Connected Vehicle Pilot Deployment Program

Privacy White Paper

www.its.dot.gov/index.htm

Final Report – September 21, 2016
FHWA-JPO-17-450

U.S. Department of Transportation

U.S. Department of Transportation
Office of the Assistant Secretary for Research and Technology

Notice

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
FHWA-JPO-17-450		

4. Title and Subtitle	5. Report Date
Connected Vehicle Pilot Deployment Program: Privacy White Paper	September 21, 2016
	6. Performing Organization Code

7. Author(s)	8. Performing Organization Report No.
Edward Fok, Claire Barnette, Dana Sade	

9. Performing Organization Name and Address	10. Work Unit No. (TRAIS)
Federal Highway Administration 1200 New Jersey Avenue Washington, DC 20590	11. Contract or Grant No.

12. Sponsoring Agency Name and Address	13. Type of Report and Period Covered
Federal Highway Administration 1200 New Jersey Avenue Washington, DC 20590	14. Sponsoring Agency Code

15. Supplementary Notes

16. Abstract

Connected Vehicle (CV) technologies are beneficial when users feel safe broadcasting their Basic Safety Messages and trust in their safety and mobility applications. Users must also accept and have a right to know how their privacy is impacted by being a part of the CV eco-system. User doubts or uncertainties in the ability of the connected vehicle ecosystem to protect their identity can slow down the rate of adoption or forcibly opt out of the system. The consequences of such action are fatalities and injuries in situations where CV systems could have mitigated or prevented collisions.

17. Keywords	18. Distribution Statement
Connected vehicle, privacy, security, PII, SPII	

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
		10	

Form DOT F 1700.7 (8-72) **Reproduction of completed page authorized**

Table of Contents

1. Objective of this Paper 1
2. Objective of a Privacy Management Plan 2
3. Protecting Privacy 3
4. Terminologies Expressing Objectives, Controls, and Risk 4
5. How to Assess Privacy Risk 8
Appendix A. List of Acronyms 10

1. Objective of this Paper

Connected Vehicle (CV) technologies are beneficial when users feel safe broadcasting their Basic Safety Messages and trust in their safety and mobility applications. Users must also accept and have a right to know how their privacy is impacted by being a part of the CV eco-system. User doubts or uncertainties in the ability of the connected vehicle ecosystem to protect their identity can slow down the rate of adoption or forcibly opt out of the system. The consequences of such action are fatalities and injuries in situations where CV systems could have mitigated or prevented collisions.

Connected Vehicle systems are designed to use Security Credential Management System (SCMS) pseudo certificates to establish message trust. The core Basic Safety Message (BSM) does not contain any Personally Identifiable Information (PII). The rotating certificates used by the SCMS provide a level of PII protection equivalent to what an individual can expect in a public space. Deployments of the SCMS by the Pilot sites are addressed in the SCMS Management Plans. This whitepaper will address considerations and proposed processes useful in a Privacy Management Plan.

This white paper is intended for the following audiences:

- CV Pilot site team members
- FHWA Staff and contractors

There are no security sensitive information or confidential unclassified information in this document.

2. Objective of a Privacy Management Plan

The Privacy Management Plan shall identify the privacy Objectives of the agency and the project/deployment. Identify the Controls going into establishing these goals and identify metrics that can determine the degree of privacy protection deployed. The plan shall provide traceability between the Objectives and the Controls.

The considerations going into a Privacy Management Plan can include, but are not limited to: local/state/and Federal legal requirements, Consumer Protection standards, Federal Standards such as National Institute of Standards and Technologies (NIST) Specials Publication (SP) 800-53 (Security and Privacy Controls for Federal Information Systems), FIPS 199 (Standards for Security Categorization of Federal Information and Information Systems), NIST SP800-60 (Guide for Mapping Types of Information and Information Systems to Security Categories), and other Standards can be useful in developing a Privacy Management Plan. These Standards will be referenced where appropriate.

The Privacy Management Plan shall describe a consistent process to evaluate privacy risk. The Pilot sites have a limited number of applications and objectives that can be tested to determine if appropriate protection exists in the design. CV Pilot sites differ from operational deployments because they include a significant evaluation component and involve Human Subjects. In addition to any Federal, State, or local regulations and Standards, it is important to consider the objectives of the Human Use Agreement when developing the privacy objectives. Consistent processes also provide transparency on how privacy protection is delivered and is needed for auditing purpose.

