves its intended safety purposes.

In particular, NHTSA makes clear that

the system will not collect or store any data on individuals or individual vehicles, nor will it enable the government to do so. There is no data in the safety messages exchanged by vehicles or collected by the V2V security system that could be used by law enforcement or private entities to personally identify a speeding or erratic driver. The system—operated by private entities—will not permit tracking through space or time of vehicles linked to specific owners or drivers or persons. Third parties attempting to use the system to track a vehicle would find it extremely difficult to do so, particularly in light of far simpler and cheaper means available for that purpose. The system will not collect financial information, personal communications, or other information linked to individuals. It will enroll V2V enabled vehicles automatically, without collecting any information identifying specific vehicles or owners. The system will not provide a “pipe” into the vehicle for extracting data. The system will enable NHTSA and motor vehicle manufacturers to find lots or production runs of potentially defective V2V equipment without use of VIN numbers or other information that could identify specific drivers or vehicles.¹⁹

In addition, the V2V Report indicates that the system design will ensure that no one party can match records to re-identify a particular individual or vehicle.²⁰ Such data collection

¹⁹ V2V Report, *supra* note 2, at 144. The report indicates that, while there will be, “on a very limited basis, some V2V data linking V2V device production lots to security credentials,” it explains that “neither the V2V system nor NHTSA will collect, store or have access to information that links production lots of defective V2V devices with specific VINs or owners.” *Id.* at 146.

²⁰ *Id.* at 176.

limitations, which should include both technical and administrative safeguards to help ensure against re-identification, are key in addressing consumer concerns about possible third-party sharing and other secondary uses.²¹

Third, NHTSA's attention to potential security issues is equally thorough and demonstrates a clear commitment to creating both a functional and secure communications system based on research efforts over more than a decade.²² The Commission agrees that "public acceptance and the adoption of cooperative V2V safety applications will depend on appropriate levels of security as an integral part of the system."²³ In particular, the Commission supports the choice not to connect the V2V device to other onboard computers in a way that would permit hackers to access those computers through vulnerabilities in the device. The Commission also applauds the additional work that NHTSA plans to do with respect to the system's security, which includes obtaining an independent assessment of the proposed system's security controls.²⁴

IV. CONCLUSION

The Commission supports NHTSA's commitment to the principle that any regulation of V2V technologies should "both protect[] individual privacy and promote[] this important safety technology"²⁵ and be rooted in the framework of the Fair Information Practice Principles.²⁶ The

²¹ See generally FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 21-22 (2012), available at <http://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policy-makers> (explaining that companies should employ both technical and administrative measures to help ensure that data is de-identified and is not subsequently re-identified).

²² *Id.* at 158, 177-79.

²³ *Id.* at 158.

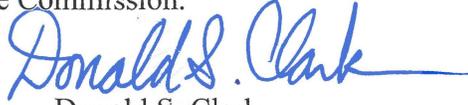
²⁴ *Id.* at 189 (Research Need IX-2-33).

²⁵ *Id.* at 147.

²⁶ *Id.* at 148-150.

Commission appreciates the opportunity to provide comments on the ANPRM and accompanying V2V Report, which reflect NHTSA's close attention to the privacy and security implications of V2V technologies.

By Direction of the Federal Trade Commission.



Donald S. Clark
Secretary
October 20, 2014