epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION

Federal Motor Vehicle Safety Standards; V2V Communications

[Docket No. 2016-0126]

April 12, 2017

By notice published on January 12, 2017 the National Highway Traffic Safety Administration ("NHTSA") requested comment on a notice of proposed rulemaking ("NPRM") for a new Federal Motor Vehicle Safety Standard ("FMVSS") to mandate vehicle-to-vehicle ("V2V") communications in new light vehicles and to standardize the message and format of V2V transmissions.[1] Pursuant to this NPRM, the Electronic Privacy Information Center ("EPIC") hereby submits these comments and recommendations to address the privacy risks in the agency's proposal.

While NHTSA has taken steps to address some of the privacy concerns that arose in the advanced noticed of proposed rulemaking ("ANPRM"), privacy concerns still remain with regard to V2V communications. In the final rule, we urge NHTSA to 1) revise the definition of "reasonably linkable" and "as a practical matter linkable" to take into account changes in

[1] *Request for Comment on "Federal Motor Vehicle Safety Standards; V2V Communications,"* 82 Fed. Reg. 3854 (Jan. 12, 2017) (hereafter "NPRM").

technology that could allow for easier discovery of personal information 2) further detail NHTSA's relationship with the Security Certificate Management System ("SCMS") and how they envision protecting consumer data 3) allow consumers to "opt-out" of enabling V2V devices on their vehicles 4) ensure transparency for consumers about the data that is collected and how it is used and 5) to clarify that the NHTSA is not "occupying the field" of V2V communications and welcomes states to participate in shaping the development and use of these technologies.

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy and human rights related 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, such as V2V technology and other devise comprising the "Internet of Things."[3] EPIC has considerable expertise in the Internet of Things and other connected devices and has testified before Congress on connected vehicles and submitted numerous comments to various agencies concerning connected devices.[4] Additionally, EPIC has routinely submitted comments to NHTSA regarding the privacy risks inherent in Event Data Recorders and privacy considerations in for automated vehicles.

---

[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 Associate Director Khaliah Barnes, Testimony Before the U.S. House of Representatives, Committee on Oversight and Government Reform, Subcommittees on Information Technology and Transportation and Public Assets, *The Internet of Cars* (Nov. 18, 2015), https://epic.org/privacy/edrs/EPIC-Connected-Cars-Testimony- Nov-18-2015.pdf; EPIC Statement to the House Committee Subcommittee on Communications and technology, Feb. 2, 2017, https://epic.org/testimony/congress/EPIC-Statement-NTIA-02-02-2017.pdf; Comments to the NTIA "On the Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things," June 2, 2016, https://epic.org/apa/comments/EPIC-NTIA-on-IOT.pdf.

Revising the Definition of "Reasonably Linkable"

EPIC supports some of the changes that have been made to Basic Safety Messages ("BSM") since the ANPRM was published.[5] Specifically, we applaud the agency's decision not to include data elements that could link a specific vehicle to an individual. We urge the agency to adopt these changes in the final rule in order to protect consumer privacy. As the agency has stated, the ultimate goal of V2V technology is safety and consumers and their vehicles do not need to be identified to achieve that goal.

However, EPIC is disappointed with the agency's decision not to require that BSM messages are encrypted and again urges the agency to mandate encryption for BSM's.[6] Even with individual and vehicle identifying information removed from BSM's, safety messages are precisely the type of information that a nefarious third party may want to intercept and tamper with. While it is important that the agency has taken steps to identify messages that may have been tampered with,[7] it would be preferable to takes steps to minimize such tampering in the first place.

EPIC supports the steps taken to ensure that personally identifiable data is not used. This will protect both the safety and privacy of the individuals in the vehicle. The agency has stated that "V2V communications technology may not include data directly identifying a specific private vehicle or individual regularly associated with it, or data reasonably linkable or linkable, as a practical matter, to an individual." The agency further defines "reasonably linkable" and "as

[5] NPRM at 3904.
[6] *Privacy Impact Assessment: Notice of Proposed Rulemaking (NPRM) on V2V Communications,* Department of Transportation (hereinafter "PIA"); Comments of EPIC, *Federal Motor Vehicle Safety Standards: "Vehicle-to-Vehicle (V2V) Communications*, Oct. 20, 2014, https://epic.org/apa/comments/EPIC-NHTSA-V2V-Comments.pdf (hereinafter "ANPRM Comments").
[7] NPRM at 3912.

a practical matter linkable" to mean "capable of being used to identify a specific individual on a persistent basis without unreasonable cost or effort, in real time or retrospectively, given available resources."

