Proposal for Privacy Use Case Template Test Use Case

**HIGH LEVEL USE CASE DESCRIPTION**

1. Use Case Title

“Acme Insurance Company App to Track Vehicle Data”

2. Category of Use Case [To be established as Used Cases are submitted - may be Application categories or Model categories]

Application Type: “Mobile – Vehicular”

Model Type: “Five Domain”

3. Provide a general description of the Use Case

The Acme Insurance Company offers customers the opportunity to enroll in a program to have specific vehicular data automatically transmitted from their vehicle to the company. In exchange for data subject agreement this transmission and usage, the Acme Insurance Company offers a program of increasing reductions in the customer’s policy deductibles if specified driving patterns are recorded.

4. Provide a summary inventory for the Use Case, including:

* Application(s) associated with Use Case
  + Vehicle’s Internal Communications Application (Vehicle to Vehicle Manufacturer)
  + Vehicle Manufacturer Backend Data Collection Application
  + Insurance Company’s Data Collection and Analysis App
* Data subject(s) associated with Use Case
  + The registered Insured person associated with the vehicle VIN
* Parties and Business processes associated with Use Case
  + Customer, Insurance Company, Vehicle Manufacturer’s Vehicle Communication and Data Division, Telecom Carrier communicating vehicle data, Insurance Company’s Data Analysis Department
* Systems supporting the Use Case applications
  + Insurance Web Portal (customer interface)
  + Insurance back-end processing systems
  + Vehicle Manufacturer Data Management/Communication System
  + ….
* Products Created in Use Case
  + Raw datasets of vehicle information
  + Sub-sets of vehicle information associated with operation of the vehicle, including date/time of operation, location, speed, braking data, airbag deployment….
  + Driving evaluation assessment data derived from insurance company algorithms
  + Summary assessment information
* PI and PII covered by the Use Case
  + Registered driver name, VIN
  + linked vehicle information
  + linked driving information
  + linked evaluation assessment and summary information
  + …
* Legal, regulatory and /or business policies governing the Use Case
  + Government(s) regulations
  + Vehicle Manufacturer privacy policies
  + Telecom Carrier privacy policies
  + Insurance Company privacy policies
  + Data Subject Consent preferences
  + ….
* Privacy Policies Associated with Each Application
  + Specific policy governing “Good Driving App”

5. Provide or include link to a PIA if available

* [http://acmeinsurancegroupinc.biz/vehicle privacy/](http://acmeinsurancegroupinc.biz/vehicle%20privacy/)
* <http://BigCarCompany.biz/vehicle> privacy
* ….

-----------------------------------------------------------------------------------------------------------------

**DETAILED USE CASE DESCRIPTION**

1. Identify Participants having operational privacy responsibilities.

2. Identify the Systems where PI /PII is collected, communicated, processed, stored or disposed within a Privacy Domain.

**3.** Identify the Privacy Domains included in the Use Case together with the respective Domain Owners.

* A “Domain” covers both physical areas (such as a customer site or home) and logical areas (such as a wide-area network or cloud computing environment) that are subject to the control of a particular domain owner. Privacy Domains may be under the control of data subjects as well as other Participants
* A “Domain Owner” is the Participant responsible for ensuring that privacy controls and PMRM services are managed in business processes and technical systems within a given Domain.

4. Identify the roles and responsibilities assigned to specific Participants and Systems in each Privacy Domain in the Use Case

5. Identify the touch points at which the data flows intersect with Privacy Domains or Systems within Privacy Domains.

* Touch Points are the intersections of data flows with Privacy Domains or Systems

6. Specify the PI/PII collected, created, communicated, processed or stored within Privacy Domains or Systems in the Use Case, in three categories:

* Incoming PI/PII
* Internally generated PI/PII
* Outgoing PI/PII

7. For Incoming, Internally Generated and Outgoing PI, specify the privacy controls required/implemented to enforce the privacy policy associated with the PI/PII.

* Privacy controls are typically associated with specific Fair Information Practices Principles (FIP/Ps) that apply to the PI/PII.

8. For each category of PI/PII, specify the controls in three Control Categories:

* Inherited Privacy Controls
  + For example, controls defined by Data Subject consent
* Internal Privacy Controls
  + For example, controls defined by the business system or embedded I the application
* Exported Privacy Controls
  + For example, controls that must be implemented by a third or any external domain, system, application with which PI/PII is shared