The SCMS provides a mechanism for trust and privacy protection between certified devices conforming to SAE and IEEE Standards. But information flowing into these systems from legacy components can be compromised. Such legacy systems should be identified and the risk assessed to the type of data the legacy systems are permitted to handle, how those data can be protected, how to determine if a violation occurred, and how to respond to a privacy violation

3. Protecting Privacy

PII comes in several different forms with different degrees of information content. PII are any information that can be used to identify an individual rather than a device, vehicle, or transmitter. Basic information such as name, address, telephone number, and equipment identification can be considered PII.

Potential PII (pPII) are any information that when combined with other sources can identify an individual. Examples of potential PII are MAC Addresses, vehicle dimensions, and session cookies.

Sensitive PII (sPII) are any information that if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Sensitive PII requires stricter handling guidelines because of the increased risk to an individual if the data are compromised. SPII may contain any of the following:

- Social Security number (SSN)
- Passport number
- Driver's license number
- Vehicle Identification Number (VIN)
- Biometrics, such as finger or iris print
- Financial account number such as credit card or bank account number
- The combination of any individual identifier and date of birth, or mother's maiden name, or last four of an individual's SSN

Non-PII can become PII when additional information is made publicly available. This applies to any medium and any source that, when combined with other available information, could be used to identify an individual. Some PII may be deemed sensitive based on context. For example, a list of employee names is not sPII; however, a list of employees' names and their performance rating would be considered sPII.

Connected Vehicle technologies are designed without any need for PII or sPII. Evaluation of pilot site performance could require PII or sPII from some human subjects. It is important that participants understand this as part of the Human Use Approval agreement.

What are the responsibilities of vehicle systems and legacy systems? Legacy systems utilizing or storing PII should be validated to meet existing PII policy of the operating agency. When the PII protection does not achieve the Standard needed by Connected Vehicle technologies, the agency should determine if the PII used by the legacy system will be a part of the pilot. Any PII data used for the pilot should conform to the Privacy Management Plan developed for the Pilot Deployment. PII generated by aftermarket and mobile devices created for the Pilot Deployment shall conform to the Privacy Management Plan

4. Terminologies Expressing Objectives, Controls, and Risk

FIPS 199 recommends a standard description for Objectives in a secure system. The objectives are described as confidentiality, integrity, and availability (or C/I/A):

- Confidentiality is defined as "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" [44 U.S.C., Sec. 3542] where a loss of confidentiality is the unauthorized disclosure of information. (source: FIPS 199, page 2)
- Integrity is defined as "Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity…" [44 U.S.C., Sec. 3542] where a loss of integrity is the unauthorized modification or destruction of information. (source: FIPS 199, page 2)
- Availability is defined as "Ensuring timely and reliable access to and use of information…" [44 U.S.C., SEC. 3542] where a loss of availability is the disruption of access to or use of information or an information system. (source: FIPS 199, page 2)

The mechanism and processes used to insure C/I/A objectives are achieved involves the application of controls. Controls are based on the original Fair Information Practice Principles (FIPP) developed by the Federal Trade Commission (FTC). The principles of FIPP are expressed in NIST SP800-53 in the following general categories (source: NIST SP800-53r4, Appendix J, Page J-2, Table J-1). Each category of controls cited in SP800-53 contains references to specific controls suitable to meet PII protection for each of the following categories:

1. Authority and Purpose (Control: AP, page J-6): This establishes that the organization has the legal bases where PII can be collected or can conduct activities that impacts privacy. It also requires that the organization documents the purpose(s) for which PIIs are collected.
    - Has the organization's authority to collect PII passed review by legal counsel within the organizations?
    - Authority should be documented in System of Records Notice (SORN) and/or Privacy Impact Assessment (PIA) or other applicable documents
    - Is there clear documentation of the purposes PII are being collected?
    - Are personnel with access to PII well defined and offered PII handling training?

