April 12, 2017

Docket Management Facility (M-30)
US Department of Transportation
1200 New Jersey Avenue SE
Room W12-140
Washington, DC 20590-0001

RE: Comments on NHTSA Notice of Proposed Rule for FMVSS No. 150, V2V Communications (Docket No. NHTSA-2016-0126)

Submitted by Professors Leonid Reyzin, Anna Lysyanskaya, Vitaly Shmatikov, and Adam D. Smith and the Center for Democracy & Technology

Dear Sir/Madam:

We submit the following comments in response to the National Highway Traffic Safety Administration's (NHTSA) notice of proposed rulemaking to establish a new Federal Motor Vehicle Safety Standard (FMVSS), No. 150, which intends to mandate and standardize vehicle-to-vehicle (V2V) communications for new light vehicles. We are professors of computer science with extensive research expertise in cryptography, data privacy, and network security (we detail our qualifications below). We are joined in these comments by the Center for Democracy & Technology (CDT), a nonprofit advocacy organization that works to promote democratic values by shaping technology policy and architecture and that supports laws, corporate policies, and technologies that protect privacy and security online.

Our comments highlight our concern that NHTSA's proposal standard may not contain adequate measures to protect consumer privacy from third parties who may choose to listen in on the Basic Safety Message (BSM) broadcast by vehicles. Inexpensive real-time tracking of vehicles is not a distant future hypothetical. Vehicle tracking will be exploited by a multitude of companies, governments, and criminal elements for a variety of purposes such as vehicle repossession, blackmail, gaining an advantage in a divorce settlement, mass surveillance, commercial espionage, organized crime, burglary, or stalking.

Our concern is that the privacy protections currently proposed for V2V communications may be easily circumvented by any party determined to perform large-scale real-time tracking of multiple vehicles at once. This poses a serious costs for both individual privacy and society at large, and we caution that the proposed privacy statement does not adequately disclose these threats to consumers. We also note that they are not accounted for in the proposed rule's cost-benefit analysis.

A more privacy-conscious design employing advanced cryptographic techniques (as opposed to a simple public broadcast accompanied by a digital signature) may help resolve some of the privacy concerns.

1. Qualifications

We have extensive experience in data privacy, cryptography, and computer network security. Here we list brief biographical sketches to illustrate our qualifications and interests.

Leonid Reyzin is a professor of Computer Science at Boston University, specializing in cryptography, data security, and network security. He worked at RSA Laboratories, earned his Ph.D. from MIT in 2001, and has held visiting positions at UCLA and IST Austria. His work was recognized with the 2014 Applied Networking Research Prize, 2015 Theory of Cryptography Test of Time Award, and 2017 Eurocrypt Best Paper Award.

Anna Lysyanskaya is a professor of Computer Science at Brown University. She joined Brown in 2002, after obtaining her Ph.D. at MIT. Her research area is cryptography, especially privacy-preserving cryptographic protocols. She is famous for her work on anonymous credentials, which are algorithms that allow users to prove that they are authorized without disclosing any additional information. She is a recipient of the NSF Career award and numerous other grants, the Sloan Foundation Fellowship, and the Google and IBM Faculty Fellowships. Signature schemes and anonymous authorization protocols from her Ph.D. thesis are a part of the Trusted Computing Group Standard's TPM architecture, incorporated into most PC's microprocessors on the market today.

Vitaly Shmatikov is a professor of Computer Science at Cornell Tech. He has been working on digital privacy problems for over 15 years. He is an expert on de-anonymization, inference attacks, and tracking. Prior to joining Cornell Tech, he worked at the University of Texas at Austin and SRI International. He earned his Ph.D. in computer science and M.S. in engineering-economic systems from Stanford University. He received the PET Award for Outstanding Research in Privacy Enhancing Technologies twice, in 2008 and 2014, and was a runner-up in 2013. His research group won the Best Practical Paper or Best Student Paper Awards at the 2012, 2013, and 2014 IEEE Symposiums on Security and Privacy ("Oakland"), as well as the 2012 NYU-Poly AT&T Best Applied Security Paper Award, NDSS 2013 Best Student Paper Award, and the CCS 2011 Test-of-Time Award.

