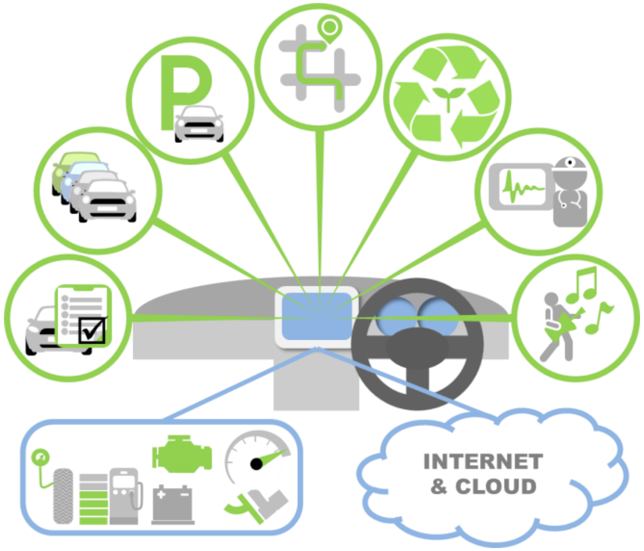
W3C Automotive WG/BG

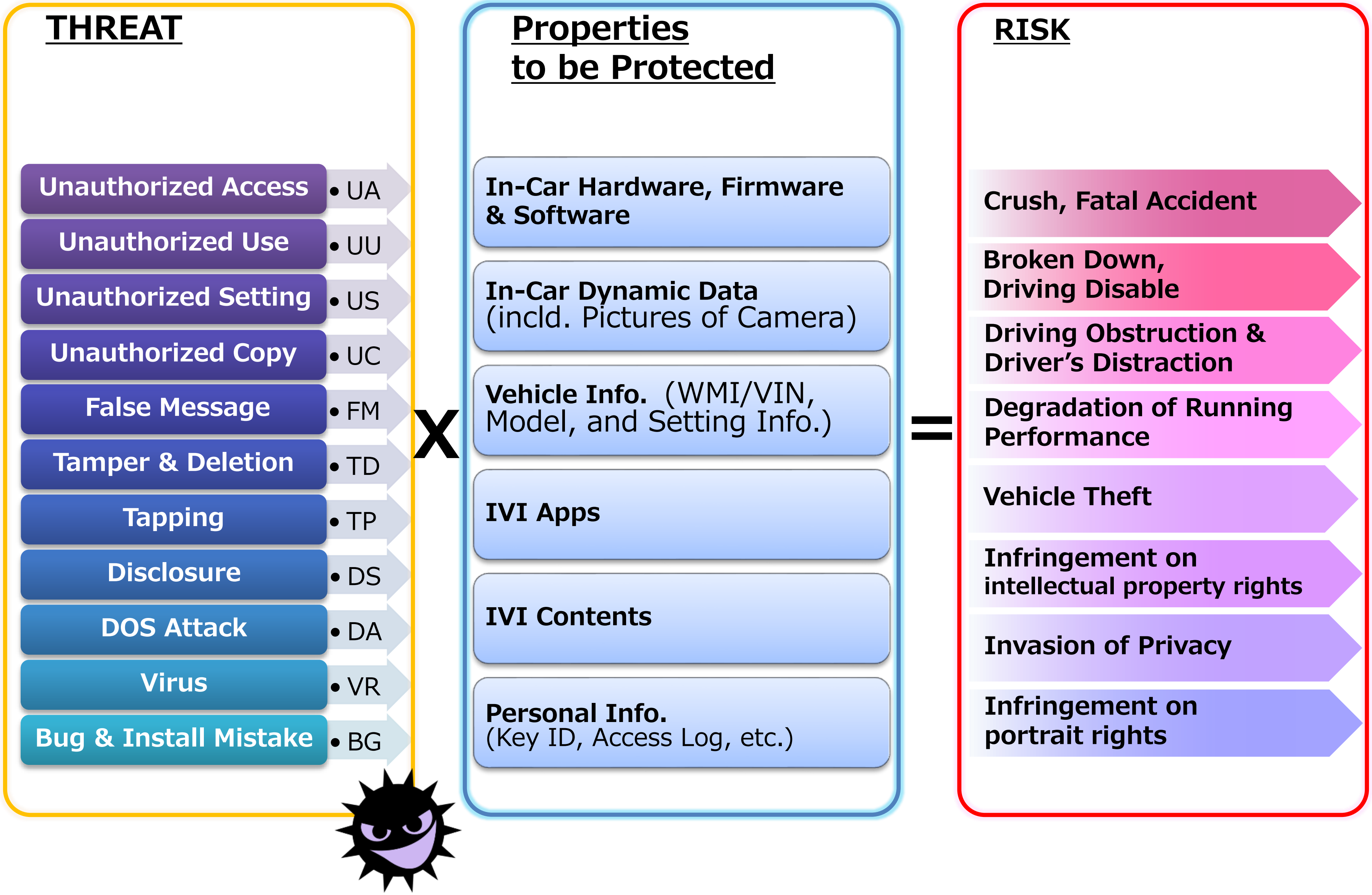
Proposed Collaborative Work Procedures for Security & Privacy Consideration (Rev.)



