COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION

Federal Motor Vehicle Safety Standards:
"Vehicle-to-Vehicle (V2V) Communications"

49 C.F.R. Part 571
Docket No. NHTSA-2014-0022
RIN 2127-AL55

October 20, 2014

By notice published on August 20, 2014, the National Highway Traffic Safety Administration ("NHTSA") proposed to create a new Federal Motor Vehicle Safety Standard ("FMVSS") requiring vehicle-to-vehicle ("V2V") communication capability for "light vehicles" including passenger cars and light truck vehicles.[1] Pursuant to NHTSA's advance notice of proposed rulemaking ("ANPRM"), the Electronic Privacy Information Center ("EPIC") hereby submits these comments and recommendations to address the substantial privacy risks posed by the agency's proposal.

EPIC acknowledges NHSTA's initial privacy assessment and commitment to publish a draft Privacy Impact Assessment ("PIA") in the future. However, both the ANPRM and the V2V Readiness Report fail to adequately assess the privacy and security implications arising from V2V communications technology. Therefore, NHTSA should complete a more detailed privacy and security assessment of V2V communications. Additionally, NHTSA should: (1) not collect PII without the express, written authorization of the vehicle owner; (2) ensure that no data will be stored either locally or remotely; (3) require end-to-end encryption of V2V communications, including the basic safety messages ("BSMs"); (4) require end-to-end anonymity; and (5) require auto manufacturers to adhere to the Consumer Privacy Bill of Rights.

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values.[2] EPIC is a leading advocate for consumer privacy and privacy enhancing techniques for emerging technology, like V2V technology and other devices comprising the "Internet of Things."[3] In 2013, EPIC submitted extensive comments to the Federal Trade Commission ("FTC") regarding the privacy and security implications of the Internet of Things.[4] EPIC recommended that the FTC require

---

[1] Federal Motor Vehicle Safety Standards: Vehicle-to-Vehicle (V2V) Communications, 79 Fed. Reg. 49,270 (proposed Aug. 20, 2014) (to be codified at 49 C.F.R. pt. 571) [hereinafter FMVSS: V2V Communications].
[2] *About EPIC*, EPIC, http://epic.org/epic/about.html.
[3] *See*, *e.g.*, EPIC, *Consumer Privacy*, http://epic.org/privacy/consumer/; EPIC, *Big Data and the Future of Privacy,* https://www.epic.org/privacy/big-data/; EPIC, *Internet of Things (IoT),* http://epic.org/privacy/internet/iot/default.html.
[4] EPIC, *Comments on the Privacy and Security Implications of the Internet of Things* (June 1, 2013), *available at* http://epic.org/privacy/ftc/EPIC-FTC-IoT-Cmts.pdf.

companies to adopt privacy enhancing techniques, respect a consumer's choice not to be tracked, profiled, or monitored, minimize data collection, and ensure transparency in both design and operation of Internet-connected devices.[5]

Additionally, EPIC has routinely submitted comments to NHTSA regarding the privacy risks inherent in Event Data Recorders (EDRs).[6] As with EDRs, the deployment of V2V technology raises significant privacy considerations.

I. NHTSA Mandates Threaten Driver Privacy

In 2003, NHTSA began a process that led to the deployment of more EDRs in U.S. motor vehicles. In that year, NHTSA solicited public comments on the "safety benefits, technical issues, and privacy issues" arising from EDRs.[7] EPIC filed comments pointing out the privacy implications of EDRs.[8] EPIC recommended that the collection of driving-related data follow Fair Information Practices, including ensuring an opt-in system where drivers must unambiguously consent to the collection of such information.[9] EPIC also recommended that any databases constructed with driver data comply with the Privacy Act of 1974.[10] This could be accomplished by constructing the EDR database to preserve the privacy of drivers so that only aggregate information is collected.[11]