Adam Smith is a professor of Computer Science and Engineering at Pennsylvania State University. His research interests lie in data privacy and cryptography, and their connections to machine learning, statistics, information theory, and quantum computing. He obtained his Ph.D. from MIT in 2004 and has held visiting positions at the Weizmann Institute of Science, UCLA, Boston University and Harvard. He received a Presidential Early Career Award for Scientists and Engineers (PECASE) in 2009; a Theory of Cryptography Test of Time award in 2016; and the 2017 Gödel prize.

We are joined in our comments by the Center for Democracy & Technology via Chief Technologist Joseph Lorenzo Hall[1] and Privacy & Data Policy Counsel, Joseph Jerome.[2]

2. The fundamental problem: Linkability

NHTSA asks whether "any data element (or combination of data elements) currently in the Basic Safety Message (BSM) is reasonably linkable to an individual on a persistent basis?"[3] We argue that the answer is, unfortunately, "yes." BSMs from a single vehicle will be linkable to each other and to the individual who drives the vehicle via a variety of readily available, inexpensive means, as we discuss below. None of the privacy mitigating controls described in section IV.D.5 of the NPRM are sufficient to prevent this problem.[4]

2.1 Linking a vehicle to an individual

The NPRM proposes that vehicle location accurate to within 1.5 meters be included in every BSM. Such high accuracy is sufficient to identify a vehicle's specific parking spot. Assuming a suburban environment where the parking spot is a driveway, this information is enough to identify the owners or tenants of the unit through the use of a geographic information system and public address data, thus linking a vehicle to a person or a household.

Vehicles can be further disambiguated among members of a household or people sharing parking spots by when they leave and where they go. For instance, shift workers, 9-to-5 office workers, high school students, and stay-at-home parents will all have different, distinguishable patterns of vehicle use. Even among office commuters, the first few turns after leaving the driveway will be very useful for disambiguating people working at different locations. A vast majority of American workers can be uniquely identified given their home and work locations with only block-level precision.[5] (Work location data can be readily obtained from a variety of commercially available data sets.)[6]

---

[1] Hall's bio is available here: https://cdt.org/about/staff/joseph-lorenzo-hall/.
[2] Jerome's bio is available here: https://cdt.org/about/staff/joe-jerome/.
[3] 82 Fed. Reg. 3904 (Jan. 12, 2017).
[4] *Id.* at 3929.
[5] Philippe Golle and Kurt Partridge, "On the anonymity of home/work location pairs", Pervasive Computing, 7th International Conference, 2009, pp. 390-397, Table 1, showing that 99% of workers are uniquely identified given home and work locations at census block level, available at: https://crypto.stanford.edu/~pgolle/papers/commute.pdf.
[6] The "Technical Memorandum: Modeling and simulation of Areas of Potential V2V Privacy Risk" (in Docket No. NHTSA–2016–0126) confirms our concerns, by stating "Home addresses, home/work address pairs and similar location information may be exploited through readily available on-line products including mapping tools and property tax records to identify a vehicle's owner, and other on-line sources including social media then could yield a more complete profile of that individual" (Technical Memorandum p.12) and "it is possible that trip origin, destination, and route could be used in conjunction with data sources outside of the V2V system to develop a profile of the individual who owns or operates the V2V device/vehicle broadcasting BSMs" (Technical Memorandum p.23).

