U.S. Department of Transportation

Privacy Impact Assessment

National Highway Traffic Safety Administration

Notice of Proposed Rulemaking (NPRM) on V2V Communications

Responsible Official

Ryan Posten
Associate Administrator, Rulemaking
202-366-0542
ryan.posten@dot.gov

Reviewing Official

Claire W. Barrett
Chief Privacy & Information Asset Officer
Office of the Chief Information Officer
privacy@dot.gov

CLAIRE W BARRETT

Digitally signed by CLAIRE W BARRETT
DN: c=US, o=U.S. Government, ou=OSTHQ, ou=DOT Headquarters, cn=CLAIRE W BARRETT
Date: 2016.12.29 16:43:39 -05'00'

Executive Summary

The United States Department of Transportation (USDOT) and the National Highway Traffic Safety Administration (NHTSA) have been conducting research on Vehicle-to-Vehicle (V2V) crash avoidance technology for more than a decade. In August 2014, NHTSA released a research report entitled "Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application"[1] (V2V Readiness Report) that explored the technical, legal, and policy issues relevant to V2V communications, analyzed the research conducted thus far, the technological solutions available for addressing the safety problems identified by the agency, the policy implications of those technological solutions, legal authority, and legal issues such as liability and privacy. Concurrent with release of the V2V Readiness Report, NHTSA published an Advance Notice of Proposed Rulemaking (ANPRM) on V2V Communications seeking comment on the technical, legal and policy issues discussed in the report. Through its Notice of Proposed Rulemaking (NPRM),[2] NHTSA now proposes to establish a new Federal Motor Vehicle Safety Standard (FMVSS), No. 150, to mandate vehicle-to-vehicle (V2V) communications for new light vehicles and to standardize the message and format of V2V transmissions. This will create an information environment in which vehicle and device manufacturers can create and implement applications to improve safety, mobility, and the environment. Implementation of the new standard will enable vehicle manufacturers to develop safety applications that employ V2V communications as an input, two of which are estimated to prevent hundreds of thousands of crashes and prevent over one thousand fatalities annually. This Privacy Impact Assessment (PIA) of NHTSA's V2V NPRM is being issued concurrent with NHTSA's publication of that proposal. NHTSA looks forward to receiving comments on this PIA and to working with stakeholders and privacy advocates to ensure that it provides the public with a clear and transparent understanding of the how the V2V system operates, potential privacy impacts stemming from the proposed V2V systems, the technical, policy and physical controls that mitigate those potential privacy impacts, and residual impacts that cannot be mitigated without impeding the operation of this important, life-saving safety technology.

What is a Privacy Impact Assessment?

The Privacy Act of 1974 articulates concepts for how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information (PII). The E-Government Act of 2002, Section 208, establishes the requirement for agencies to conduct privacy impact assessments (PIAs) for electronic information systems and collections. The assessment is a practical method for evaluating privacy in information systems and collections, and documented assurance that privacy issues have been identified and adequately addressed. The PIA is an analysis of how information is handled to—i) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; ii) determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and iii)examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.[1]

[1] Office of Management and Budget's (OMB) definition of the PIA taken from guidance on implementing the privacy provisions of the E-Government Act of 2002 (see OMB memo M-03-22 dated September 26, 2003).

[2] The NPRM may be found at https://www.nhtsa.gov/press-releases/us-dot-advances-deployment-connected-vehicle-technology-prevent-hundreds-thousands. NOTE: The NPMR has been signed and is being submitted for publication in the Federal Register. While we have taken steps to ensure the accuracy of this Internet version of the document, it is not the official version. Please refer to the official version in a forthcoming Federal Register publication or on GPO's Web Site. You can access the Federal Register at: www.federalregister.gov.

Conducting a PIA ensures compliance with laws and regulations governing privacy and demonstrates the DOT's commitment to protect the privacy of any personal information we collect, store, retrieve, use and share. It is a comprehensive analysis of how the DOT's electronic information systems and collections handle personally identifiable information (PII). The goals accomplished in completing a PIA include:

- *Making informed policy and system design or procurement decisions. These decisions must be based on an understanding of privacy risk, and of options available for mitigating that risk;*
- *Accountability for privacy issues;*
- *Analyzing both technical and legal compliance with applicable privacy law and regulations, as well as accepted privacy policy; and*
- *Providing documentation on the flow of personal information and information requirements within DOT systems.*

Upon reviewing the PIA, you should have a broad understanding of the risks and potential effects associated with the Department activities, processes, and systems described and approaches taken to mitigate any potential privacy risks.

Introduction & System Overview

NHTSA's V2V NPRM

Safety technology has developed rapidly since the National Highway Traffic Safety Administration (NHTSA) began regulating the auto industry[3]over the last several decades, vehicles have evolved to protect occupants much better in the event of a crash due to advanced structural techniques propagated by more stringent crashworthiness standards, and some crash avoidance technologies (e.g., electronic stability control) are now standard equipment. As a result of existing NHTSA standards for crashworthiness and crash avoidance technologies, along with market-driven improvements in safety, motor vehicles are safer now than they have ever been, as evidenced by a significant reduction in highway fatalities and injuries from 52,627 fatalities in 1970,[4] to 35,092 in 2015 a nearly 38 percent reduction.[5] However, NHTSA believes the greatest gains in highway safety in coming years will result from broad-scale application of crash avoidance technologies.[6] One such technology is the Vehicle to Vehicle (V2V) system proposed by NHTSA in its V2V NPRM.

NHTSA's NPRM would mandate that vehicles transmit and receive from neighboring vehicles important safety information (called V2V messages or Basic Safety Messages (BSMs)) about a vehicle's speed, heading, brake status and other safety-relevant data. By making use of these safety messages, the V2V system would increase a vehicle's capability to warn drivers of potential crash situations because it has greater range and "line-of-sight" capabilities than current and near-term radar and camera based systemsin some cases, nearly twice the range. This longer detection distance and ability to "see" around corners or "through" other vehicles will help the V2V

[3] NHTSA was established by the Highway Safety Act of 1970, as the successor to the National Highway Safety Bureau, to carry out safety programs under the National Traffic and Motor Vehicle Safety Act of 1966 and the Highway Safety Act of 1966. NHTSA also carries out consumer programs established by the Motor Vehicle Information and Cost Savings Act of 1972.