In the final rule EPIC urges NHTSA to clarify this definition to make clear that any data that can now or in the future link a vehicle to an individual should not be used in any V2V communications technology. While the data that is currently contemplated to be used in BSM's may not currently link a vehicle to an individual, as technology changes data that cannot link an individual to a vehicle today may be able to do so in the future. The final rule should anticipate this problem.

Cybersecurity Risks of BSM Data

We applaud the agency's foresight in considering potential cybersecurity risks that could occur as V2V communications technology is implemented.[8] Currently, nearly all cars on the road today contain at least one wireless entry point ("WEP").[9] WEPs are essential to the functionality of built-in wireless features such as tire pressure monitoring systems, Bluetooth, keyless entry, anti-theft systems, and navigation.[10] However, WEPs also provide entry points for remote vehicle hacking. A 2011 report by computer scientists showed how a hacker could use WEPs to "take control of various features – like the car locks and brakes – as well as to track the vehicle's

[8] NPRM at 3916.
[9] *Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk*, Sen. Edward J. Markey (D-Mass) (Feb. 2015), https://www.markey.senate.gov/imo/media/doc/2015-02- 06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf [hereinafter "Markey Report"].
[10] *Id.* at 5.

location, eavesdrop on its cabin and steal vehicle data."[11] More recently, Chrysler was forced to recall 1.4 million cars after remote hacking of a jeep.[12]

The very real possibility of remote car hacking poses substantial risks to driver safety and security. Cars can be remotely hacked from anywhere in the world via the internet.[13] Wireless hacking can give hackers access to the cars physical location which would facilitate crimes such as harassment, stalking, and car theft.[14] Given that vehicles in their current state can already be remotely compromised, the agency is right to be concerned about cybersecurity risks in V2V communications. Furthermore, we support NHTSA's recognition of Fair Information Practices ("FIPs") in this context.

However, the NPRM and the Privacy Impact Assessment state that a private entity, that is not subject to federal record keeping or disposal regulations, will be responsible for receiving BSM data .[15] Although NHTSA will play a role developing policies and procedures for this entity, it is of concern that the entity will not be subject to the same standards of record keeping and privacy protections. We urge the agency to be as transparent as possible with the policies and procedures that are developed for this entity. Furthermore, we expect that this entity will track federal rules for record keeping and disposal of records and minimize the data that is collected and stored.

---

[11] John Markoff, *Researchers Show How a Car's Electronics Can Be Taken Over Remotely*, N.Y. Times (Mar. 9, 2011), http://www.nytimes.com/2011/03/10/business/10hack.html.
[12] NBC News, "Chrysler Recalls 1.4 Million Cars After Remote Hacking of Jeep," July 24, 2015, http://www.nbcnews.com/tech/tech-news/chrysler-recalls-1-4-million-cars-after-remote-hacking-jeep-n397851.
[13] Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway – With Me in It*, WIRED (July 21, 2015), https://www.wired.com/2015/07/hackers-remotelykill-jeep-highway/.
[14] *Id*.; *See also* Bruce Schneier, *The Internet of Things Will Turn Large-Scale Hacks Into Real World Disasters*, MOTHERBOARD, Jul. 25, 2016, https://motherboard.vice.com/read/the-internet-of-things-will-cause-the-first-ever-large-scale-internet-disaster.
[15] NPRM at 3916; PIA at 15-16.

EPIC has long argued that the best way to prevent loss or misuse of sensitive personal information is to avoid gathering or storing it in the first place.[16] Data that is not collected or retained cannot be subject to unauthorized access or disclosure. Minimizing stored user data reduces incentives for hackers to attack data storage systems by reducing the amount of data available to steal. This practice also reduces the costs of data breaches.

Strong privacy protections are also a necessary and pragmatic part of risk mitigation in the age of the ubiquitous cybersecurity breach. Failure to protect user privacy frequently stems from failure to adequately secure user data, which can result in enormous liability for companies.[17] The more data a company stores, the more valuable a target its database is for hackers; and the more stored data, the greater the company's losses in the event of a breach.[18]

Consumer Ability to Opt-In to V2V Communications

The NPRM describes V2V communications as a mandate to the automotive industry to fully implement V2V communications technology.[19] The NPRM acknowledges that despite NHTSA's best efforts to protect consumer privacy and minimize data collection and retention,

[16] *See, e.g.* Comments of EPIC, *Standards for Safeguarding Customer Information Request for Public Comment* (Nov. 7, 2016), https://epic.org/apa/comments/EPIC-FTC-Safeguards-Rule-Comments-11-07-2016.pdf; Reply Comments of EPIC, *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services* 11-12, WC Docket NO. 16-106 (July 6, 2016), https://epic.org/apa/comments/EPIC-FCC-Privacy-NPRM-Reply-Comments-07.06.16.pdf; Comments of EPIC, Request for Information: Big Data and the Future of Privacy (April 4, 2014), https://epic.org/privacy/big-data/EPIC-OSTP-Big-Data.pdf; Brief of Amicus Curiae Electronic Privacy Information Center in Support of Respondent, *City of Ontario v. Quon*, 560 U.S. 746 (2010), https://epic.org/privacy/quon/Quon_Brief_Draft_final.pdf.