2.2 Linking BSMs to construct a pattern of vehicle movement

Linking by Observing the Moment when IDs and Certificates Change

The temporary ID and the security certificate, with their five-minute lifetimes, make it trivial to link BSMs until these values change. Moreover, linking BSMs observed shortly before and after the changeover of these values presents only a minor challenge. Speed, heading, acceleration, and yaw data provide enough information that two BSMs sent within a short time of each other can be linked together based on location (at 60 miles per hour, a vehicle travels only about 2.7m between two consecutive BSMs, which are sent at every 0.1 seconds; this distance is much smaller than typical inter-car distance, making it easy to link consecutive BSMs). Moreover, the 300m path history included in the BSM gives about 11 seconds' worth of past vehicle locations at 60 mph, and even more at lower speeds. Thus, it is enough to observe two BSMs a few seconds before and after the changeover of the temporary id and the security certificate in order to link these values to the previous ones. A continuous, ten times per second observation, is not necessary.

Linking through other message content

Even if this window for observing the same vehicle is missed when a changeover happens, other possibilities for linking BSMs abound. The vehicle size attribute, with its .2m precision in each dimension, is sometimes enough to distinguish vehicles in the same class: for example, to distinguish a 2017 Toyota Sienna from a 2017 Chrysler Pacifica by width. We analyzed lengths and widths of 343 vehicles[7] to find that, at .2m precision, there are 30 categories of vehicles; 7 models are alone in their category and 8 more are in a category with only one other model. For instance, a Ford F-250 and a Ram 3500 share their category with no other vehicle. In areas where these vehicles are not frequent, two BSMs with reasonable time and space proximity can be linked to a single vehicle with high confidence, regardless of whether the five-minute changeover moment was missed.

Even within vehicles of the same dimensions, it will be possible to disambiguate models by subtle, manufacturer-dependent differences. For example, the relationship among the speed, acceleration, steering angle, and yaw will vary subtly among different makes and models; this variability can be exploited to disambiguate vehicles of the same reported dimension and decide which BSMs to link to a single vehicle. Similarly, the way manufacturers implement the proposed standard – such as the way they calculate path history and path prediction, which options they choose to implement, the exact rate at which they transmit, or even the physical characteristics of the signal – will vary from manufacturer to manufacturer and model to model, providing further ability to fingerprint devices and link their BSMs. Indeed, the possibility of

[7] Using data available at: http://www.consumerreports.org/cro/cars/types/exterior-and-cargo-comparison.htm (last visited Apr. 10, 2017).

linking through physical characteristics of the signal is confirmed and considered a risk by the Privacy Issues Report.[8]

Linking through security certificates

The proposed security certificates present an additional possibility for linking across days and hours, even when observation is sporadic and linking based on other attributes is unreliable. NHTSA proposes a system where each vehicle will have 20 valid security certificates each week to "strike a balance between privacy and efficiency."[9] However, any vehicle that starts and stops in the same driveway multiple times per day would permit an observer to link most of a vehicle's weekly allotment of certificates to the same driveway and, thus, to the same vehicle.

All BSMs sent with these certificates are linkable regardless of whether the moment of certificate changeover is observed. Furthermore, assuming a vehicle is driven for about 1 hour per day, we expect about 84 certificate changeovers to happen during a week. It is enough to observe only a portion of those changeovers in order to link most of the 20 weekly certificates together. A single well-placed antenna can observe many certificate changeover moments and thus link weekly certificates: if a vehicle stands at a traffic light or moves slowly in a traffic jam and thus remains within antenna range for a minute, the antenna will observe a changeover of certificates with probability 20%. Once enough changeover moments are observed for a single vehicle, most of the certificates for the week, and thus their BSMs, can be linked together.[10]

Linking through other vehicles

In a high-density highway traffic scenario, BSMs from the same vehicle can also be linked with high confidence based on the vehicles immediately before and after it in its lane, because the order of vehicles in a lane often persists for a few minutes[11]. Thus, if a changeover of the temporary ID and security certificate for a vehicle V is missed, but messages from its preceding vehicle U and following vehicle W are linkable over V's changeover window (by any of the methods described above), then BSMs from V before and after the changeover can also be linked with high confidence, particularly if their quasi-identifiers (discussed in the next paragraph) match.