[4] National Highway Traffic Safety Administration, Traffic Safety Facts 2012. http://www-nrd.nhtsa.dot.gov/Pubs/812032.pdf.

[5] National Highway Traffic Safety Administration, Fatality Analysis Report System (FARS) final 2013 data. For more information, see www.nhtsa.gov/FARS.

[6] For more information, see the agency policy statement on automated vehicles at www.nhtsa.gov/staticfiles/rulemaking/pdf/Automated_Vehicles_Policy.pdf.

system in vehicles to perceive some threats sooner than sensors, cameras, or radar can, and warn their drivers accordingly. By providing drivers with timely warnings of impending crash situations, the V2V system could reduce the number and severity of motor vehicle crashes, minimizing the costs to society that would have resulted from these crashes. V2V message data also can be fused with radar and camera based systems in vehicles to provide even greater capability and confidence levels than existing vehicle active safety control systems than either approach alone.

Through its V2V NPRM, NHTSA seeks to establish a new Federal Motor Vehicle Safety Standard (FMVSS) to standardize the set of V2V data and mandate the broadcast of vehicle data required to enable V2V crash-avoidance applications. A V2V system as currently envisioned would be a combination of many elements. This includes a radio technology for the transmission and reception of messages, the structure and contents of "basic safety messages" (BSMs), the authentication of incoming messages by receivers, and, depending on a vehicle's behavior, the triggering of one or more safety warnings to drivers.

The NPRM presents a comprehensive proposal for mandating DSRC-based V2V communications. That proposal includes a pathway for vehicles to comply using non-DSRC technologies that meet certain performance and interoperability standards. A key component of interoperability is a "common language" regardless of the communication technology used. Therefore, the agency's proposal includes a common specification for basic safety message (BSM) content regardless of the potential communication technology. The proposal also provides potential performance-based approaches for two security functions in an effort to obtain reaction and comment from industry and the public.

Privacy Considerations in NHTSA Rulemaking

Before turning to our detailed PIA, it is important to emphasize that NHTSA takes consumer privacy very seriously. The agency is committed to regulating the V2V system in a manner that both protects individuals and promotes this important safety technology. NHTSA has worked closely with privacy experts and our industry research partners -- CAMP[7] and the VIIC[8] to design and deploy a V2V system that helps guard against risks to individual privacy. As conceived, the system will contain multiple technical, physical, and organizational controls to help limit potential privacy impacts on consumers including those related to vehicle tracking by individuals and government or commercial entities. V2V devices will transmit BSMs in a limited geographic range. The system and V2V devices will not collect or store the contents of messages sent or received except for the limited time required for a vehicle's V2V system to provide its driver with crash-avoidance warnings, if appropriate, or to deal with device malfunction. When a device malfunctions, only BSMs relevant to assessing performance will be collected and stored by the system, consistent with the need to address the root cause of the malfunction if it is, or appears to be, widespread. Furthermore, under the standard proposed in the NPRM, V2V messages will not contain information linked or, as a practical matter, linkable to a specific consumer, vehicle, or device routinely used by the consumer. The Agency intends for the terms "linkable as a practical matter" and "reasonably linkable" to have the same meaning, specifically: "capable of being used to identify an individual on a persistent basis without unreasonable cost or effort, in real time or retrospectively, given available data sources." In our view, exclusion from the BSM of data elements "reasonably linkable" to individual consumers strikes the right balance between consumer privacy and vehicle safetyalthough we understand that this could result in the exclusion of some data elements required for crash avoidance applications, as currently designed.

[7] CAMP stands for the Crash Avoidance Metrics Partnership. CAMP is made up of eight original equipment manufacturers that work together with USDOT to perform precompetitive crash avoidance research.

[8] VIIC stands for the VII Consortium. The VIIC is made up of nine light-duty vehicle manufactures that work together to identify and analyze potential policy issues stemming from the development of crash avoidance research by CAMP.

NHTSA, with the support of the DOT Privacy Office and NHTSA's Office of the Chief Information Officer, conducted an interim privacy assessment of the V2V system prior to issuance of the Readiness Report and ANPRM. The interim assessment was intended to provide the structure and serve as a starting point for NHTSA's planned PIA, which is a more in-depth assessment of potential impacts to consumer privacy that might stem from a V2V regulatory action, and of the adequacy of the proposed system controls to mitigate those impacts. On the basis of then available information and stated assumptions, NHTSA's interim privacy assessment identified the system's business needs, relevant system functions, areas of potential privacy impact, and existing/other impact-mitigating technical and policy controls. Since that time, NHTSA has worked closely with privacy experts to identify and prioritize for further analysis specific areas of potential privacy impacts in the V2V system. Additional privacy research, such as dynamic modeling related to location tracking[9] and analysis of PKI best practices, which is ongoing, will help NHTSA further refine its approach to mitigating potential privacy impacts stemming from the V2V system.

As we noted in our V2V Readiness Report, it is important to emphasize that while the privacy controls designed into the V2V system help to mitigate potential adverse impacts on consumer privacy, the residual privacy impacts stemming from the V2V system will never be zero due in part the inherent complexity of the V2V system design and the diversity/large number of interacting components/entities, both technological and human. Additionally, technology changes at a rapid pace and may adversely impact system controls designed to help protect consumer privacy in unforeseen ways. For these reasons, as is standard practice in both the public and private sectors, the primary function of this PIA is to identify residual privacy impacts and the potential consequence/harm of such impacts. On the basis of that critical information, agency decision-makers then will be in an informed position to determine whether those residual privacy impacts are acceptable and, in the alternative, whether functionality should be sacrificed in order to achieve an acceptable level of residual risk, and if so, what functionality.

The technical framework for the V2V system has gone through many iterations and adjustments during the conduct of the V2V research program, as the system has evolved to meet revised or additional needs. For this reason, while the current proposed technical frameworks is sufficient for purposes of NHTSA's rulemaking proposal, NHTSA's assessment of the potential privacy impacts that could result from the proposed V2V system necessarily will be an ongoing process that takes into account future adjustments to the technology and security system required to support the technology, as well as ongoing privacy research.