[17] *2016 Cost of Data Breach Study: United States*, PONEMON INST., 1 (June 2016).

[18] Bruce Schneier, *Data Is A Toxic Asset*, SCHNEIER ON SECURITY, (March 4, 2016), https://www.schneier.com/blog/archives/2016/03/data_is_a_toxic.html ("saving [data] is dangerous because failing to secure it is damaging. It will reduce a company's profits, reduce its market share, hurt its stock price, cause it public embarrassment, and—in some cases—result in expensive lawsuits and occasionally, criminal charges. All this makes data a toxic asset, and it continues to be toxic as long as it sits in a company's computers and networks.").

[19] NPRM at 3855-6.

some consumers may still not feel as though their privacy is being adequately protected.[20] Consumers should always have a choice about what technologies they do or do not use, especially if their privacy is at risk. Consumers should not be forced to use technology that poses a risk to their safety or security. The mandated deployment of V2V communications technology leaves consumers with no meaningful choice. As a consequence, some consumers may keep aging cars that require expensive maintenance rather than buy cars with technology they do not want or cannot disable.

Consumers should be given the choice of whether or not they want V2V communications technology in their vehicles. Owners of these vehicles should be given the opportunity to opt-in to feature that are not mandated and have the ability to opt-out if it is mandated.

Consumer Access to Data

The NPRM addresses our earlier comments that advocate for consumer access to the data they generate.[21] However, the NPRM goes on to say that "in the context of a V2V system based on broadcast messages, the critical consumer privacy issue is not that of data ownership, but that of data access and use."[22] To facilitate this consumer knowledge, the agency provides a Privacy Statement that is to be placed in owners manuals and on manufacturer's websites.[23]

Generally, car manufacturers briefly inform consumers of data collection practices.[24] However, these notices fail to inform consumers about the true scope of data collection, and none give consumers true control over their data. Although some manufacturers allow consumers to delete already recorded data, preventing the car from constantly collecting and transmitting

[20] NPRM at 3921.
[21] EPIC ANPRM comments at 7-8.
[22] NPRM at 3926.
[23] NPRM at 3927.
[24] Markey Report at 12.

new data will often require "disabling valuable vehicle features or services."[25] In addition, car manufacturers use personal driving information for various but vague purposes, which leaves consumers in the dark about who has access to their information and why.[26] Personal driving information is often retained for years, if not indefinitely.[27]

The privacy statement provided in the NPRM does not go far enough in providing consumers access and control over the data that they generate. As the agency has previously noted, many consumers care deeply about privacy and for a new technology that presents unique privacy risks a privacy statement does provide adequate protections. This statement should be revised to provide that manufacturers will make available data that they have collected on V2V communications systems or provide reports or documentation about how that data is being used and make that information available to consumers. Providing this information will facilitate transparency as connected cars continue to be developed. As the agency has already noted, consumer trust is essential in ensuring the success of this new technology.[28] Transparency about the data being collected and how it is being used, not privacy statements buried in owners manuals and websites, will help foster this transparency.

State Involvement in V2V Communications Development

EPIC urges the agency to make clear in the final rule that states are not preempted from crafting their own privacy policies and regulations regarding V2V communications technologies. The Vehicle Safety Act preempts states from issuing any standard that regulates vehicle performance if the standard is not identical to an existing FMVSS that regulates that same aspect

[25] *Id.*
[26] *Id.* at 11.
[27] *Id.*
[28] NPRM at 3869.

of performance.[29] Historically, federal privacy laws have noy preempted stronger state law protections or enforcement mechanisms. In both the privacy and consumer protection context, federal regulations serve as baselines while allowing states to enact and enforce stronger laws.[30]

While the federal government has enacted privacy laws, more robust privacy legislation has been implemented at the state level. Many states have enacted privacy legislation that exists alongside federal law covering the same material. Furthermore, under *Hillsborough County v. Automated Medical Laboratories* there is currently a presumption that state and local governments are primarily responsible for matters related to health and safety.[31] Privacy is included in the area of health and safety regulations that are traditionally left to the states.[32]