---

[8] "Privacy Issues for Consideration by USDOT Based on Review of Preliminary Technical Framework," FHWA-JPO-15-236 in Docket No. NHTSA–2016–0126, Section 4.1.4 (Feb. 2016) [hereinafter Privacy Issues Report].

[9] 82 Fed. Reg. 3911.

[10] The possibility of learning most of the weekly certificates, and its implications for the tracking, is also confirmed and considered a risk by the Privacy Issues Report (*supra* note 8), Section 4.1.2.1.

[11] See, for example, "A Comprehensive Examination of Naturalistic Lane-Changes", DOT HS 809 702, available at https://www.nhtsa.gov/DOT/NHTSA/NRD/Multimedia/PDFs/Crash%20Avoidance/2004/Lane%20Change%20Final.pdf

2.3 The linking trade-off: both sophisticated and simple observers benefit

The discussion so far has demonstrated a variety of approaches to linking BSMs. The basic approach relies on good coverage by receivers, in order to observe a vehicle continuously; this approach requires only the location, speed and heading fields of the BSM. If coverage has gaps, relying on other fields in the BSM, such as the temporary ID, vehicle dimension, or location history might permit tracking at lower receiver cost and higher computational cost. Thus, a privacy-violating tracker can choose the point on the tradeoff that is most beneficial for the particular situation.

3. Limited transmission range does not prevent tracking

First, the proposed standard sets no maximum range, no maximum power, nor any other requirements to limit the transmission radius. Furthermore, it has been experimentally demonstrated that limited transmission range does not prevent snooping from a distance: a well-designed bluetooth antenna has been used in field experiments to compromise bluetooth-enabled mobile phones from over a mile (1600m) away, despite the fact that bluetooth in mobile phones (i.e., class 2 bluetooth) has design range of only 10m.[12] Therefore, there is no reason to believe 300m is anywhere near the limitation of a well-designed antenna or collection of antennas.

4. The tracking study in the docket justifies our concerns

The docket includes a report on a study performed by MITRE entitled “Technical Memorandum: Modeling and Simulation of Areas of Potential V2V Privacy Risk.” This study considered the possibilities of linking BSMs for large-scale aggregate tracking in two scenarios: a 14-mile limited access highway and an urban grid. The study concluded that “our modeling indicates that attacks based on combining BSM data elements to associate certificates with V2V devices in vehicles are analytically feasible and, in many cases, practically feasible with respect to the computing resources required.”[13]

4.1 Using only very limited linking and 25% coverage, the study tracked over half the vehicles in an urban setting

The MITRE study considered very limited strategies for linking BSMs: via temporary IDs and certificates, size information, and path history. Even within these variables, the study considered fewer linking possibilities than would be present in a real world deployment. Specifically, the

[12] "'Rifle' Sniffs Out Vulnerability in Bluetooth Devices," All Things Considered (Apr. 13, 2005), https://www.npr.org/templates/story/story.php?storyId=4599106.

[13] Technical Memorandum: Modeling and Simulation of Areas of Potential V2V Privacy Risk in Docket No. NHTSA–2016–0126, at 42 (Mar. 2016) [hereinafter Technical Memorandum].

study did not consider the possibility that links between most of the 20 weekly certificates could be learned within a week's worth of data when changeovers are observed, permitting BSM linking even at times when changeovers are not observed. The study also did not consider less common size categories (choosing only top 10 categories, for which linking is the hardest), and used a simplified version of path history, which covered only 200m with two points, instead of 300m with up to 23 points as in the proposed FMVSS.

It is notable that with only these three simplified opportunities for linking, and with only 25% coverage, the study was able to find full paths for *over 60%* of the vehicles on the road in the urban driving simulation. The study also concluded that even if receivers limited strictly by the 300m radius, placing a receiver per traffic signal is sufficient to provide 100% coverage in the example urban environment--and therefore track all the vehicles.