System Overview and Components

The agency's proposal to regulate V2V technology is broken into distinct functional components, some of which have alternatives that potentially could be employed "in-conjunction-with" or "in-place-of" the agency's proposal. The distinct functional components are: the actual communications technology itself (Section III.E), proposed messaging format and content requirements (Section I.BIII.E.2), , authenticating V2V messages (Section I.CIII.E.3), V2V device misbehavior detection and reporting (Section I.DIII.E.4), malfunction indication requirements (Section IIII.E.5), software and certificate updating requirements (Section I.FIII.E.6), and proposed cybersecurity related requirements (Section I.GIII.E.7).

V2V devices in vehicles would send out V2V safety messages (called BSMs, as noted above) to alert other vehicles to their presence, and receive BSMs from other vehicles in order to determine whether to warn their drivers of an imminent crash situation. Under the primary message authentication proposal, BSMs must be accompanied by message authentication capabilities so that the receiving V2V device can have greater confidence in the authenticity of messages in order to provide consumers increased safety.

[9] See Report: "Technical Memorandum: Modeling and simulation of Areas of Potential V2V Privacy Risk" March 8, 2016 located in Docket No. NHTSA-2016-0126

The agency is proposing to require that V2V devices be capable of broadcasting V2V messages in an interoperable manner, i.e., that devices can both transmit and receive BSMs using V2V communications from all other vehicles equipped with a V2V communications technology. We believe that the requirements described in the NPRM will ensure interoperability. We aim to ensure a uniform method for sending basic safety information about the vehicle. In this way, any vehicle seeking to utilize the V2V information environment to deliver safety benefits would have a known and uniform method for doing so.

In order to create this uniform method, the agency's proposed FMVSS contains requirements in several areas. First, it establishes the content of the information to be sent to the surrounding vehicles (by not only specifying the type of information to send, but also the measuring unit for each information element and the level of precision needed). Second, the proposal specifies requirements for the wireless transmission of the content (i.e., how far, how often, etc.). Third, it specifies a standard approach to authenticate V2V messages that are received to improve confidence in message contents.

In addition to those three points, the FMVSS specifies other aspects of performance for a V2V-communications system in order to support full-scale deployment and enable full functionality including security. The agency recognizes that some capabilities are not necessarily needed to support operations during the first few years of deployment, but would be required as the V2V vehicle fleet grows.

First, the devices regardless of the communication technology need a uniform method for dealing with possible occurrences of high volumes of messages(e.g., potentially reducing the frequency or range of messages in high congestion situations). Second, to help identify and reduce the occurrence of misconfigured or malicious devices transmitting BSM messages, the FMVSS identifies several methods for identifying misbehaving devices. Finally, to support the above functions, the FMVSS identifies requirements for V2V devices in vehicles to communicate with security infrastructure such as a Security Certificate Management System (SCMS) (e.g., in order to obtain new security certificates or report misbehaving devices, and receive information about misbehaving devices).

In short, NHTSA's proposed FMVSS explains: (1) what information needs to be sent to the surrounding vehicles; (2) how the vehicle needs to send that information; (3) how a vehicle validates and assigns confidence in the information; and (4) how a vehicle makes sure the prior three functions work in various operational conditions (i.e., broadcast under congested conditions, manage misbehavior, and update security materials).

At its most basic level, the V2V system proposed in the NPRM consists of the following primary components:

1. **V2V Devices/V2V Safety Messages (also called BSMs)**: V2V devices in vehicles and the safety messages that these devices broadcast and receive via DSRC (or a future interoperable technology);
2. **A Method for Validating and Authenticating the BSM:** It is important that a safety application can place as much confidence as possible in the data contained within BSM messages and detect when messages are modified or changed while in transit. To help improve the level of confidence in BSM messages the agency's primary message authentication proposal describes a Public Key Infrastructure (PKI) approach to message authentication. The proposal envisions a security entity to administer the PKI (i.e., the SCMS), possibly made up of different entities and functions, and infrastructure needed to issue, distribute, and revoke the digital security certificates that permit vehicle to authenticate and rely on V2V messages received from neighboring vehicles. The SCMS also would be designed to detect and remove misbehaving devices.

   In addition the NPRM presents two alternative validation and authentication methods for comment. This first alternative for message authentication set out for comment is less prescriptive and defines a performance-based approach rather than a specific architecture or technical requirement. The second alternative set out for comment stays silent on message authentication and does not specify a message authentication requirement, leaving authentication at the discretion of V2V device implementers.

3. **A Communications Network**: Use of a PKI approach to message authentication and validation would require a communications network capable of permitting secure transmission of security certificates and misbehavior information between V2V devices in cars (and, potentially roadside infrastructure) and the authentication entity the SCMS.

PIA Approach and Scope

As noted above, the V2V system is complex and involves many different components, entities, communications networks, and data flows (within and among system components). Due to these complexities, NHTSA opted not to analyze the potential privacy impacts in the proposed V2V systems on a component-specific basis. Rather, NHTSA focused its PIA on discrete data flows within the systems proposed, as an organic whole. NHTSA worked with privacy experts to zero in on discrete aspects of the proposed V2V system most relevant to individual privacy for impact assessment purposes, identify and prioritize potential privacy impacts requiring further analysis (such as dynamic modeling), and refine the privacy-related requirements in NHTSA's regulatory proposal.

This PIA identifies those V2V transactions involving data most relevant to consumer privacy and the technical, physical and policy controls designed into the V2V system to help mitigate those impacts. The PIA also analyzes the system proposed specifically in terms of the Fair Information Practice Principles (FIPPs), as is required of all DOT PIAs.

Readers interested in reviewing a more comprehensive and technical description of the proposed V2V system and its components are encouraged to review NHTSA's V2V NPRM.

To place our discussion of V2V privacy in context, we first briefly discuss several non-V2V methods of tracking a motor vehicle that currently exist.