In June 2004, NHTSA issued a Notice of Proposed Rulemaking that would: (1) require that EDRs that had been voluntarily installed record "a minimum set of specified data elements," (2) standardize the date format in EDRs, and (3) require automobile manufacturers to make EDR crash data publicly available.[12] In response, EPIC filed another comment with NHTSA highlighting that EDRs present serious privacy issues that had developed incrementally over time. EPIC recommended that NHTSA incorporate Fair Information Practices, which the proposed rule had only incorporated one of the practices.[13] EPIC recommended that the proposed rule be amended to protect the privacy of vehicle owners and drivers.[14] Among other recommendations, EPIC stated that the vehicle owner should be explicitly recognized as the owner of EDR data, that consent should be required for any disclosure of EDR data, and that vehicle identification number should only be partially collected to exclude the personal identifier portion.[15]

---

[5] *Id*.
[6] EPIC, *Automobile Event Data Recorders (Black Boxes) and Privacy*, http://epic.org/privacy/edrs/.
[7] National Highway Traffic Safety Administration: Event Data Recorders, 67 Fed. Reg. 63,493, 63,494 (proposed Oct. 11, 2002).
[8] EPIC, *Comments on the Development and Installation of Event Data Recorders (EDRs) in Motor Vehicles, Docket No. NHTSA-2002-13546* (Feb. 28, 2003), *available at* http://epic.org/privacy/drivers/edr_comments.pdf.
[9] *Id.* at 1.
[10] *Id.*
[11] *Id.*
[12] National Highway Traffic Safety Administration: Event Data Recorders, 69 Fed. Reg. 32,932 (proposed June 14, 2004) (to be codified at 49 C.F.R. pt. 563).
[13] *Id.*
[14] *Id.*
[15] *Id.*

Most recently, in February 2013, EPIC, along with members of privacy, consumer rights, civil rights organizations, and members of the general public ["hereinafter Privacy Commentators"], submitted privacy recommendations regarding NHTSA requiring the installation of EDRs in passenger vehicles. [16]

The comments highlighted that auto manufacturers collect large volumes of EDR data. For example, EDRs may record "(1) pre-crash vehicle dynamics and system status, (2) driver inputs, (3) vehicle crash signature, (4) restraint usage/deployment status, and (5) post-crash data such as the activation of an automatic collision notification system."[17] The comments also noted that NHTSA planned to expand EDR capabilities and data usage, citing a *January 2013 Significant Rulemaking Report of the USDOT* that referenced a pending rulemaking to expand data collection.[18] The pending rulemaking "would expand the utility of the amount and type of data Event Data Recorders (EDRs) capture in light vehicles in the event of a crash."[19] Additionally, the "rulemaking would make revisions to the optional data elements to account for the latest advances in vehicle safety."[20] Although NHTSA currently only requires a limited scope of data from EDRs, the Privacy Commentators urged NHTSA to restrict the type of data that will be required pursuant the 2014 mandate. The comments also explained how the market for and amount of EDR data collected has expanded, thereby increasing third party access to EDR data.

The Privacy Commentators recommended that NHTSA: (1) explicitly restrict the amount of data that EDRs collect; (2) conduct a comprehensive privacy impact assessment before mandating EDR installation; (3) uphold Privacy Act protections and grant vehicle owners and operators control over their data; (4) require security standards to maintain the integrity of EDR data; and (5) establish best practices to fully protect the privacy rights of vehicle owners and operators.[21]

Compiled from state laws limiting the use of EDR data, the EDR best practices affirmatively protect consumers[22] and treat EDR data as "private," "exclusively owned by the owner of the motor vehicle," and "not [to] be retrieved or used by another person or entity" without driver consent or a court order.[23] Taken together, these laws create a substantive basis for EDR data collection best practices.

NHTSA's new V2V proposal raises many of the same privacy risks associated with EDRs, as well as new privacy issues. NHTSA must adequately safeguard driver privacy before mandating V2V technology.