4.2 The study can be improved to track better, cheaper, and in real-time

The MITRE study does not consider using other quasi-identifiers, such as the slight variations in the reported relationship among speed, acceleration, heading and yaw; the way path history and path prediction are calculated; the way optional fields of the BSM are implemented; or the physical characteristics of the signal. Nor did the study consider linking through the reuse of weekly security certificates, more detailed path history, or position relative to other vehicles, even though some of these possibilities are considered risks in MITRE's own Privacy Issues Report.[14]

In the study, using the very limited (only 2-point, 200m) path history for linking resulted in a large increase in the number of vehicles tracked – in one case, the increase in the number of tracked vehicles was almost nine-fold.[15] It stands to reason that using other linking techniques will also increase percentages of vehicles tracked.

The study also had other limitations. It suggested that tracking on limited-access highways was considerably more difficult but did not consider the possibility of linking via information from preceding and following vehicles. The study assumed that all temporary IDs and certificates change at once, making tracking harder; this assumption is not justified by the proposed standard. Furthermore, the study did not consider many other typical driving scenarios and settings, such as small-town driving, stop-and-go traffic, or nighttime driving where tracking and linking would be easier due to lower speeds and/or lower density of vehicles.

The study considered a vehicle untrackable if it was lost during a single changeover – while, in fact, a vehicle may be lost for a five-minute period and then picked up again using a previously

[14] Privacy Issues Report, *supra* note 8.
[15] Technical Memorandum, *supra* note 13, at 23.

discovered certificate. Furthermore, the study did not consider whether better receiver units could track a vehicle beyond the 300m range.

The study concluded that vehicles would not be trackable in real-time using the hardware and software used in the study, and that post-processing would be required. However, the study used very limited resources: a single computer running as many as eight simultaneous tracking experiments.[16] Obtaining inexpensive hardware resources should not a problem given the availability of cloud computing and the study's own conclusion that data transfer to the cloud should not present a problem.[17] Furthermore, the tracking algorithms were written in Python,[18] which results in slow-running code; simply rewriting the same programs in a faster programming language may improve their performance by as much as an order of magnitude,[19] making all the analysis time reflected in Table 7 of the study less than the simulated time, and thus making real-time tracking possible even with the limited hardware resources used in the study.

To sum up, the adage that "attacks only get better" is applicable here. If the proposed technology is deployed, there will be a race to improve on the tracking attacks presented by the study, and as we have demonstrated, there is ample opportunity for improvement. A competition to track, driven by market and research incentives, will quickly ensue. Open-source tools will be developed and improved upon, bringing tracking capabilities up and costs down.

5. Incentives and costs to track

5.1 Sophisticated tracking

Vehicle tracking is already a big business, with multiple highly skilled, sophisticated companies (for example, INRIX, Navteq, TrafficCast, and others) providing ever more detailed data, such as individual trips with source, destination, and waypoints. There is no reason to doubt that business incentives will push these and similar companies to provide such data at finer granularity, greater volume, and in real time. Companies will build the infrastructure required for to provide the linking described in the previous section.

According to the required transmission range, a receiver should cover about 0.1km^2; it will likely cover a lot more, as discussed above. A town of 100 km^2 can thus be covered by tens or hundreds of receivers. Given the estimated component cost in the proposed standard (in the range of $250-$350), the cost to provide a continuous collection and linking of all BSMs in a

[16] As the study states, "During the analysis, we often ran multiple instances (up to 8) of the tracking analysis in parallel, which resulted in longer individual running times" (Technical Memorandum, *supra* note 13, at 32).
[17] Technical Memorandum, *supra* note 13, section 4.3.3.
[18] *Id.* at 33.
[19] See, for example, https://blog.famzah.net/2016/02/09/cpp-vs-python-vs-perl-vs-php-performance-benchmark-2016/, indicating that Python is about 15 times slower than C.

town will be in the thousands or tens of thousands for initial equipment, which will amortize over several years after purchase (and likely come down in price, as well). Since most trips are relatively short (under 10 miles[20]), most of the trips in a town will be fully observable from beginning to end in real time for less money than a part-time employee. The amortized cost per vehicle observed will be likely measured in cents per year.

