How to Use the Privacy Risk Assessment Methodology (PRAM for Connected Vehicle Environment (CVE)

Introduction

The Privacy Risk Assessment Methodology (PRAM) is a voluntary tool that was developed by the National Institute of Standards and Technology (NIST) that allows decision-makers to systematically identify risks to privacy and develop appropriate solutions. The process is an on-going cycle whose iterative steps include: Framing Business Objectives and Organizational Privacy Governance; Assessing System Design; Assess Privacy Risk; Selecting Privacy Controls; and Monitoring Change. The PRAM consists of four worksheets to guide users through this process in a clear and systematic way.

- Worksheet 1 walks connected vehicle environment managers (users) through how to frame business objectives and organizational privacy governance requirements
- Worksheet 2 outlines how to assess the system design for privacy risks by identifying data actions taken by the system and related contextual factors.
- Worksheet 3 enables assessment and prioritization of privacy risks in systems by having users assign likelihood and risk estimates to each data action.
- Worksheet 4 suggests potential controls and considerations for addressing the privacy risks associated with each data action, as derived from Worksheets 2 and 3.

The PRAM for CVE

The US Department of Transportation (USDOT) worked with NIST to develop the PRAM for CVE to serve as a voluntary tool for connected vehicle technology implementers. It adapts the NIST PRAM for CVE program use by providing generic examples of PRAM content based on lessons learned from real-world connected vehicle test sites and research environments. To help organizations use the PRAM for CVE and provide project managers and planners with a starting point, the PRAM for CVE worksheets are partially pre-populated with a generic CV deployment assessment. Illustrative examples are provided where applicable.

Individual deployers can decide if and how to use the PRAM for CVE. Users can either modify the generic PRAM for CVE for worksheets or use them as a model. Either way, the entries in the generic assessment can be modified, deleted, and added to as necessary to capture and analyze the specifics of a given program or organization. Note that the generic assessment is not completely filled in. Although the nature of CV systems provides some consistency across implementations and their associated privacy risk assessments, scoring elements such as likelihood and impact is wholly dependent on individual environmental and implementation details. Therefore, the scores for such elements are left blank.

The organizational framing that takes place in Worksheet 1 includes CV-specific annotations to prompt users to consider relevant issues such as the scope of sensitive data and privacy governance. Some data actions are sufficiently common that they can be thought of as constituting a generic CV system. Those data actions, along with potential issues and associated problematic data actions and problems for individuals, are pre-populated in Worksheets 2 and 3.

Likelihoods and impacts, however, are so system-specific that it is not appropriate to pre-populate these and, by extension, prioritize risks. Irrespective of actual system-specific risk levels, it is possible to suggest recommended controls for those data actions. Ultimately, it is left to every CV program to determine which controls are desirable and feasible, those that are not, and the impact of those decisions on the system's privacy risk posture.

Additional Considerations

Privacy risk assessment, like any other form of risk assessment, typically requires some degree of appropriate privacy as well as connected vehicle technical expertise. While risk assessment instruments and tools can potentially reduce the amount of required expertise, they cannot eliminate it. An appropriate objective, therefore, is to facilitate the contributions of non-experts in terms of what the various CV systems need to achieve, while balancing the privacy needs and requirements. CV implementers will need to recognize and plan for the necessity of engaging technical privacy experts.

Worksheet 1: Framing Business Objectives and Organizational Privacy Governance

Worksheet 1 provides points to consider when framing business objectives and organizational privacy governance, and includes sample responses. It also includes an overall introduction to the PRAM and to the worksheets.

Task 1: Frame Business Objectives

Understanding the purpose and intended benefits of a system supports the selection of controls (later in Worksheet 4) that can both mitigate assessed privacy risks and support the ability of the system to meet objectives. Ideally, privacy protection would not adversely affect business performance. This worksheet contains the following sections that are partially filled out to reflect some basic Connected Vehicle Environment functionality:[1]

1. Describe the functionality of the system: This identifies the capabilities and processes the system needs to meet its objectives.
2. Describe the business needs that the system serves: This guides the selection of controls that can mitigate privacy risks without adversely affecting system performance.
3. Describe any marketable privacy-preserving functionality goals for the system: This will help to ensure that the assessment and control selection provide a basis of evidence for these claims and demonstrate the system's trustworthiness.

Example: CV environments employ a wide variety of back-end systems that provide data collection and processing functionality. The data serves a number of business needs, for instance an agency's ability to enact time-sensitive strategies for rush-hour regional mobility. An important privacy-preserving function might be to ensure "no tracking" is possible while still allowing the data to be used for real-time operational strategies.