Non V2V Methods of Tracking

For comparative purposes, it is useful to consider the potential privacy impacts of the V2V system in the context of tracking mechanisms that do not involve any aspect of the V2V system (non-V2V tracking methods). These non-V2V methods of tracking inform the Agency's risk analysis because, to the extent that they may be cheaper, easier, and require less skill or access to a motor vehicle, they are relevant to our assessment of the likelihood of an individual or entity attempting to use V2V as a method of tracking. Examples of mechanisms that currently may be used to track a motor vehicle target include physical surveillance (i.e., following a car by visual observation), placement of a specialized GPS device on a motor vehicle, physical access to Onboard GPS logs, electronic toll transactions, cell phone history, vehicle-specific cell connections (e.g., OnStar), traffic surveillance cameras, electronic toll transponder tracking, and databases fed by automated license plate scanners. As compared to the potential approaches to V2V tracking discussed below, many of these non-V2V tracking methods may be cheaper, easier, require less (and/or no skill) under certain scenarios.

V2V Data Flows/Transactions with Privacy Relevance

As a starting point for the analysis that underlies this PIA, NHTSA identified and examined all data flows within the proposed V2V systems to determine which would include data fields that may have potential consumer privacy impacts, either alone or in combination, and over time. We identified three data flows relevant for privacy impact purposes:

- Broadcast and receipt of V2V messages (BSMs)
- Broadcast and receipt of Misbehavior Reports
- Distribution of Certificate Revocation List (CRL)

Below, we describe these three data flows and detail the technical, policy and physical controls designed into the system to mitigate potential privacy impacts in connection with each flow. We then discuss the potential privacy impacts that remain, notwithstanding existing privacy controls. These constitute potential areas of residual risk for consideration by decision-makers.

Broadcast and Receipt of the Basic Safety Message (BSM)

BSMs are one of the primary building blocks for V2V communications. They provide situational awareness information to individual vehicles regarding traffic and safety. BSMs are broadcast ten times per second by a vehicle and are designed to warn the drivers of neighboring vehicles of crash imminent situations.

Under NHTSA's proposal and any future adaptation of the technology, BSMs would contain information regarding a vehicle's GPS position, speed, path history, path trajectory, breaking status and other data, as detailed in Section **Error! Reference source not found.**III.E of the NPRM. As discussed below, some data transactions necessitated by the security system may result in additional potential privacy impacts, some of which may be residual.

BSMs are not encrypted. For this reason, as discussed below, observers with specialized roadside or mobile equipment can collect, store and use BSM data for safety, mobility, environmental, commercial and other purposes. Devices covered by the proposed rule have limits on how long they can retain data and how they can use it. Collection, retention, and use of BSM message data by devices not covered by the rule are not limited in use.

Broadcast and Receipt of Misbehavior Messages

Under NHTSA's proposal, when a vehicle receives a BSM from a neighboring vehicle, its V2V system validates the received message and then performs a cross check to evaluate the plausibility of data in the message. For example, it might compare the message content with other received messages or with equivalent information from onboard vehicle sensors. As a result of that cross check, the vehicle's V2V system may identify certain messages as faulty or "misbehaving." NHTSA's primary proposal for misbehavior reporting proposes that the V2V system then prepares a misbehavior report and sends it to the V2V security entity. The security entity evaluates the misbehavior report and may identify a defective V2V device. If it does, the V2V security entity will update the Certificate Revocation List (CRL) with information about the certificates assigned to the defective V2V device. The CRL is accessed by all V2V system components and vehicles on a periodic basis and contains information that warns V2V system participants not to rely on messages that come from the defective device. The security entity also might blacklist the device, in which case it will be unable to obtain additional security credentials from the security entity.

Also under our proposal, organizational and/or legal separation of information and functions within the security entity are important privacy impact-mitigating controls that are designed to prevent a single component or insider from having sufficient information to identify certificates assigned to a specific vehicle or owner. NHTSA plans to work closely with stakeholders to develop policies and procedures to institutionalize appropriate separation of data and functions within the National SCMS.

Under the second alternative for misbehavior reporting, the no misbehavior reporting proposal would not involve any requirement of additional broadcast or transmission of reports to V2V security entities. This means that no additional privacy risk would be imposed under the no misbehavior reporting alternative.

Misbehavior Reports

As described above, NHTSA's primary proposal for misbehavior reporting proposes that the V2V equipment in vehicles send misbehavior reports to the V2V security entity. Such reports will include the received BSM (which appears to be faulty) and other information, such as:

- Reporter's pseudonym certificate
- Reporter's signature
- Time at which misbehavior was identified
- 3D GPS coordinates at which misbehavior was identified
- List of vehicles (device/pseudonym certificate IDs) within range at the time
- Average speed of vehicles within range at the time
- Suspicion type (warning reports, proximity plausibility, motion validation, content and message verification, denial of service)
- Supporting evidence
  - Triggering BSM(s)
  - Host vehicle BSM(s)
  - Neighboring vehicle BSM(s)
  - Warnings
  - Neighboring devices
  - Suspected attacker

Distribution of Certificate Revocation List

As explained above, by evaluating misbehavior reports, the security entity envisioned may identify misbehaving V2V devices in vehicles and place information about those devices on the CRL. The security entity then would make updated CRLs available to V2V system participants and other system parts on a periodic basis to alert V2V devices in the system to ignore BSMs coming from the defective V2V equipment. There is only one type of CRL. Current system design plans do not include placing individual security certificates on the CRL. Rather, each CRL would contain information (specifically, linkseed1, linkseed2, time period index, and LA Identifiers 1 and 2) that OBEs could use to calculate the values of the certificates in messages that should be ignored.

Privacy-Mitigating Controls

From the inception of the research program that would result in V2V technology over a decade ago, NHTSA has worked with its research partners, CAMP and the VIIC, to purse an integrated, privacy positive approach to the V2V system. For this reason, the V2V system described in our proposal would contain multiple layers of technical, policy and physical controls to help mitigate potential privacy impacts system-wide. Below, we discuss the privacy impact-mitigating controls that would apply to each of the three privacy-relevant data flows discussed above. In the course of this discussion, we detail some of the key privacy controls that we expect to see in a National SCMS (based on the current SCMS technical design, see Section IIIV.B.2).

Privacy Controls Applicable to the Broadcast and Receipt of the Basic Safety Message (BSM)

No directly identifying or "reasonably linkable" data in V2V transmissions: Under our proposal, the BSM would not contain information that directly identifies a private motor vehicle (as through VIN, license plate or registration information) or its owner or driver. BSM transmissions also would exclude data "reasonly linkable" or "as a practical matter" linkable[10] to a specific individual.