Of course, there will also be data collection, processing, and storage costs. However, those are unlikely to present a substantial challenge: most BSMs are immediately linkable with the previous, and thus only location information needs to be stored, downsampled to a location every few seconds. Some BSMs will need to be saved for subsequent postprocessing by the linking algorithms we describe above, but they will represent a small fraction of the total. A single laptop would easily store data for a day's worth driving in a town; furthermore, real-time uploading to cloud storage for post-processing and linking by centralized servers would be easy given the bandwidth available today.

The market will, naturally, bring the costs down and make BSM-based surveillance devices readily available (similarly to how cell-phone surveillance is more readily available and common today than it was a decade ago, with costs starting at under $2,000[21]).

5.2 Unsophisticated tracking

As already mentioned, a privacy-violating tracker can choose the point on the tradeoff between receivers, computation, and linking that is most beneficial for the particular situation. Even small players who would not have sufficiently many receivers for sophisticated linking – for example, stalkers and petty criminals – will benefit from BSM-based tracking. For a burglar, knowing when all the cars in a given driveway leave is valuable information. Without BSMs, the burglar would have to observe individual driveways. With BSMs, a burglar armed with a single receiver can watch a small neighborhood. Similarly, a stalker can monitor his victim's car from an out-of-sight location (by linking the BSM to the driveway) and easily follow her car without visibly tailing it.

6. Comparison and synergy of BSM-based tracking with other tracking

One can ask whether BSM-based tracking will be worse than the status quo. Indeed, the NPRM mentions other methods of vehicle tracking,[22] and the Privacy Technical Analysis Report[23]

[20] Santos, A., McGuckin, N., Nakamoto, H. Y., Gray, D., & Liss, S. (2011). Summary of travel trends: 2009 national household travel survey (No. FHWA-PL-ll-022), available at: http://nhts.ornl.gov/2009/pub/stt.pdf.
[21] Jeremy Scahill & Margot Williams, A Secret Catalogue of Government Gear for Spying on Your Cellphone, The Intercept (Dec. 17, 2015), https://theintercept.com/2015/12/17/a-secret-catalogue-of-government-gear-for-spying-on-your-cellphone/ ; L. Carol Ritchie, Who's Catching Your Cellphone Conversations?, All Tech Considered (Oct. 21, 2014), http://www.npr.org/sections/alltechconsidered/2014/10/21/356191015/whos-catching-your-cellphone-conversations.
[22] 82 Fed. Reg. 3928.

analyzed a variety of other options for vehicle tracking. Many options, such as physically following a car or placing a GPS device on it, do not allow for mass tracking of most vehicles in a given area. Some options, such as cell phone tracking or toll collection history, require specialized access to a private infrastructure. Cellular data does not provide precise position information to just anyone who listens in. In fact, the Technical Memorandum[24] concludes that "[n]either cell/toll history nor GPS seems practical for aggregate tracking."

Moreover, cellular technology is evolving rapidly—today it provides more privacy than in the past, and it is reasonable to believe that better cellular privacy protections will continue to be implemented in decades to come, when the proposed FMVSS will still be operational.

The commonly used license-plate-based tracking requires a line of sight to a given vehicle, and thus is usually neither pervasive nor real-time. A vehicle can be observed driven or parked, but not tracked continuously unless followed. Only a few vehicles can be observed by a camera at any given time. Thus, license-plate-based tracking provides only episodic reports of locations for most vehicles.

In contrast, because receiving the BSM does not require a line of sight and the BSM is transmitted ten times per second, multiple vehicles can be tracked simultaneously, continuously, and in real time.