For example, seventeen states have already passed laws regarding privacy aspects of connected cars as it relates to event data recorders ("EDRs").[33] EDRs are devices that can record, retain, and report data related to drivers' operation of an automobile. The data stored can also be accessed by third parties. Several states have limited when EDR data can be accessed or require the driver's consent. Virginia, for example, prohibits insurance companies from reducing coverage, increasing premiums, applying surcharges, or denying discounts solely because a

---

[29] "When a motor vehicle safety standard is in effect under this chapter, a State or a political subdivision of a State may prescribe or continue in effect a standard applicable to the same aspect of performance of a motor vehicle or motor vehicle equipment only if the standard is identical to the standard prescribed under this chapter." 49 U.S.C. § 30102(b)(1).

[30] *See e.g.* Electronic Communications Privacy Act; Right to Financial Privacy Act; Cable Communications Privacy Act; Video Privacy Protection Act; Employee Polygraph Protection Act; Telephone Consumer Protection Act; Driver's Privacy Protection Act; Gramm-Leach-Bliley Act.

[31] *Hillsborough County v. Automated Medical Laboratories*, 471 U.S. 707 (1985).

[32] *See e.g. Hill v. Colorado*, 530 U.S. 703 (2000) (upholding a law that protected the privacy and autonomy of individuals seeking medical care because the law was intended to serve the traditional exercise of State police power to protect the health and safety of its citizens).

[33] Ark. Code § 23-112-107; Cal. Veh. Code § 9951; Colo. Rev. Stat. § 12-6-401, -402, -403; Conn. Gen. Stat. § 14-164aa; Del. Code § 3918; Me. Rev. Stat. Ann. tit. 29-A §§ 1971, 1972, 1973; Mont. Code § 61-12-1001 et seq.; Nev. Rev. Stat. § 484D.485; N.H. Rev. Stat. § 357-G:1; N.J. Stat. § 39:10B-7 et seq.; N.Y. Veh. & Traf. Code § 416-b; N.D. Cent. Code § 51-07-28; Or. Rev. Stat. § 105.925 et seq.; Tex. Transp. Code § 547.615; Utah Code § 41-1a-1501 et seq.; Va. Code §§ 38.2-2212(C)(s), 38.2-2213.1, 46.2-1088.6, 46.2-1532.2; Wash. Rev. Code §46.35.010.

vehicle operator or owner refuses to grant her insurance company access to EDR data.[34] And Arkansas prohibits insurance companies from requiring EDR data access as a condition of an insurance policy.[35] Connecticut law requires law enforcement to obtain search warrants before accessing EDR data without owner consent.[36]

In addition, NHTSA would benefit from allowing states to play a role in crafting privacy regulations as V2V communications technology advances. States have a unique perspective allowing them to develop innovative programs to protect consumers. As V2V communications technology evolves, the states should be allowed to operate as laboratories of democracy – a role they have traditionally held in the field of privacy.[37] State legislatures are closer to their constituents and the entities that they regulate and are often the first to recognize trends and emerging problems, and are well suited to address new challenges and opportunities as they arise and as technology evolves.

Conclusion

EPIC supports the steps the agency has taken to protect privacy in V2V communications. However, the agency should make several further changes before finalizing the rule. It must be clear that privacy will be protected in BSM's no matter how technology changes and steps must be taken to protect privacy by both federal agencies and private entities involved in V2V communications. Consumers should retain the ability to opt-out of features they do not desire. The goal of improving safety on American roads should not come at the expense of consumer

[34] Va. Code Ann. § 38.2-2213.1 (West).
[35] Ark. Code Ann. §23-112-107 (West).
[36] Conn. Gen. Stat. Ann §14-164aa (West).
[37] *Hill v. Colorado,* 530 U.S. 703, 715 (2000) (upholding a law protecting the privacy and autonomy of individuals seeking medical care, as the law was intended to serve the "traditional exercise of the States' 'police powers to protect the health and safety of their citizens'").

choice and trust. Entities collecting storing data must be transparent with consumers about what data they have and how they are using it. Finally, as connected vehicle technology progresses, the states cannot be left out of the conversation and NHTSA should explicitly provide in this and any other FMVSS related to connected cars that states are welcome to craft their own privacy regulations.

Respectfully Submitted,

/s/ Marc Rotenberg
Marc Rotenberg
EPIC President

/s/ Kim Miller
Kim Miller
EPIC Policy Fellow