Rotating Security Credentials: Under the primary proposal for message authentication, a critical control to help mitigate privacy risks created by signing messages is limiting the risk that message authentication credentials could be used to compromise privacy. At the time of manufacture, a vehicle's V2V equipment would receive 3

[10] NHTSA intends for the terms "linkable as a practical matter" and "reasonably linkable" to have the same meaning, specifically: "capable of being used to connect V2V messages to a specific person on a persistent basis without unreasonable cost or effort, either in real time or retrospectively, given available data sources."

years' worth of security certificates. Once the device is initialized into the V2V security system, the security system would send to the device keys on a weekly basis that will unlock 20 certificates at a time. During the course of the week, a vehicle's V2V equipment would use the certificates on a random basis, shuffling certificates at five minute intervals. These certificates would enable a vehicle's V2V system to verify the authenticity and integrity of a received BSM or, in the alternative, identify V2V messages that should be ignored (i.e., those that the security entity has identified as coming from misbehaving V2V equipment and placed on the CRL). The shuffling and random use of certificates every five minutes also will help reduce the risk of vehicle tracking by mitigating the use of security certificates as a de facto vehicle identifier (also referred to as a "quasi-identifier") for tracking vehicles.

Limited Transmission Radius: V2V equipment in vehicles would transmit safety information in a very limited geographical range, typically only to motor vehicles within a 300 meter radius of a V2V device. This limited broadcast is sufficient to enable V2V crash avoidance applications in neighboring vehicles, while limiting access by more geographically distant vehicles that cannot benefit from the safety information.

No BSM Data Collection or Storage within the V2V System: Neither V2V devices in motor vehicles, nor the V2V system (consisting of all V2V devices covered by the proposed rule) as a whole would collect or store the contents of V2V messages sent or received, except for the short time period necessary for a vehicle to use messages for safety applications or in the limited case of device malfunction. These technical controls would help prevent standard in-vehicle V2V systems or the V2V system, as a whole, from after-the-fact tracking of a vehicle's location by accessing and analyzing a vehicle's BSMs. Although specialized roadside and mobile equipment would be able to access and collect BSMs, the V2V data collected would contain no information directly identifying or reasonably linkable to a specific private vehicle or its driver or owner, because the transmission of such information would not be allowed by the V2V rule. Research is ongoing on the methods, cost and effort required to use collected BSMs in combination with other available information or over time to track a specific, targeted vehicle or driver. The Agency believes that such linkage between collected BSMs and a specific vehicle or driver is plausible, but has not yet determined whether it is practical or reasonable, given the resources or effort required. This additional research will help to ensure that our proposed V2V FMVSS incorporates all available, appropriate controls to mitigate unreasonable privacy risk related to collection of BSM transmissions by roadside or mobile sensors. We acknowledge that introduction of this technology will result in residual privacy risk that cannot be mitigated. We seek comment on these tentative conclusions.

FIPS 140-2 Level III Hardware Security Module (HSM): NHTSA has proposed performance requirements that include use of FIPS-140-2 Level 3 hardware security module (HSM) in all V2V equipment in motor vehicles. This physical computing device would safeguard and manage a vehicle's security certificates and guard against equipment tampering and bus probing. This type of secure hardware provides evidence of tampering, such as logging and alerting of tampering, and tamper resistance such as deleting keys upon tamper detection.

Consumer Notice: NHTSA would require that motor vehicle manufacturers, at a minimum, include a standard V2V Privacy Statement in all owner's manuals (regardless of media) and on a publicly accessible web location that current and future owners may search by make/model/year to obtain the data access and privacy policies applicable to their motor vehicle, including those specifically addressing V2V data and functions, as detailed in Section II.DIV.C of the NPRM. As discussed above, NHTSA is also considering the possibility of requiring additional methods for communicating the V2V Privacy Statement to consumers and seeks comment on the most effective methods for providing such notice.

Privacy Controls Applicable to Broadcast and Receipt of Misbehavior Messages

Under the primary misbehavior reporting proposal, when a V2V device in a motor vehicle appears to malfunction, the V2V system would collect and store only BSMs relevant to assessing the device's performance, consistent with the need to address the root cause of the malfunction if it is, or appears to be, widespread. The

alternative no misbehavior reporting proposal does not transmit reports and thus the following controls do not apply.

Encryption of Misbehavior Report: Like all security materials exchanged between V2V equipment in vehicles and a security authority, misbehavior reports would be encrypted. This would help limit but not prevent potential privacy risks that could stem from unintended or unauthorized access to data in misbehavior messages. Specifically, this would reduce the possibility that BSMs contained in misbehavior reports may provide information about the past location of a reporting vehicle (and thereby of the vehicle owner's activities and relationship between the two vehicles), or of vehicles located nearby the reporting vehicle.

Functional/Data Separation within the Security Entity (the SCMS): A key privacy-mitigating control applicable to this data stream is the technical design for the security entity proposed by NHTSA, which provides for functional and data separation across different organizationally and/or legally separate SCMS components. This technical control is designed to prevent individual SCMS entities or insiders from using information, including from misbehavior messages, for unauthorized purposes. The technical separation of information and functions within the security entity could be overcome only by a specific entity within the security organization (called the Misbehavior Authority or MA) after determining, based on misbehavior messages, that a vehicle's V2V equipment is malfunctioning and needs to be blacklisted (i.e., prevented from obtaining any additional security certificates). In order to do so, the MA would need to gather information from the various independent, separate parts of the security entity to identify the device to be blacklisted.

Misbehavior Reports Are Stripped of Geographic Location Information: An example of information separation serving as a privacy control is evident in one particular component of the security organization – the Location Obscurer Proxy (LOP). Misbehavior messages (like other communications between a vehicle's V2V equipment and the security entity) travel through the LOP entity to get to other parts of the security organization. The LOP would strip out information from the misbehavior message that otherwise would permit other parts of the security organization (like the MA) to associate a vehicle's V2V messages with its geographic location. This technical separation of geographic information from messages transmitted between vehicle's V2V systems and the security entity is designed to prevent individual security entities or V2V security organization insiders from colluding to use BSM information inappropriately or to track individual vehicles.

