Privacy Risk Assessment Methodology

Worksheet 1:
Framing System Business Objectives and Organizational Privacy Governance

The Privacy Risk Assessment Methodology (PRAM) consists of four worksheets to guide users through the process in a clear and systematic way. To facilitate completion of the PRAM for Connected Vehicle Environments (CVE), each worksheet has been partially filled in with a generic CV environment assessment. Derived from discussion with pilot sites, this generic assessment provides CV deployers with a starting point for carrying out the PRAM. Deployers can either directly modify the worksheets for the generic CVE PRAM or use them as a model. Either way, it is expected that the entries in the generic assessment will be modified, deleted, and added to as necessary to capture and analyze the specifics of a given environment. Note that the generic assessment is not completely filled out as downstream aspects of it—the scoring of likelihoods and impacts, in particular—are so wholly dependent on environmental and implementation details that there is little to be gained from attempting to do so generically.

Worksheet 1 of the generic assessment (this document) provides points to think about when framing business objectives and privacy governance. While the former need not be identical to the mission objectives identified through the Cybersecurity Framework Profile for Connected Vehicle Environments (CFS Profile for CVE), they should be consistent with them. For example, some mission objectives may not be directly relevant for the purposes of privacy risk assessment while others might be usefully combined and made more general. In other cases, it might make sense to decompose a single objective into multiple, more precise ones for purposes of the PRAM.

Worksheet 2 also provides some things to think about with respect to contextual factors, while the data action analysis describes a generic CV environment. Fifteen distinct data actions are identified, together with the personal information they implicate. These are accompanied by contextual elaboration and a listing of potential summary privacy issues. These are all intended as starting points and should be edited, deleted, and amended as necessary to accurately reflect the deployment being assessed. For example, if the deployment will be capturing video of pedestrian study participants (and likely non-participants as well), data actions related to this will need to be added. Corresponding changes should be made to any corresponding data map. Note that the data actions and summary issues identified in Worksheet 2 are carried through the remaining worksheets. Deployment-specific changes to these, therefore, must also be carried through the other worksheets.

Worksheet 3 suggests problematic data actions that might be associated with the previously identified summary issues and the possible problems for individuals that could result. Each of these problems would be scored for likelihood and business impacts. However, as noted above, these are so dependent on the specifics of the deployment being assessed that the generic assessment does not attempt to score them. Once this scoring has been completed, each data action can be assigned a privacy risk score and ranked accordingly.

Worksheet 4 suggests some potential controls and considerations for addressing the privacy risks associated with each data action as represented by the unique problems for individuals associated with it. However, as throughout, these are intended only as starting points and individual deployers should alter them as necessary, including rearranging them to align with changes to the data actions. Finally, the controls actually implemented must be described.

Worksheet 1 has two tasks to complete:

1. <u>Frame business objectives -including the organizational needs served.</u> Understanding the purpose and intended benefits of a system supports the selection of controls that can mitigate assessed privacy risks while maintaining the beneficial performance. Identifying how you might highlight or market any privacy protections will help to ensure that your assessment and control selection provide a basis of evidence for these claims and demonstrates your system(s) trustworthiness.

2. <u>Frame organizational privacy governance.</u> Understand the governance structure for your organization by identifying privacy-related legal obligations and commitments to principles or other organizational policies. This will help you to identify the privacy requirements for your system and better calculate the impact of system processing of personal information on your organizational responsibilities and values for individuals' privacy.

Task 1: Frame Business Objectives

1. Describe the functionality of your system(s).

Privacy Risk Assessment Methodology

Worksheet 1:
Framing System Business Objectives and Organizational Privacy Governance

- Vehicle/vulnerable road user (VRU)/roadside unit (RSU) device capabilities
- Vehicle to vehicle/RSU/backend (direct) communication
- VRU to vehicle/RSU/backend (direct) communication
- RSU to vehicle/VRU/backend communication
- Backend system capabilities
- Backend to city/state/federal government/private sector/academia communication

2. Describe the business needs that your system(s) serve(s).

- Traffic management
- Safety
- Trust

3. Describe any privacy-preserving functionality goals for your system(s) that you may plan to market to users or customers.

- Privacy integrated into design and operation
- Participant confidentiality
- No tracking

Task 2: Frame Organizational Privacy Governance

1. Identify any privacy-related statutory, regulatory, contractual and/or other frameworks within which the organization must operate (i.e., the legal environment). List any specific privacy requirements.

Privacy Risk Assessment Methodology

Worksheet 1:
Framing System Business Objectives and Organizational Privacy Governance

- Contractual privacy and security requirements
- Local/state privacy and security statutes and regulations
- Common rule for protection of human research subjects
    - Institutional Review Board

2. Identify any privacy-related principles or other commitments to which the organization adheres (e.g., Fair Information Practice Principles, Privacy by Design principles (FIPPs), Privacy by Design).

- Inward facing privacy and security principles
- Inward facing privacy and security policies

3. Identify any privacy goals that are explicit or implicit in the organization’s vision and/or mission.

- Protecting individuals’ privacy
- Enabling individuals’ control

4. Identify any privacy-related policies or statements within the organization, or business unit.

Privacy Risk Assessment Methodology

Worksheet 1:

Framing System Business Objectives and Organizational Privacy Governance

- Outward facing privacy and security policies and notices
- Consent instruments
- Public presentations and descriptive materials