- Overview of Security Incidents
- Attack Vectors & Threat in Security Aspects
- Overview of Privacy Protection Functionality
- Bibliography for Privacy Framework
- Section & Process of Privacy Breach
- Proposed Procedure
  for Security & Privacy Consideration
- An Example of Case Study Sheet

KDDI Research Institute
Executive Analyst
Tatsuhiko Hirabayashi

Overview of Security Incidents



THREAT

Unauthorized Access	• UA
Unauthorized Use	• UU
Unauthorized Setting	• US
Unauthorized Copy	• UC
False Message	• FM
Tamper & Deletion	• TD
Tapping	• TP
Disclosure	• DS
DOS Attack	• DA
Virus	• VR
Bug & Install Mistake	• BG

X

Properties to be Protected

- **In-Car Hardware, Firmware & Software**
- **In-Car Dynamic Data** (incld. Pictures of Camera)
- **Vehicle Info.** (WMI/VIN, Model, and Setting Info.)
- **IVI Apps**
- **IVI Contents**
- **Personal Info.** (Key ID, Access Log, etc.)

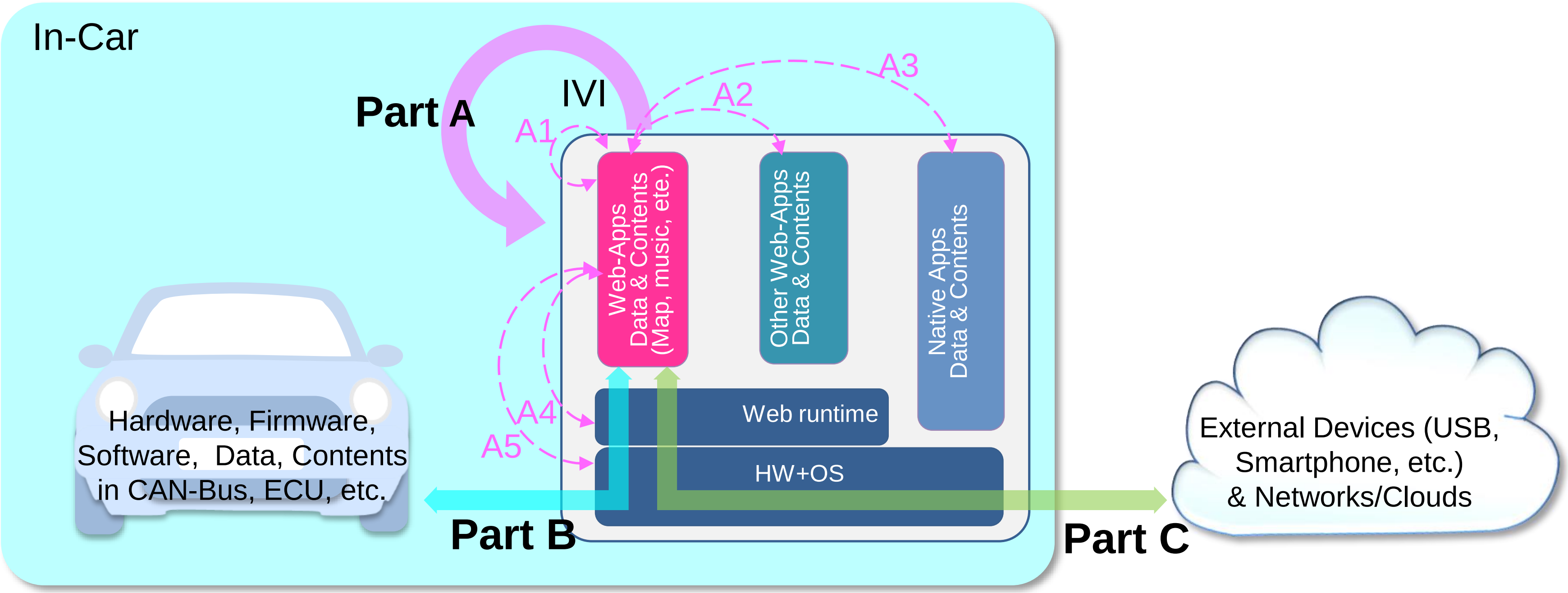
=

RISK

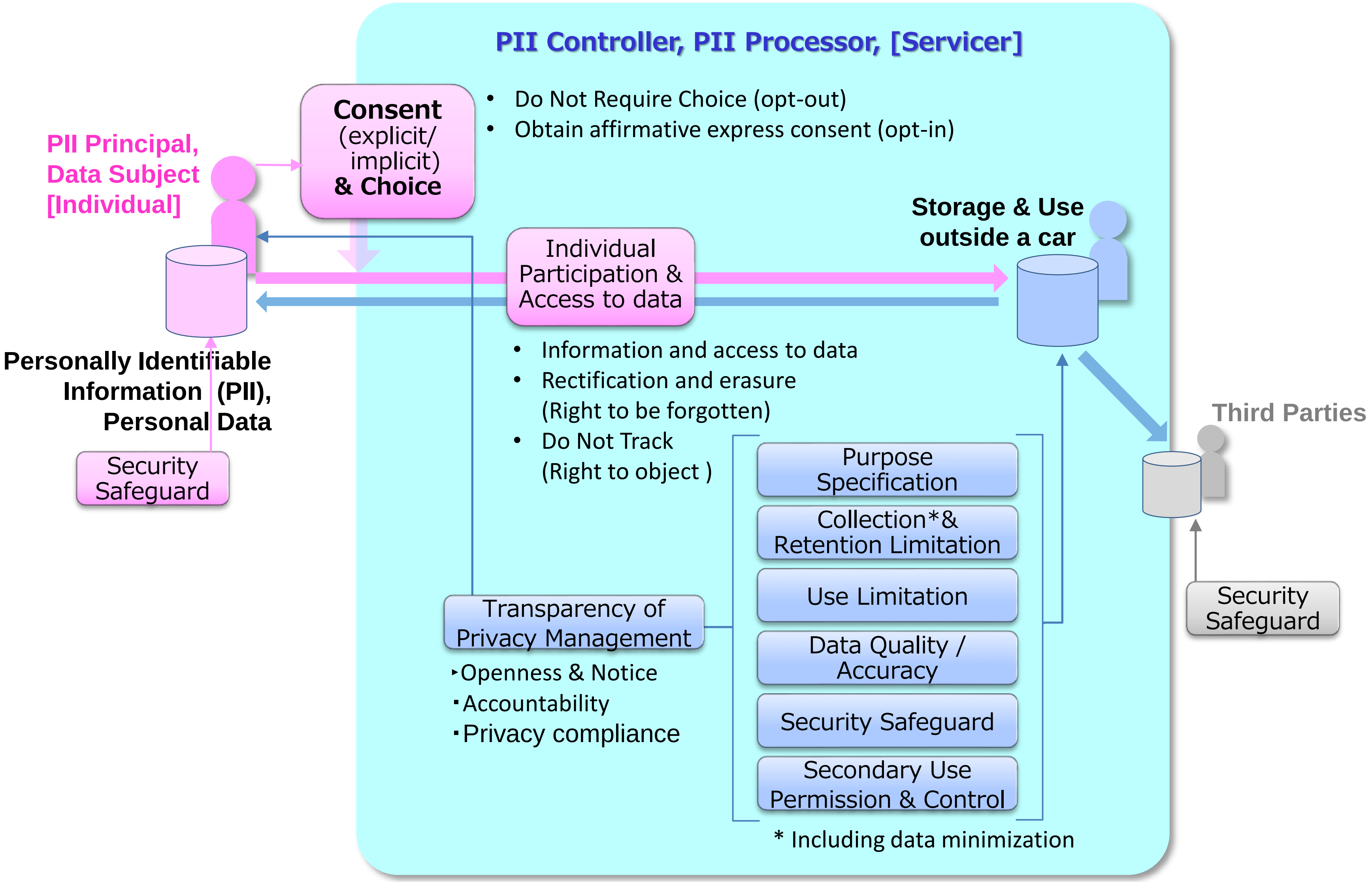
- **Crush, Fatal Accident**
- **Broken Down, Driving Disable**
- **Driving Obstruction & Driver's Distraction**
- **Degradation of Running Performance**
- **Vehicle Theft**
- **Infringement on intellectual property rights**
- **Invasion of Privacy**
- **Infringement on portrait rights**