Separation of Security Organization Governance: The design for the V2V security entity (or SCMS) calls for the separation of some critical functions into legally distinct and independent entities that, together, make up the SCMS. This legal separation of security entity governance is designed to prevent individual entities or V2V security organization insiders from colluding to use information for unauthorized purposes such as tracking individual vehicles.

Privacy Controls Applicable to Distribution of the CRL List

Misbehaving V2V equipment in a vehicle stops broadcasting: Under the primary misbehavior reporting proposal, it is possible that information regarding a vehicle's revoked security certificates could enable all revoked certificates to be associated with the same vehicle. This might be used to persistently identify a vehicle during the vehicles' activities. In order to mitigate this potential privacy risk, once a vehicle's V2V system determines that information about it is on the CRL and that the security organization has revoked its security certificates, it would stop broadcasting the BSM.

Potential Privacy Issues by Transaction Type

Based on our analysis of the privacy relevant data flows and controls discussed above, we identified five potential privacy scenarios for further research and/or consideration by the Agency. Table 1 below summarizes the scenarios and corresponding system transactions identified for further analysis

Table 1 Transactions Identified for Further Analysis

Transaction Type	Description
BSM Broadcast Transaction	1. Can data elements, such as location, in the BSM be combined to form a temporary or persistent vehicle identifier
BSM Broadcast Transaction	2. Under the primary message authentication proposal, can data elements in the BSM be combined to identify vehicles temporarily so that different security certificates can be associated with the same vehicle during the vehicle's activities
BSM Broadcast Transaction	3. Can the physical characteristics of the carrier wave (i.e., the wave's fingerprint) be associated with a vehicle's BSM serve as a vehicle identifier
Broadcast and Receipt of a Misbehavior Message	4. Under the primary misbehavior reporting proposal, do BSMs in misbehavior reporting provide sufficient information about the past location of the reporting or other vehicles to retrospectively track the vehicle's path?
Certificate Revocation List (CRL) Distribution Transaction	5. Under the primary misbehavior reporting, does information regarding blacklisted vehicles' security certificates enable all vehicle security certificates to be associated with one another and thus, with the same specific vehicle?

As noted above, based on our exploration of privacy impacts and analysis of the V2V system design to date, it is NHTSA's expectation that the multiple technical, policy and physical controls incorporated into the design of the V2V system detailed will help to mitigate privacy risks to consumers. Methods of tracking vehicles, such as surveillance and use of specialized GPS devices already exist and may be easier, less expensive, and require less skill and access than would vehicle tracking using V2V messages or other information in the V2V system in certain conditions. Nevertheless, DOT is continuing to work with privacy experts to perform dynamic modeling and explore the viability of additional controls that might further mitigate any potential impacts demonstrated in the privacy-relevant transactions identified above for further analysis. The planned implementation by DOT of a PoC security entity (SCMS) and related PKI policy research will provide an operational environment in which to continue to explore the viability of additional privacy-mitigating controls applicable to the V2V System, as currently envisioned and designed. We seek comment on whether there are other potential privacy risks stemming from the V2V systems proposed that the agency should investigate and, if so, what specific risks.

Fair Information Practice Principles (FIPPs) Analysis

The Fair Information Practice Principles (FIPPs) are rooted in the tenets of the Privacy Act and are mirrored in the laws of many U.S. states, as well as many foreign nations and international organizations. The FIPPs are common across many privacy laws and provide a framework that will support DOT efforts to appropriately identify and mitigate privacy risk. The FIPPs-based analysis DOT conducts is predicated on the privacy control families articulated in the Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) v.3i, which is sponsored by the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), and the Federal Chief Information Officers Council.

Transparency

Sections 522a(e)(3) and (e)(4) of the Privacy Act and Section 208 of the E-Government Act require public notice of an organization's information practices and the privacy impact of government programs and activities.

Accordingly, DOT is open and transparent about policies, procedures, and technologies that directly affect individuals and/or their personally identifiable information (PII). Additionally, the Department should not maintain any system of records the existence of which is not known to the public.

Through this PIA, NHSTA's V2V NPRM and a proposed V2V Privacy Statement (appearing below), NHTSA intends to provide the public with transparent and understandable notice of any potential privacy impacts affecting individuals or their personal information that could result from the proposed V2V FMVSS. NHTSA plans to work with the Federal Trade Commission (FTC), motor vehicle manufacturers and privacy advocates to develop a strategy for providing the V2V Privacy Statement to consumer in a way that incorporates the concepts of layered and just-in-time consumer privacy notices. NHTSA intends to collaborate with motor vehicle manufacturers to build on their recent commitment to make privacy-related information clearer and more readily available to consumers.[11] To this end, NHTSA's regulatory proposal requires that motor vehicle manufacturers, at a minimum, include the following V2V Data Privacy Statement in all owner's manuals (regardless of media) and in a publicly accessible web location that current and future owners may search by make/model/year to obtain the data access and privacy policies applicable to their motor vehicle, including those specifically addressing V2V data and functions.

V2V Privacy Statement

V2V Messages

The National Highway Traffic Safety Administration (NHTSA) requires that your vehicle be equipped with a Vehicle-to-Vehicle (V2V) safety system. The V2V system is designed to give your vehicle a 360 degree awareness of the driving environment and warn you in the event of a pending crash, allowing you to take actions to avoid or mitigate the crash, if the manufacturer of your vehicle has installed V2V safety applications.

Your V2V system periodically broadcasts and receives from all nearby vehicles a V2V message that contains important safety information, including vehicle position, speed, and direction. V2V messages are broadcast ten times per second in only the limited geographical range (approximately 300 meters) necessary to enable V2V safety application to warn drivers of pending crash events.

To help protect driver privacy, V2V messages do not directly identify you or your vehicle (as through vehicle identification number or State motor vehicle registration), or contain data that is reasonably or, as a practical matter, linkable to you. For purposes of this statement, V2V data is "reasonably" or "as a practical matter" linkable to you if it can be used to trace V2V messages back to you personally for more than a temporary period of time (in other words, on a persistent basis) without unreasonable expense or effort, in real time or after the fact, given available data sources. Excluding reasonably linkable data from V2V messages helps protect consumer privacy, while still providing your V2V system with sufficient information to enable crash-avoidance safety applications.