Task 2: Frame Privacy Governance

When addressing issues related to privacy, it is important to know what levels of legal, institutional, or circumstantial (e.g., human subject research) requirements are applicable. Identifying privacy-related legal obligations and commitments to principles or other organizational policies forms the basis to understand the organization's governance structure. This helps to identify the system's privacy requirements and calculate the impact that the use of personal information has on organizational responsibilities. This worksheet contains the following sections that are partially filled out to reflect some basic Connected Vehicle Environment functionality:

1. Identify any privacy-related statutory, regulatory, contractual and/or other frameworks within which the organization must operate. List any specific privacy requirements.
2. Identify any privacy-related principles or other commitments to which the organization adheres.
3. Identify any privacy goals that are explicit or implicit in the organization's vision and/or mission.
4. Identify any privacy-related policies or statements within the organization or business unit.

[1] While the business objectives need not be identical to the Mission Objectives identified through the Cybersecurity Framework Profile, they should be consistent with them. See [Link to the CV Profile]

Example: A CV pilot project intending to collect information on the reactions or behaviors of drivers in various scenarios would need to adhere to statutory limits on human subject research, such as informed consent and limits on the collection, use, and storage of data related to the participants. Additional privacy concerns, such as the anonymity for CVs, would be subject to any privacy and security policies adopted by the organization, like the Fair Information Practice Principles (FIPPs). An organization may have internal policies also, such as supporting customer control of their own data; and individual business areas may have privacy controls as well - in the form of consent forms, etc.

Worksheet 2: Assessing System Design

Worksheet 2 helps to identify and catalog the inputs for the risk analysis (Worksheet 3). These inputs are the data actions performed by the system, the personal information (PI) processed by each data action, and relevant contextual factors. This worksheet has two tabs: Contextual Factors and Data Action Analysis.

One suggestion for using this worksheet is to consider PI broadly; not just as biographic information, but as transactional information as well, including how the system may influence the behaviors or activities of individuals.

As a starting point, fifteen distinct data actions and the PI related to them are provided, along with contextual factors and potential summary privacy issues. These should be edited, deleted, and amended as necessary to reflect accurately the system being assessed.

Task 1: Map Data Processing within the System

Data processing includes the full data lifecycle (e.g., collection, generation/transformation, use, disclosure, retention, and disposal). Data actions are information system operations that process PI. Data actions should be described at a sufficiently granular level to be useful in the risk analysis effort. Early stages of system design may preclude the ability to do this, but as the system design matures, data actions should be captured and clarified. A visual data map can be helpful in identifying data actions[2].

Task 2: Identify Contextual Factors (worksheet tab)

The Contextual Factors tab allows the user to record the circumstances surrounding the processing of PI by the system. It offers three categories (organization, system, and user) and lists considerations that may be helpful in capturing factors that could either increase or decrease the likelihood of a data action being problematic. Sample contextual factors for a generic CV system are

[2] To create a data map, the worksheet provides the following reference – "Worksheet 2: Supporting Data Map" PowerPoint; downloadable at https://github.com/usnistgov/PrivacyEngCollabSpace/blob/master/tools/risk-assessment/NIST-Privacy-Risk-Assessment-Methodology-.

provided. There also may be contextual factors that are specific to a particular data action that can be captured in the specific context column in the Data Action Analysis tab (see Task 3, below).

Task 3: Perform Data Action Analysis (worksheet tab)

The Data Action Analysis tab provides a table (pre-populated with sample data from a generic CV system) for the tracking of identified data actions, the PI used in each data action, the specific context of each action, and a summary of the potential privacy issue(s) involved in each instance.

Users might choose to consider additional factors: the duration or frequency of the data actions being taken by the system; the visibility of the data actions to the user; the relationship between data actions being taken by the system and an operational purpose (e.g., in what manner or to what degree is the PI being collected or generated contributing to the operational purpose?); and the degree of sensitivity of the PI (as a whole, or in part).

The Summary Issues column captures observations about the collected information or open questions.

Worksheet 3: Assessing Privacy Risk

Worksheet 3 provides structure for the analysis and risk assessment. Determining the privacy risk of a particular data action requires determining the likelihood that a data action will be problematic (i.e. creates the potential for adverse effects on individuals) and its impact. Users assess likelihood and impact, then calculate and prioritize risk. This worksheet uses inputs from Worksheets 1 and 2. The NIST PRAM includes a document, *Catalog of Problematic Data Actions and Problems (Catalog of PDAP),*[3] which outlines a sample set of problematic data actions and adverse effects that individuals might experience as a result. That document is a good starting point for this process.

Task 1: Assess Likelihood

Likelihood is defined as the possibility that a data action will become problematic for an individual whose PI is being used.