2. Accountability, Audit, and Risk Management (Control: AR, Page J-7): There should be effective controls for governance, monitoring, risk management, and assessment to demonstrate that organizations are complying with applicable privacy protection requirements and minimizing overall privacy risk.

3. Data Quality and Integrity (Control: DI, J-12): Will any of the information collected be used to make any decision about the subject? If such possibility exists during the term of the pilot program, there shall be controls in places to insure PII data quality and ability for error corrections.
    - Does the document describe the controls used to insure the PII used is correct?
    - Is the error correction mechanism described to correct the error in the PII and reconsider the decision?

4. Data Minimization and Retention (Control: DM, J-14): Confirm there is a use case for the PII that is either traceable to a data flow in an application or identified by the evaluation plan.
    - Is there a description of what PII is needed to support the application data flow?
    - Are PII being collected for Evaluation?
        - Is the evaluation goal clearly traceable to an application or pilot site goal?
        - Is there a description of what PII is needed (location PII, activity, etc.) for the identified evaluation performance measures?
    - Are there any other references to PII in the deliverables?
        - If these references are not used by V2I applications or for evaluation, what are they for?
        - Has the site provided justification for why non-PII information cannot be substituted?
    - SSN cannot be collected without a clearly defined need that cannot be met using any other information.
    - Collected data shall be destroyed once the purpose of the collection is satisfied.

5. Individual Participation and Redress (Control: IP, J-17): Does the participant have a role to decide the use of their PII?
    - Is there a way for someone to correct any error in the collected PII?
    - Is there a way to handle complaints?
        - Is there a mechanism for someone to file a complaint?
        - Is there a mechanism for the organization to address and resolve a complaint?

6. Security (Control: SE, J-20): Is there sufficient description of how collected PII will be protected and handled? The security will apply to both physical and electronically stored media containing PII.
    - Does the description address protection against risks such as data loss; unauthorized access, use, destruction or modification; or unintended or inappropriate disclosure?
    - Does the document addresse all reasonably anticipated threats to releases of PII?
    - Do the minimum controls meet or exceed controls described in NIST FIPS-199 Standards?
    - If encryption is needed, do they meet established NIST cryptographic standards? It is very important to use standard based cryptographic tools that are vetted by NIST.
    - Is there an approval process to determine what computing or mobile devices are allowed to store encrypted PII data?
    - Is there an incident detection and response plan?
        - Does the plan contain a clear definition of a breach for staff to determine if a breach is occurring?
        - When a breach is detected, is the response plan described in the deliverables?

    - Does the plan include a notification time to inform the affected individuals of a breach?

7. Transparency (Control: TR, J-22): Look for instances where PII is collected, either deliberately or as a secondary result of an activity
    - Is there a description of how individual consent is obtained for the collection, use, dissemination and maintenance of PII?
    - Does the description include how consent is obtained from individuals for new uses of their PII?

8. Use Limitation (Control: UL, J-24): Are data sharing arrangements clearly described in the document? This includes any arrangements between Federal Government and the leading pilot site agency, between the lead agency and their external partners, and other departments within the lead agencies.
    - Make sure PII are being used as described in any public notice. For example: As described to the individuals when obtaining their consent.
    - Look for the possibility of any monetization from the collected PII either directly or indirectly by any entity with authorized access. This is not allowed under any condition.
    - Do the pilot sites identify a MOU or equivalent instrument to explicitly define the purpose, condition, and authorized uses of the shared PII?
    - Do the pilot sites describe how they will determine if the organization receiving the shared information has sufficiently protected the PII?

The degree of impact from failure to satisfy an objective are described using three standardized categories from FIPS 199:

1. Low Impact: The loss of C/I/A could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. (source: FIPS 199, page 2)
2. Moderate Impact: The loss of C/I/A could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals (source: FIPS 199, page 2)
3. High Impact: The loss of C/I/A could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. (source: FIPS 199, page 3)

Vehicle position, despite not including PII themselves, can be linked together to create unique vehicle trajectories of an individual. These data could track an individual's home, work, or other personal locations and identities. For this reason, vehicle location and trajectories shall be obfuscated to maintain privacy. There are a several methods to accomplish this task:

- Remove the beginning and end of all vehicle trips. This generally removes home and work locations
- Remove all locations that a vehicle stops at, but engine remains running, for a period of 2 minutes or longer.
- Add uncertainty to trajectory removal by setting a random amount of distance, time, or intersections crossed as a minimum threshold for data removal.