Collection, Storage and Use of V2V Information

Your V2V system does not collect or store V2V messages except for a limited time needed to maintain awareness of nearby vehicles for safety purposes or in case of equipment malfunction. In the event of malfunction, the V2V system collects only those messages required, and keeps that information only for long enough to assess a V2V device's misbehavior and, if a product defect seems likely, to provide defect information to your vehicle's manufacturer.

[11] See, "Privacy Principles for Vehicles and Technologies" http://www.autoalliance.org/?objectid=865F3AC0-68FD-11E4-866D000C296BA163 (last accessed 12/8/2015)

NHTSA does not regulate the collection or use of V2V communications or data beyond the specific use by motor vehicles and motor vehicle equipment for safety-related applications. That means that other individuals and entities may use specialized equipment to collect and aggregate (group together) V2V transmissions and use them for any purpose including applications such as motor vehicle and highway safety, mobility, environmental, governmental and commercial purposes. For example, States and localities may deploy roadside equipment that enables connectivity between your vehicle, roadways and non-vehicle roadway users (such as cyclists or pedestrians). These technologies may provide direct benefits such as use of V2V data to further increase your vehicle's awareness of its surroundings, work zones, first responders, accidents, cyclists and pedestrians. State and local entities (such as traffic control centers or transportation authorities) may use aggregate V2V safety messages for traffic monitoring, road maintenance, transportation research, transportation planning, truck inspection, emergency and first responder, ride-sharing, and transit maintenance purposes. Commercial entities also may use aggregate V2V messages to provide valuable services to customers, such as traffic flow management and location-based analytics, and for other purposes (some of which might impact consumer privacy in unanticipated ways). NHTSA does not regulate the collection or use of V2V data by commercial entities or other third parties.

While V2V messages do not directly identify vehicles or their drivers, or contain data reasonably linkable to you on a persistent basis, the collection, storage and use of V2V data may have residual privacy impacts on private motor vehicle owners or drivers. Consumers who want additional information about privacy in the V2V system may review NHTSA's V2V Privacy Impact Assessment, published by The U.S. Department of Transportation at http://www.transportation.gov/privacy.

If you have concerns or questions about the privacy practices of vehicle manufacturers or third party service providers or applications, please contact the Federal Trade Commission https://www.ftc.gov.

Individual Participation and Redress

DOT should provide a reasonable opportunity and capability for individuals to make informed decisions about the collection, use, and disclosure of their PII. As required by the Privacy Act, individuals should be active participants in the decision making process regarding the collection and use of their PII and be provided reasonable access to their PII and the opportunity to have their PII corrected, amended, or deleted, as appropriate.

The collaborative nature of V2V technology requires that all motor vehicles transmit the same information using the same method, so NHTSA's has proposed a regulatory mandate requiring that all new motor vehicles satisfy V2V performance standards. All consumers who choose to purchase new motor vehicles would be participants in the V2V System. As proposed, the regulation would not permit individuals to "opt-out" of the system. However, the Agency's NPRM seeks comment on an "if equipped" option. NHTSA also is requesting comment on possible approaches to deactivating V2V related hardware and software for various reasons, including due to privacy concerns.

Statutory Authority and Purpose Specification

DOT should (i) identify the legal bases that authorize a particular PII collection, activity, or technology that impacts privacy; and (ii) specify the purpose(s) for which its collects, uses, maintains, or disseminates PII.

NHTSA has broad statutory authority to regulate motor vehicles and items of motor vehicle equipment under the National Traffic and Motor Vehicle Safety Act (the "Safety Act"). As applied in this context, the agency's authority includes all or nearly all aspects of a V2V system. Congress enacted the Safety Act in 1966 with the purpose of reducing deaths and injuries as a result of motor vehicle crashes and non-operational safety hazards attributable to motor vehicles. The Safety Act, as amended (codified at 49 U.S.C. §§ 30101 et seq) gives NHTSA

the legal authority to mandate the broadcast of V2V safety messages in light vehicles that will enable crash-avoidance V2V safety applications.

As detailed in the system overview, the V2V system will collect, disseminate, and use three primary categories of data:

1. **Basic Safety Messages (BSMs)**: BSMs are the primary building blocks for V2V communications. They provide situational awareness information to individual vehicles regarding traffic and safety. BSMs are broadcast ten times per second by a vehicle to all neighboring vehicles and are designed to warn the drivers of those vehicles of crash imminent situations. BSMs would contain information regarding a vehicle's GPS position, speed, path history, path trajectory, breaking status and other data, as detailed in the NPRM. Under NHTSA's proposal, BSMs would exclude data linked or "reasonably linkable" to an individual (meaning capable of being used to trace BSM data back to a specific vehicle or its owner on a persistent basis without unreasonable cost or effort, in real time or retrospectively, given available data sources).
2. **Misbehavior Reports**: Under the primary misbehavior reporting approach proposed by NHTSA, V2V equipment in vehicles would send misbehavior reports to a V2V security entity (SCMS). Such reports will include the received BSM (which appears to be faulty) and other information, such as:
   - Reporter's pseudonym certificate
   - Reporter's signature
   - Time at which misbehavior was identified
   - 3D GPS coordinates at which misbehavior was identified
   - List of vehicles (device/pseudonym certificate IDs) within range at the time
   - Average speed of vehicles within range at the time
   - Suspicion type (warning reports, proximity plausibility, motion validation, content and message verification, denial of service)
   - Supporting evidence
     - Triggering BSM(s)
     - Host vehicle BSM(s)
     - Neighboring vehicle BSM(s)
     - Warnings
     - Neighboring devices
     - Suspected attacker
3. **Certificate Revocation List (CRL)**: Also under the primary misbehavior reporting approach proposed by NHTSA, the SCMS evaluates misbehavior reports received from system participants to identify misbehaving V2V devices in vehicles, information about which it places on the CRL. The security entity then would make updated CRLs available to V2V system participants and other system parts on a periodic basis to alert OBEs to ignore BSMs coming from the defective V2V equipment. There is only one type of CRL. Current system design plans do not include placing individual security certificates on the CRL. Rather, each CRL would contain information (specifically, linkseed1, linkseed2, time period index, and LA Identifiers 1 and 2) that OBEs could use to calculate the values of the certificates in messages that should be ignored.