Attack Vectors & Threat in Security Aspects

	UA	UU	US	UC	FM	TD	TP	DS	DA	VR	BG
Part A: Intra-IVI											
A1: Web apps		✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
A2: Apps to Apps	✔	✔	✔		✔	✔		✔	✔	✔	✔
A3: Apps to Native Apps	✔	✔	✔		✔	✔			✔	✔	✔
A4: Apps to WRT	✔		✔		✔	✔			✔	✔	✔
A5: Apps to IVI OS	✔		✔		✔	✔			✔	✔	✔
Part B: IVI to In-Car	✔	✔	✔		✔	✔	✔		✔	✔	✔
Part C: IVI to External Devices	✔	✔	✔		✔	✔	✔	✔	✔	✔	✔



Overview of Privacy Protection Functionality



PII Controller, PII Processor, [Servicer]

PII Principal,
Data Subject
[Individual]

Consent (explicit/ implicit) **& Choice**

- Do Not Require Choice (opt-out)
- Obtain affirmative express consent (opt-in)

Individual Participation & Access to data

- Information and access to data
- Rectification and erasure (Right to be forgotten)
- Do Not Track (Right to object)

Storage & Use outside a car

Personally Identifiable Information (PII), Personal Data

Security Safeguard

Third Parties

Security Safeguard

Transparency of Privacy Management

‣Openness & Notice
▪Accountability
▪Privacy compliance

Purpose Specification

Collection*& Retention Limitation

Use Limitation

Data Quality / Accuracy

Security Safeguard

Secondary Use Permission & Control

* Including data minimization

LEGEND: 🟪 🟦 ⬜ Key Functions mainly derived from ISO/IEC 29100

Bibliography for Privacy Framework

KDDI Research Institute

- **ISO/IEC 29100:2011**
  - **Information technology — Security techniques — Privacy framework**
    http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=45123
- **OECD**
  - **THE OECD PRIVACY FRAMEWORK**
    http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm

THE OECD PRIVACY FRAMEWORK

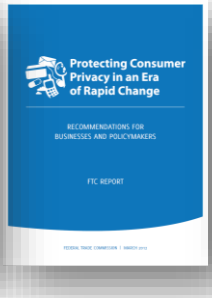
OECD 2013

- **EU**
  - **DIRECTIVE 95/46/EC**
    The protection of individuals with regard to the processing of personal data and on the free movement of such data
    http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN
  - **Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)**
    http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf
- **APEC**
  - **APEC PRIVACY FRAMEWORK**
    http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx2015
  - **APEC Privacy Framework Stocktake: Comparative review against 2013 updates to OECD Privacy Guidelines**
    http://mddb.apec.org/Documents/2015/ECSG/DPS1/15_ecsg_dps1_006.pdf
- **US**
  - **CONSUMER DATA PRIVACY IN A NETWORKED WORLD**
    https://www.whitehouse.gov/sites/default/files/privacy-final.pdf
  - **ADMINISTRATION DISCUSSION DRAFT CONSUMER PRIVACY BILL OF RIGHTS ACT**
    https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf
  - **FTC REPORT: Protecting Consumer Privacy in an Era of Rapid Change**
    https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf
  - **FTC Staff Report: internet of things Privacy & Security in a Connected World**
    https://www.ftc.gov/sites/default/files/documents/public_events/internet-things-privacy-security-connected-world/final_transcript.pdf
- **Japan**
  - **Act on the Protection of Personal Information**
    http://www.japaneselawtranslation.go.jp/law/detail_main?id=130&
  - **Bill to revise the Act on the Protection of Personal Information submitted at the 189th ordinary Diet session in Japan**
    http://www.cas.go.jp/jp/houan/189.html
    (Japanese Only)