---

[16] EPIC et al., *Comments on Federal Motor Vehicle Safety Standards; Event Data Recorders, Docket No. NHTSA-2012-0177* (Feb. 11, 2013), *available at* http://epic.org/apa/comments/EPIC-Coalition-NHTSA-EDR-comments-FINAL-1.pdf.

[17] *Id* at 2; *Welcome to the NHTSA Event Data Recorder Research Web site*, NAT'L HIGHWAY TRAFFIC SAFETY ADMIN, http://www.nhtsa.gov/Research/Event+Data+Recorder+%28EDR%29/Welcome+to+the+NHTSA+Event+Data+Recorder+Research+Web+site.

[18] *Id*.

[19] *Id*.

[20] *Id*.

[21] *Id.* at 2.

[22] *Id.* at 5; *See*, *e.g*., Wash. Rev. Code Ann. § 46.35.050 ("The legislature finds that the practices covered by this chapter are matters vitally affecting the public interest . . . . A violation of this chapter is not reasonable in relation to the development and preservation of business and is an unfair or deceptive act in trade or commerce and an unfair method of competition . . ." *See also* N.H. Rev. Stat. Ann. § 357-G:1 (VI) ("Violations of this section shall constitute an unfair or deceptive act or practice" under New Hampshire state law).

[23] *Id.*; *See*, *e.g*., Ark. Code Ann. § 23-112-107 (West).

II. Deployment of V2V Technology Presents Substantial Privacy and Security Risks

V2V technology allows vehicles to "access, consume, create, enrich, direct, and share digital information between businesses, people, organization, infrastructures, and things."[24] V2V technology is one example of Internet of Things ("IoT") as connectivity. The IoT is an ever-expanding network of devices capable of connecting to other devices and people through the existing Internet infrastructure.[25] These devices connect and communicate in many ways.[26] Law professor Frank Pasquale notes that the IoT "sets the stage for extraordinarily targeted monitoring and manipulation [of individuals]." [27] Professor Pasquale also notes that the IoT "will be a tool for other people to keep tabs on what the populace is doing."[28] Law professor Jerry Kang coauthored an article and case study on pervasive computing, which is a past term to refer to the Internet of Things.[29] In his article, Professor Kang calls for there to be a federal statutory law that requires that any information collected from the IoT should only be used if "functionally necessary" to the transaction at hand, and that no other data or distribution should be allowed, including advertising.[30]

Some car manufacturers already collect data about their vehicles remotely through centralized servers. Famously, Jim Farley, global vice president in Ford's marketing and sales division, admitted that the company is already collecting copious amounts of data.[31] "We know everyone who breaks the law; we know when you're doing it. We have GPS in your car, so we know what you're doing," Farley boasted to crowds at the Consumer Electronics Show.[32] This tremendous collection of data and broadcast of messages from vehicles puts consumers at risk of private information falling into the hands of third parties or law enforcement.

NHTSA states that mandating V2V capability is required, as "no single manufacturer would have the incentive to build vehicles able to 'talk' to other vehicles."[33] NHTSA believes that mandating the communication capability, but not requiring particular safety applications, will "facilitate market-driven development and introduction of a variety of safety applications, as well as mobility and environment-related applications."[34] While NHTSA states that the data will not be stored on individuals or individuals' vehicles and that the system "will not permit tracking through time or space of vehicles," it concedes that

---

[24] Thilo Koslowski, Forget the Internet of Things: Here Comes the 'Internet of Cars,' Wired (Jan. 4, 2013) http://www.wired.com/2013/01/forget-the-internet-of-things-here-comes-the-internet-of-cars/.
[25] EPIC, *Internet of Things (IoT)*, http://epic.org/privacy/internet/iot/.
[26] *Id.*
[27] PEW RESEARCH CENTER, *Digital Life in 2025: The Internet of Things will Thrive by 2025*, (May 14, 2014). http://www.pewinternet.org/files/2014/05/PIP_Internet-of-things_0514142.pdf.
[28] Tanya Roscorla, *6 Things to Expect from the Internet of Things by 2025*, GOVERNMENT TECHNOLOGY, May 14, 2014, *available at* http://www.govtech.com/internet/6-Things-to-Expect-from-the-Internet-of-Things-by-2025.html.
[29] Jerry Kang & Dana Cuff, *Pervasive Computing: Embedding the Public Sphere*, 62 Wash. & Lee L. Rev. 93, 134-35 (2005).
[30] *Id.* at 134-35.
[31] RUSSIA TIMES, *Ford VP: 'We have GPS in your care, so we know what you're doing,'* Jan. 9, 2014 *available at* http://rt.com/usa/ford-vp-auto-surveillance-382/.
[32] *Id.*
[33] FMVSS: V2V Communications, 79 Fed. Reg. at 49,270.
[34] *Id.*