Data Minimization & Retention

DOT should collect, use, and retain only PII that is relevant and necessary for the specified purpose for which it was originally collected. DOT should retain PII for only as long as necessary to fulfill the specified purpose(s) and in accordance with a National Archives and Records Administration (NARA)-approved record disposition schedule.

By design, NHTSA's NPRM proposes to mandate the ongoing broadcast and collection by V2V devices of only those data elements necessary to enable crash-avoidance safety applications in motor vehicles. Except as required for temporary situational awareness and misbehavior detection, the V2V system would not collect or maintain V2V messages (BSMs) broadcast or received by motor vehicles for crash avoidance purposes. Only V2V message (BSM) data included in Misbehavior Reports transmitted to the SCMS would be retained for the period of time necessary for the Misbehavior Authority (MA) to determine whether an OBE is misbehaving, to eradicate such misbehavior and, in the event that a defect appears to be widespread, to notify the manufacturer of the vehicle containing the device.

The National SCMS is expected to be a private entity so will not be subject to Federal record retention or disposition requirements. However, DOT expects to play a central role in developing the policies and procedures that will govern the SCMS, including those designed to limit the collection and retention of misbehavior data by the SCMS only to that necessary to identify and respond effectively to misbehavior in the V2V system.

Use Limitation

DOT shall limit the scope of its PII use to ensure that the Department does not use PII in any manner that is not specified in notices, incompatible with the specified purposes for which the information was collected, or for any purpose not otherwise permitted by law.

The V2V NPRM contains technical performance requirements that enable the transmission, collection and use of vehicle safety data (BSMs) by motor vehicles for crash avoidance purposes, as well as for purposes of identifying and addressing misbehavior in the V2V system. The NPRM excludes from BSM transmissions data linked or reasonably linkable to a specific individual.

As noted elsewhere in this PIA, observers with specialized roadside or mobile equipment may collect and use BSM transmissions for any purpose. NHTSA does not have legal authority to limit the collection or use of V2V communcations by such observers. However, NHTSA believes that the utility of BSM data collected in this manner will be limited primarily to aggregate uses that do not create unreasonable privacy risks for individual consumers.[12] By excluding from the BSM data linked or, as a practical matter linkable to a specific individual, NHTSA has taken meaningful steps to limit the privacy risks to individuals that might otherwise result from the collection and use of BSMs by third parties.

Under the primary authentication and validation approach proposed by NHTSA, a National SCMS is expected to be a private entity so its internal use of misbehavior reports and other V2V-related information will not be subject to direct Federal oversight or management. However, as noted above, DOT expects to play a central role in developing the draft policies and procedures that will govern that entity -- including those designed to ensure that SCMS entities or insiders do not use V2V data in any manner that is not specified in this PIA or the V2V Privacy Statement provided to owners, in ways incompatible with the specified purposes for which the information was collected, or for any purpose not otherwise permitted by law – and will do it in a way that limits use of V2V data only to those specified purposes.

[12] For a discussion of potential data uses by third parties, see the Consumer Privacy Notice detailed above.

Data Quality and Integrity

In accordance with Section 552a(e)(2) of the Privacy Act of 1974, DOT should ensure that any PII collected and maintained by the organization is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in the Department's public notice(s).

The V2V performance requirements proposed by NHTSA contain multiple technical checks on data integrity and viability designed to ensure data quality and integrity system-wide. V2V messages also would be authenticated by digital certificates provided by the National SCMS. These security certificates would enable vehicles to place confidence in V2V messages received from nearby vehicles. As part of message validation, a vehicle's V2V device would perform crosschecks to evaluate the accuracy of data provided by the received messages. One approach to this check process is to compare the message content with other received messages or with equivalent information from onboard vehicle sensors. The results of that evaluation may identify messages that appear to be faulty, whether due to poor source data, transmission errors over wireless channels, or OBE sensor failures. These messages may be identified as "Misbehaving," which will result in a Misbehavior Reports being sent to the security entity (SCMS) for assessment. After evaluation, the security entity might identify the V2V device that is the source of the misbehavior and place information about the misbehaving V2V device on a Certificate Revocation List (CRL). System participants and parts would acess updated CRLs from the SCMS on a periodic basis. The CRLs would alert OBEs in vehicles to ignore BSMs tranmitted from malfunctioning V2V devices.

DOT expects to play a central role in developing the policies and procedures that will govern the National SCMS, including those designed to ensure data quality and integrity within the SCMS.

Security

DOT shall implement administrative, technical, and physical measures protect PII collected or maintained by the Department against loss, unauthorized access, or disclosure, as required by the Privacy Act, and to ensure that organizational planning and responses to privacy incidents comply with OMB policies and guidance.

From a technical perspective, NHTSA has proposed performance requirements that require use of FIPPS 140-2 Level III hardware security modules (HSMs) in all V2V devices in motor vehicles. This physical computing device would safeguard and manage a V2V device's digital keys for strong authentication and provide for secure cryptoprocessing to prevent tampering and bus probing. This type of HSM provides evidence of tampering, such as logging and alerting of tampering, and tamper resistance such as deleting keys upon tamper detection.

From a policy perspective, DOT expects to play a central role in developing the policies and procedures that will govern the National SCMS, including those relating to data security, training, organizational and policy controls deployed; role base access, unique login, encryption, intrusion detection, and related data security controls. We expect that the policies and procedures that will apply to the National SCMS will be consistent with PKI best practices for similar privacy and safety sensitive systems.

Accountability and Auditing

DOT shall implement effective governance controls, monitoring controls, risk management, and assessment controls to demonstrate that the Department is complying with all applicable privacy protection requirements and minimizing the privacy risk to individuals.

As noted above, DOT expects to play a central role in developing the policies and procedures that will govern the National SCMS, including those relating to accountability and auditing. Additionally, DOT expects to enter into agreements with a private entity to manage and coordinate SCMS functions that will include minimum policy and procedure requirements designed to ensure continuity of function, cybersecurity and appropriate privacy-risk controls.

Responsible Official

Ryan Posten
Associate Administrator, Rulemaking
ryan.posten@dot.gov

Approval

Claire W. Barrett
Chief Privacy & Information Asset Officer
Office of the Chief Information Officer
privacy@dot.gov