In the Pilot Deployment's privacy management plan, Confidentiality and Integrity should be the most common objectives to sustain. Availability is also important where an evaluator requires access to information as needed to meet objectives, and where the Pilot Site or Individual owners of such information seek access for other purposes.

5. How to Assess Privacy Risk

PII should be protected in every part of the deployed system. PII could leak over other systems indirectly connected to the application and evaluation system. It is important to consider all potential attack surfaces where PII can be released or compromised either directly or through secondary connected systems. Vulnerabilities include organizational risks from staff and contractors. Staff and contractors identified as having authorized access to PII shall receive proper training on data handling and storage.

The architecture diagrams used in the Concept of Operations are a good starting point for a thorough analysis of privacy risk for a particular application. The application architecture should be reflective of what is being deployed. Where multiple applications are present, it is important to identify where elements have similarities, pose a risk of conflicting objectives or are disruptive to each other. A possible approach is to analyze each application independently. The results of these analyses could be compared as part of a trade analysis to identify opportunities for synergies or conflicts. Architecture elements (terminator, processes, flows in the architecture) used by multiple applications or multiple evaluation efforts could require different levels of protection representing different PII risks. This could be an opportunity to establish a common set of controls for these architecture components to mitigate PII risks over multiple applications if it does not increase risks in other pilot or evaluation objectives.

Once the application architectures are identified, the analysis should review each architecture element for PII risks according to the appropriate objectives identified in Section 4. Each end device, data flow, and process used by the application and evaluation team should be reviewed to determine if it generates, receives, transmits, or stores any PII. Each piece of PII should support a clearly defined CV application and evaluation objectives. The result should be assessed for its C/I/A requirement to meet the goal of the application, the goal of the evaluation team, and contain the appropriate controls.

Some basic questions that can be used to frame the analysis comes from NIST SP800-53r4 as referenced in section 4. Examples of the kind of considerations, but not an exhaustive list of considerations, could include the following:

- Authority and Purpose (Control: AP)
    - Confirm the architecture element contains or utilizes PII critical for meeting the objective of the application or evaluation objectives.
- Accountability, Audit, and Risk Management (Control: AR)
- Data Quality and Integrity (Control: DI)
    - Identify the precision, accuracy, and verifiability required of the PII data to meet the objective or evaluation objectives
- Data Minimization and Retention (Control: DM)
    - Is the content of the PII the minimum needed to meet the objective or evaluation objectives?
- Individual Participation and Redress (Control: IP)

    - Did the PII owner opt in to allowing uses of their PII?
    - Is there a mechanism for the PII owner to redress their information?
- Security (Control: SE)
    - Is the PII data protected electronically?
    - Is the PII data treated with sufficient physical control?
    - Is there a mechanism to detect when PII data are accessed or released without authorization?
- Transparency (Control: TR)
    - Is there a way for the PII owner to review the information they shared with the project team?
    - Is there a clear explanation to the PII owners regarding how their information will be used?
- Use Limitation (Control: UL)
    - Is there a process where the internal uses are monitored and assured to meeting stated objectives?
    - Is there a process where external uses are monitored where allowed to insure it meets stated objectives?

Appendix A. List of Acronyms

BSM	Basic Saftey Message
C/I/A	Confidentiality/Integrity/Availability
CV	Connected Vehicle
FHWA	Federal Highway Administration
FIPP	Fair Information Practice Principles
FIPS	Federal Information Processing Standard
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
PII	Personally Identifiable Information
pPII	Potential Personally Identifiable Information
SCMS	Secure Credential Management System
SP	Special Publication
sPII	Sensitive Personally Identifiable Information
SSN	Social Security Number
VIN	Vehicle Identification Number

U.S. Department of Transportation
ITS Joint Program Office – HOIT
1200 New Jersey Avenue, SE
Washington, DC 20590

Toll-Free “Help Line” 866-367-7487

www.its.dot.gov

FHWA-JPO-17-450

U.S. Department of Transportation