The Privacy Technical Analysis Report concluded that the only option other than BSMs that may be viable for large-scale real-time tracking without any infrastructure access is via toll transponders. However, those have a much smaller range and, unlike BSMs, require triangulation for precise positioning. In contrast to the proposed FMVSS, toll transponders are not mandated and can be easily removed even when installed. Moreover, toll transponder infrastructure can, over the coming years, be upgraded to include better privacy protections, while the proposed FMVSS will be a required standard for decades to come.

It is almost certain that, once surveillance technology based on V2V messaging matures, this technology will become the cheapest option for aggregate vehicle tracking. Moreover, this tracking can complement and enhance other tracking already done today, such as license-plate-based tracking. In particular, it is easy to link license-plate data to BSM data by combining a DSRC receiver with a license plate reader. Once the link is made, further license plate is unnecessary as long as BSMs can be linked through the means described above. Furthermore, reading the license plates only occasionally, while receiving BSM messages more frequently, can enhance the linking of BSM messages.

[23] Privacy Issues Report, *supra* note 8, Section 3.3
[24] Technical Memorandum, *supra* note 13, at 42.

7. The Need for Opt-in

NHTSA has inquired as to whether consumers should be offered opt-in or opt-out choices for privacy reasons. Due to the serious potential privacy risks addressed above, we firmly believe that, unless a considerably more privacy-conscious proposal is put forward, consumers should be given the choice to opt-in or opt-out (without a default opt-in), and should be made clearly aware of what they are opting into. For example, a stalking victim's greatest risk is her stalker, and giving her the ability to opt out (and the knowledge necessary to make an informed decision) may increase her safety more than the proposed V2V communication. Beyond that, there may need to be other more complicated accommodations that manufacturers will need to support to meet customer demands for everyday private use of vehicles; for example, a "private driving mode" (similar to web browser private browsing mode) that could be used for situations requiring heightened privacy such as attorney-client meetings or trade secret-relevant business activity. We cannot predict today all the possible risks that the loss of privacy will entail several years from now, and we cannot possibly weigh them against the safety benefits of the proposal.

8. The Insufficiency of the Privacy Statement

In light of the above discussion, we believe that the proposed privacy statement in the NPRM is not sufficiently clear to inform consumers about the privacy issues in V2V technologies and BSMs.

Several statements may be misleading. For example, it states that "V2V messages are broadcast … in only the limited geographical range (approximately 300 meters) necessary to enable V2V safety application..." As already discussed above, the standard does not mandate a maximum range, which may be well over 300m. A good receiver antenna will likely greatly increase this range, similar to how the 10m design distance of Bluetooth class 2 devices was increased to 1 mile. The privacy statement goes on to say that "To help protect driver privacy, V2V messages do not … contain data that is reasonably or, as a practical matter, linkable to you." However, as we have discussed, one's driveway location is, as a practical matter, easily linkable to an individual at relatively low cost.

The long explanation following this statement, which uses words "reasonably" and "as a practical matter" in quotation marks (leaving their meaning to interpretation), does nothing to tell the consumer of the very real possibility that someone could be undetectably watching all the driveways on her block, neighborhood, or town, from a distance.

The examples of third-party collection provided in paragraph (b) of the privacy statement mention only benign collection for beneficial purposes, such as accident avoidance, transit maintenance, or valuable commercial services. They selectively highlight the socially beneficial uses of V2V information without mentioning commercial services may not valuable for consumers or other potential detrimental or even criminal uses. This is especially troubling

because NHTSA disclaims having any authority to regulate the collection and use of V2V information beyond safety applications.

Instead, the proposed statement concludes by noting that V2V technologies may have "residual privacy impacts," which does little to tell consumers about actual privacy risks they may face. A stalking victim would not know, from reading this statement, the very real risk to her safety that the BSM entails. It does not mention other potential uses that we expect BSM collection to be put: collection for the purposes of vehicle repossession, blackmail, domestic disputes, mass surveillance, commercial espionage, organized crime, burglary, or stalking. These are serious and very real possibilities; given that we do not know the actual purposes of hypothetical future data collection, selectively mentioning possible socially beneficial uses without mentioning the possible detrimental ones is misleading to the consumer.