it is possible for third parties to use the system to track vehicles, even though more difficult than other methods.[35] This ability to track vehicles raises substantial privacy risks to drivers.

NHTSA concedes that consumer privacy issues "are intertwined with consumer and industry acceptance of V2V technologies. For this reason, privacy considerations are critical to the analysis underlying NHTSA's decision about whether and, if so, how to proceed with V2V research or regulation."[36] The agency acknowledges that consumer privacy considerations are "inherent in mandated V2V technologies," and the agency poses a number of questions regarding these privacy issues.[37] The privacy issues include how to protect both the anonymity of drivers and V2V data, which privacy policy framework would best fit the case of V2V communications, how V2V communications are viewed in light of the fair information practices ("FIPs"), and what role the government should play in protecting individual privacy in connection with V2V communication.[38]

NHTSA also discusses the findings of its interim privacy risk assessment, finding that "a properly-designed V2V system would curtail any serious risks to privacy."[39] Even so, the agency acknowledges that it can never completely eliminate privacy risks.[40] NHTSA plans on performing a more comprehensive look at privacy risks and "welcomes privacy-related comments in response to the research report and [advance notice of proposed rulemaking]."[41]

III. Recommendations for Addressing the Privacy and Security Risks of V2V Technology

A. V2V Data Should Not Be Stored Either Locally or Remotely

Today's motor vehicles collect vast amounts of data including speed, timestamps of events, GPS location of vehicles, and internal mechanical failures.[42] The data that vehicles will share in dedicated short-range communications ("DSRC"), like those in V2V technology, allow vehicles to warn other vehicles of unsafe conditions via basic safety messages ("BSMs") that are broadcasted from the car. NHTSA's initial report states that BSMs "contain the relevant elements and describe them accurately (e.g., vehicle speed; GPS position; vehicle heading; DSRC message ID, etc)."[43]

There are two main types of BSMs that vehicles with V2V technology send: BSM Part I messages and BSM Part II messages. BSM Part I messages are broadcast more frequently than BSM Part II messages and contain information such as vehicle size, speed, vehicle position, heading, and brake

---

[35] *Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application,* NAT'L HIGHWAY TRAFFIC SAFETY ADMIN, http://www.nhtsa.gov/staticfiles/rulemaking/pdf/V2V/Readiness-of-V2V-Technology-for-Application-812014.pdf (hereinafter V2V Readiness Report).
[36] V2V Readiness Report at 144.
[37] *Id*.
[38] *Id.* at 144-50.
[39] *Id.* at 150-57.
[40] *Id.* at 157.
[41] FMVSS: V2V Communications, 79 Fed. Reg. at 49,273.
[42] Lucas Wang et al., *Data Naming in Vehicle-to-Vehicle Communications*, COMPUTER COMMUNICATIONS WORKSHOPS: 2012 IEEE CONFERENCE (Mar. 25, 2012), *available at* http://irl.cs.ucla.edu/data/files/papers/data-naming-v2v.pdf.
[43] V2V Readiness Report at 54.

system status.[44] These data sets will be standardized across vehicle models. BSM Part II messages are specific to the vehicle model and are only broadcasted when certain triggering events occur.[45] The information contained in BSM Part II broadcasts is much more sensitive that Part I, and includes information such as vehicle safety extensions, path history, current time and locational information, path trajectory, and vehicle identity.[46] The vehicle identity information that is attached to Part II BSMs is the most alarming. The "vehicle identity" information can include a "[d]escriptive name (DE) – typically only used for debugging", vehicle identification number ("VIN") string, owner code, temporary IDs, and the vehicle type.[47] Data of this kind alone, as well as in combination with information contained in Part I BSMs, would be valuable to third parties, such as law enforcement, insurance companies, and private vehicle owners involved in litigation.