The Likelihood tab provides a table that lists Data Actions and related Summary Issues (both from Worksheet 2), Problematic Data Actions and Potential Problems for Individuals (both from the Catalog of PDAP), and Likelihood (the value calculated from this worksheet). Problematic data actions may create more than one type of potential problem for individuals. However, some of the problems for individuals may have a higher likelihood of occurrence than others. If the data action is scored as risky, then scoring each associated problem separately may help pinpoint what type of control would be most effective in mitigating the worst of the adverse effects, thereby lowering the score of the data action as a whole to an acceptable level.

[3] Visit the NIST Privacy Engineering Program Resource page at- https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources.

For each data action, estimate on a scale of 1-10 the probability that each potential problem will occur for individuals whose PI is being processed.

Task 2: Assess Impact

Impact is broadly defined here as the secondary costs absorbed by the organization from a data action creating a problem for an individual whose PI is being processed by the system. The Impact tab provides a table that lists Data Actions and related Summary Issues (both from Worksheet 2), Problematic Data Actions and Potential Problems for Individuals (both from *Catalog of PDAP*), and calculates a number for Business Impact Factors, and Total Business Impact per Potential Problem.

Business impact factors include noncompliance costs; direct business costs; reputational costs; internal cultural costs; and other (costs). For this analysis, users determine on a scale from 1-10 the estimated effect of each potential problem for individuals (per data action) on the business impact factors. In determining each business impact factor, relevant inputs from Worksheet 1 should be taken into account. The assigned values are added to calculate total business impact per potential problem.

Task 3: Calculate Risk

The Risk tab calculates the Risk per Data Action. For each Data Action – Potential Problem for Individuals pair, Likelihood is multiplied by Business Impact to arrive at the **Risk per Potential Problem**; then all the Risk per Potential Problem results for each Data Action are summed to give **Risk per Data Action**. One table with unspecified data actions is provided to illustrate how the calculations are done and another table prepopulated with sample data actions for a generic CV deployment is also provided, but without assigned values for the calculations.

Task 4: Prioritize Risk

Prioritization (System Risk Table and Heat Map): Indicates the estimated risk presented by a data action, its estimated percentage of system risk, and its estimated rank among data actions. The risk column is the total estimated risk per data action and colored to facilitate visual prioritization. The percent of system risk column is the estimated risk per data action relative to all other data actions. The rank among data actions column assigns relative values to the data actions pursuant to their estimated system risk percentage.

Organizations can use different methodologies to prioritize risk. The Risk Prioritization SAMPLE tab provides some examples of prioritization methods. Organizations should choose prioritization methods that provide the best communication tool for their organization and that best support their decision-making about how to respond to the identified risks. The Risk Prioritization INPUT tab provides empty tables for analyst use.

Worksheet 4: Selecting Privacy Controls

Worksheet 4 supports the selection of controls to mitigate the privacy risks identified in Worksheet 3. It requires inputs from Worksheets 2 and 3. The worksheet has two tasks.

Task 1: Propose Potential Controls

The Potential Controls tab contains two tables: one as a sample and one pre-populated with data actions for a generic CV system; and instructions for how to begin the process of identifying, evaluating, and selecting privacy controls. Using the prioritization method selected in Worksheet 3, list data actions and their associated problems in order of highest to lowest priority; then list potential mitigating technical and/or policy controls. For assistance, consult NIST Special Publication 800-53, Revision 4: *Security and Privacy Controls for Federal Information Systems and Organizations.*[4]

In the Considerations column, review what kind of effects these potential controls may have on the system functionality, users, or problems. Those entries should contain enough information to compare the potential controls, and make decisions about which are worth evaluating for implementation.

NOTE: As you populate more data actions with controls, keep in mind implementation of controls on data actions earlier in the system may have effects downstream. The Considerations column may be used to maintain these cross-references.

Task 2: Analyze Selected Controls

The Selected Controls tab lays out the process for documenting in tabular form the controls selected for each data action and the rationale behind the choice. It contains two tables: one as a sample and one pre-populated with data actions for a generic CV environment.

1. List data actions and their associated problems from the Potential Controls tab.

2. List the privacy controls selected for implementation. If no controls are selected for a particular problem or data action, enter N/A.

3. Describe the rationale for selecting the controls or leaving the risk unmitigated.

4. Populate the residual risks column with unmitigated summary issues or adjusted summary issues based on the controls selected.

5. Once the selected controls are implemented, monitor and assess them for effectiveness in managing the identified privacy risks. Reassess the residual risk acceptance determination as needed. Iterate on the worksheets as changes to the system occur.

[4] See https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

Conclusion

By offering this voluntary tool, the PRAM for CVE, we hope that CV environment implementers gain:

- A process for identifying privacy risks within and throughout their CV systems;
- A consistent language for engaging and facilitating conversations with privacy experts, technical system managers, and decision-makers on how to balance privacy with system functionality and operations; and
- A clear path to identifying appropriate controls and solutions to implement as part of their CV environments.