9. Conclusion

The NPRM argues that "V2V transmissions would exclude data directly identifying a private motor vehicle or its driver or owner and reasonably linkable to an individual via data sources outside of the V2V system or over time."[25] As we have discussed above, we question whether the NHTSA's V2V standard accomplishes this. As a practical matter, the first BSM sent upon vehicle start will likely be linkable to the driveway and thus to a household via an outside data source; linking from a household to an individual will be only slightly more difficult.

The proposed rule seeks to "appropriately balance" consumer privacy with safety, but we caution that as technology catches up, consumer privacy will be compromised by V2V technologies on a large scale at low cost and in real-time. There will be no "balance" to speak of.

The NPRM states that "in the agency's view, the V2V system is protected by sufficient security and privacy measures to mitigate unreasonable privacy risks. NHTSA seeks comment on these tentative conclusions—and on whether new legislation may be required to protect consumer privacy appropriately."[26]

As argued above, we respectfully disagree with these tentative conclusions; specifically, we find the privacy measures insufficient. We express no opinion on whether the correct solution to this problem is legislative or technological; it is likely that both can be easily circumvented by a determined adversary. A legislative solution may have the drawback of leaving privacy risks hidden, because it may prevent security and privacy researchers from assessing privacy risks, while adversaries, who may be less concerned about violating the law than researchers, may continue to violate privacy. Whichever direction it pursues, the agency must solve this problem. These privacy problems represent a real and immediate danger to widespread public adoption of this technology.

[25] 82 Fed. Reg. 3926.
[26] *Id.* at 3928.

In the lengthy cost-benefit analysis for this proposal, the NPRM includes "perceived privacy loss" as a cost.[27] The word "perceived" makes it seem as if the privacy loss is not a real cost and that the tracking activities we have outlined in this document would not themselves result in real costs and even harms to drivers and passengers in future vehicles that support the BSM standard. There is no doubt that the privacy loss is very real; while its exact impact is hard to quantify and predict, it is certainly not solely "perceived." We respectfully suggest this analysis is incomplete at best.

Can V2V communication be accomplished with reduced privacy risk, while providing for revocation of rogue devices? Decades of cryptographic research give us reasons for optimism. For example, technologies such as anonymous tokens[28] can give a vehicle the ability to broadcast a message authenticated by an anonymous token; but only a limited number of such tokens can be generated per unit time. This way, a rogue vehicle that broadcasts too many messages will not remain anonymous and can be subsequently revoked. Further research in this area and a deeper engagement with the cryptography and privacy research communities are likely to yield a design that can give us the benefits of V2V communication without the devastating privacy costs.

We thank you for the opportunity to submit these comments and please do not hesitate to contact us if we can be of further assistance.

Leonid Reyzin
Professor of Computer Science, Boston University
reyzin@cs.bu.edu

Anna Lysyanskaya
Professor of Computer Science, Brown University
anna@cs.brown.edu

Vitaly Shmatikov
Professor of Computer Science, Cornell Tech
shmat@cs.cornell.edu

Adam Smith
Professor of Computer Science and Engineering, Pennsylvania State University
asmith@cse.psu.edu

---

[27] *Id.* at 3984.

[28] Camenisch, J., Hohenberger, S., Kohlweiss, M., Lysyanskaya, A., & Meyerovich, M. (2006, October). How to win the clonewars: efficient periodic n-times anonymous authentication. In Proceedings of the 13th ACM conference on Computer and communications security (pp. 201-210). ACM, available at: http://static.cs.brown.edu/people/anna/papers/chklm06.pdf.

Joseph Lorenzo Hall
Chief Technologist, Center for Democracy & Technology
joe@cdt.org

Joseph Jerome
Policy Counsel, Center for Democracy & Technology
jjerome@cdt.org