NHTSA states in its initial report that the "system will not collect or store any data on individuals or individual vehicles [… and] the system will not collect and motor vehicles will not store the messages sent or received data sent/received by V2V devices."[48] Yet, the preliminary readiness report states that the system will collect and store data that helps recall defective V2V equipment.[49] This would require linking individual vehicles to the V2V system and the greater network in order to find defective equipment.

Additionally, manufacturers will have the ability to change base settings in the V2V technology installed in their vehicles. This threat to consumer privacy is one that automobile manufacturers are already engaging in, as evidenced admissions of automobile manufacturer representatives.[50] Deploying a mandatory V2V communications infrastructure without assuring that these types of breaches are either technologically impossible or legally punishable is irresponsible and misguided.

In light of the threats to consumer privacy and the valuable information that could be contained on V2V systems, EPIC recommends that the PIA and security assessment ensure that no data will be stored either locally or remotely. Even local data storage threatens personal privacy, especially if the consumer is unable to review and remove this data.

B. Basic Safety Messages Must Be Encrypted to Ensure Privacy of Vehicle Owners and Drivers

The V2V communication of BSMs requires that the message content be "trusted but not encrypted" due to the speed in which the messages must be sent.[51] While communications that contain

[44] V2V Readiness Report at 74.
[45] V2V Readiness Report at 75-76.
[46] V2V Readiness Report at 77-79.
[47] V2V Readiness Report at 78. It is unclear what the descriptive name, typically used for debugging, will include. It is also unclear who will create the name, the possible PII that could be in the name, and who will use the name for what purposes. EPIC has referenced the "descriptive name" as a possible personal identifier for two reasons: (1) it was included in the "vehicle identity" portion of Part II BSMs, which also include other forms of PII, and (2) it is an ambiguous term that could include more traditional PII in it, depending on who creates it and who has access to it for "debugging" purposes.
[48] V2V Readiness Report at 144-45.
[49] V2V Readiness Report at 147.
[50] Mike Masnick, *Ford VP Claims The Company Is Tracking Everyone's Driving Habits…Then Denies It*, TECHDIRT, Jan. 10, 2014, *available at* https://www.techdirt.com/articles/20140110/12395525837/ford-vp-claims-company-is-tracking-everyones-driving-habits-then-denies-it.shtml.
[51] V2V Readiness Report at 73.

certificates and other security information will be subject to asymmetric cryptography, the BSMs that are sent out to other vehicles to warn of pending danger will not. Since BSMs "exchange safety data regarding vehicle state," they are particularly sensitive messages and are ones in which third parties would want to intercept.[52]

The Vehicle Infrastructure Integration Consortium's ("VIIC") has created a Privacy Policies Framework to apply to innovative advances in vehicles, much like V2V communications technology. VIIC has made several suggestions that should be implemented to bolster V2V system security, and EPIC largely supports these recommendations. In addition to the VIIC Privacy Policy Framework, end-to-end encryption of communications, including the BSMs, should be implemented as they are considered vulnerable communications.[53] Vulnerable communications are any communications that could potentially cause harm to the consumer if intercepted or used by a third-party. In the case of V2V communication technology, this would mean use for anything other than use in the V2V system.