APEC PRIVACY FRAMEWORK

CONSUMER DATA PRIVACY IN A NETWORKED WORLD:
A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY

FEBRUARY 2012



Protecting Consumer Privacy in an Era of Rapid Change

RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS

FTC REPORT

internet of things
Privacy & Security in a Connected World

FTC Staff Report

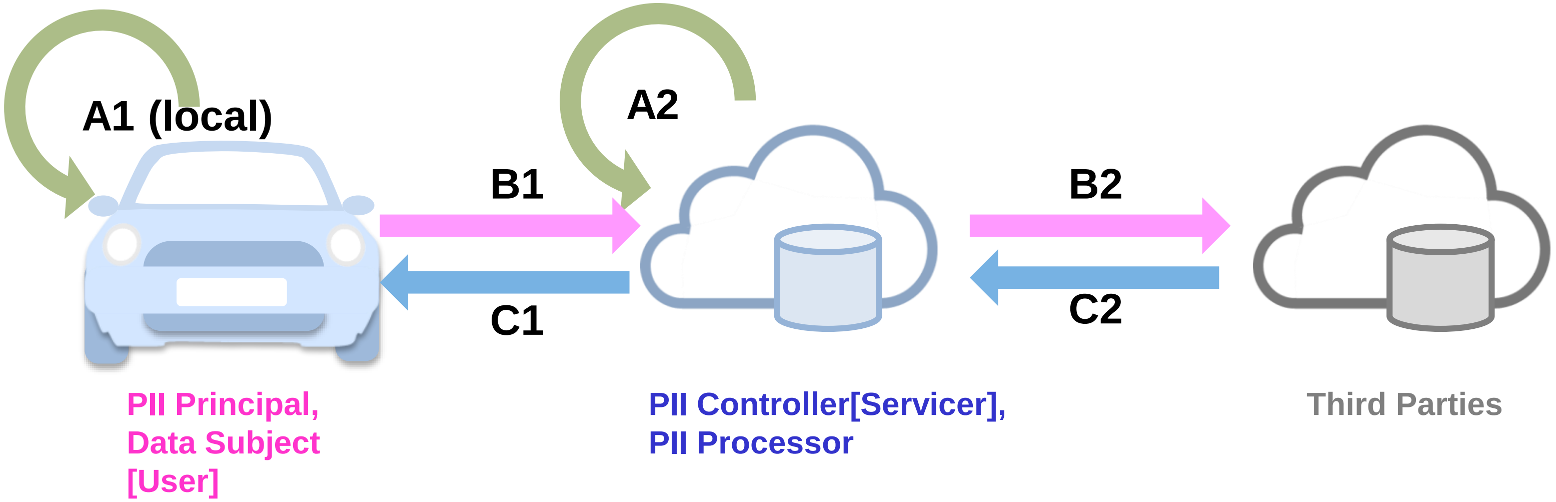
Section & Process of Privacy Breach

	A1	A2	B1	B2	C1	C2
Consent & Choice	✔	✔	✔	✔		
Individual Participation & Access	✔	✔	✔	✔	✔	✔
Purpose Specification	✔	✔	✔	✔	✔	✔
Collection & Retention Limitation	✔	✔	✔	✔	✔	✔
Use Limitation	✔	✔	✔	✔	✔	✔
Data Quality / Accuracy	✔	✔	✔	✔	✔	✔
Security Safeguard	✔	✔	✔	✔	✔	✔
Secondary Use Permission & Control	✔	✔	✔	✔	✔	✔
Transparency of Privacy Management	✔	✔	✔	✔	✔	✔

- **PRIVACY RISK**

  Physical, mental and economic injury by followings :

  - social discrimination
  - Privacy breach



Proposed Procedure
for Security & Privacy Consideration

1. **List up brief use cases and concerns using spreadsheet[1]**

   [1] https://docs.google.com/spreadsheets/d/14ij-2I-H4HbilVQ_muCmUayVqmVfdbkoke690MA0kdo/edit#gid=0

2. **Select gathered use cases & concerns in STEP 1 for our scope and investigate them deeply adding the following contents to the above spreadsheet etc.**

   (See the attached sample on an One-sheet-one-incident basis)
   - Part ID
     - A1-A5, B, C in slide 3 for security
     - A1,A2, B1,B2, C1, C2 in Slide 6 for Privacy
   - Actors
   - Attack Vector & Type of Threat for Security (From X to Y, or internal)
   - Actual or Envisioned Incident
   - Requirements
   - Best Practice and desirable measures in Web layer (if possible)
   - Remarks & Bibliography

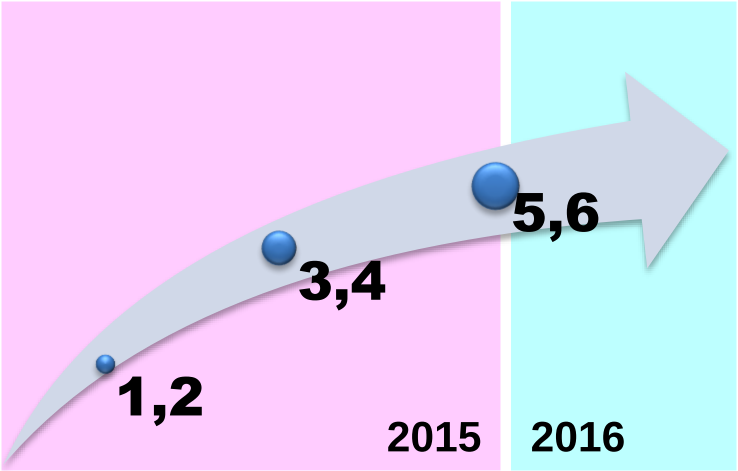
3. **Derive requirements from the investigation**

<Iterate the above steps 1-3 twice or more>

4. **TF members and other working groups, to exchange and discuss case studies in the sheet, focusing on the automotive web technologies.**

5. **Moderator and editor, to draft findings and recommendation from the work sheet, and to clarify issues to be discussed beyond LC/CR timing.**

6. **TF member, to generate the technical descriptions in the specs by year end of 2015. (to be in time for LC/CR)**



An Example of Case Study Sheet

Serial#000-R00	Part	Attack Vector (From)	Attack Vector (To)	Threat
------------------------------				
------------------------------				

for Security Incident

Use Case Title:

Actors:

Concerns:

Use Case Diagram

Best Practice and desirable measures in Web layer (if possible)

(Key words of measures)

Remarks & Bibliography

Edit record