C. Basic Safety Messages Must Not Contain PII and Must Be Anonymous

NHTSA states that the BSM will not contain any personally identifying information ("PII"), however, in the same report, the list of information included in Part II BSMs includes PII like VIN string, owner code, and a descriptive name used for debugging.[54]

Anonymity for drivers, or at least the option of anonymity for mandatory services, is crucial for consumers and comports with Fair Information Practices and VIIC Privacy Policies Framework.[55] "End-to-end anonymity" should be mandated in all V2V systems.[56] No PII should be collected, unless with the express authorization of the vehicle owner through an opt-in, not opt-out, process.

D. Auto Manufactures Must Adhere to the Consumer Privacy Bill of Rights When Deploying V2V Technology

In 2012, President Obama set out a comprehensive framework for privacy protection– the Consumer Privacy Bill of Rights ("CPBR") – that provides substantive privacy protections for users.[57] The CPBR enumerates seven principles: Individual Control, Transparency, Respect for Context, Security, Access and Accuracy, Focused Collection, Accountability.[58] These principles are central to the right of privacy, and appear in numerous frameworks, such as the Organization for Economic Cooperation and Development ("OECD") Privacy Guidelines[59] and the Privacy Act of 1974.[60]

---

[52] V2V Readiness Report at 74.
[53] V2V Readiness Report at 146.
[54] V2V Readiness Report at 144.
[55] Mary Wroten, *VIIC Cooperative Research: Privacy & Security – 2012 Government & Industry Meeting*, VIIC CONSORTIUM, Jan. 25. 2012, *available at* http://www.sae.org/events/gim/presentations/2012/wroten_ford.pdf.
[56] V2V Readiness Report at 144.
[57] *See* EXEC. OFFICE OF THE PRESIDENT, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY (2012).
[58] *Id.* at 10.
[59] OECD, OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (1980), *available at* http://www.oecd.org/internet/interneteconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#part2.
[60] Privacy Act of 1974, 5 USC § 552a.

These CPBR would impose certain requirements on the collection and use of personal information in the digital network environment. For example, Individual Control and Respect for Context would require that individuals consent to new uses or disclosures of their information. And Transparency and Access and Control would require that users be able to access all of the data that companies--in this case, auto manufacturers--keep about them. The right to access increases drivers' control by placing the locus of ownership closer to the driver, who gains the ability to inspect V2V data and take steps to correct errors.

When deploying V2V technology, auto manufacturers must ensure that drivers may exercise all of the practices encompassed in the Consumer Privacy Bill of Rights.

Conclusion

The deployment of V2V technology presents substantial threats to the privacy and security of consumers. V2V technology allows vehicles to "access, consume, create, enrich, direct, and share digital information between businesses, people, organization, infrastructures, and things."[61] This tremendous collection of data and broadcast of messages from vehicles puts consumers at risk of private information falling into the hands of third parties or law enforcement. NHTSA itself concedes that consumer privacy issues "are intertwined with consumer and industry acceptance of V2V technologies. For this reason, privacy considerations are critical to the analysis underlying NHTSA's decision about whether and, if so, how to proceed with V2V research or regulation."[62]

NHTSA must complete a detailed privacy and security assessment of V2V communications. In addition to the assessment, NHTSA should ensure that mandated V2V technology comply with the following recommendations: (1) NHTSA should not collect PII without the express, written authorization of the vehicle owner; (2) NHTSA should ensure that no data will be stored either locally or remotely; (3) NHTSA should require end-to-end encryption of V2V communications, including the basic safety messages ("BSMs"); (4) NHTSA should require end-to-end anonymity; and (5) require auto manufacturers to adhere to the Consumer Privacy Bill of Rights.

Respectfully Submitted,

Marc Rotenberg, EPIC Executive Director
Khaliah Barnes, EPIC Administrative Law Counsel
Sara Bennett, EPIC Extern
Electronic Privacy Information Center
1718 Connecticut Ave. NW Suite 200
Washington, DC 20009
202-483-1140 (tel)
202-483-1248 (fax)

[61] Koslowski, Forget the Internet of Things: Here Comes the 'Internet of Cars,' *supra* note 30.
[62] V2V Readiness Report at 144.