

# [ Applying Privacy-by-Design to **Speed Profiles** Using the ICO Handbook

Nol Venema (Technolution)

# Context

## See

- Presentation made by telephone by Judith Jones, ICO on privacy by design.

[http://www.esafetysupport.org/download/eSafety\\_Activities/eSafety\\_Working\\_Groups/eSecurityWG/Article29mtg021209/eseurity\\_20091202\\_a\\_privacydesign\\_2.pdf](http://www.esafetysupport.org/download/eSafety_Activities/eSafety_Working_Groups/eSecurityWG/Article29mtg021209/eseurity_20091202_a_privacydesign_2.pdf)

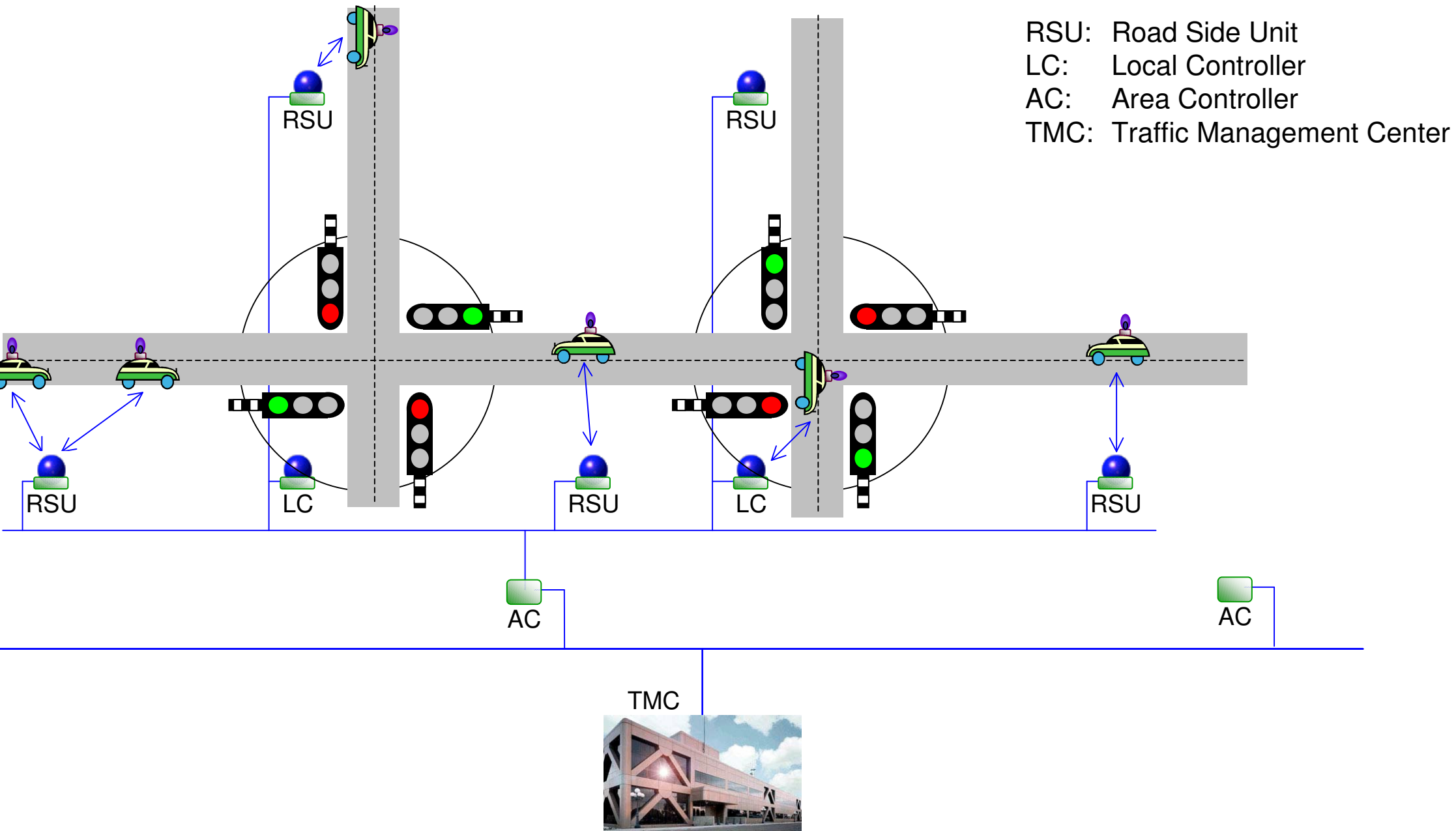
- Document prepared by Antonio (eSecurity\_2010-05-12\_Privacy By Design ICO.ppt)

■ Template includes empty sections (in red) to fill out

■ Everything in italics are phases that are skipped

- Mentioned for the sake of completeness

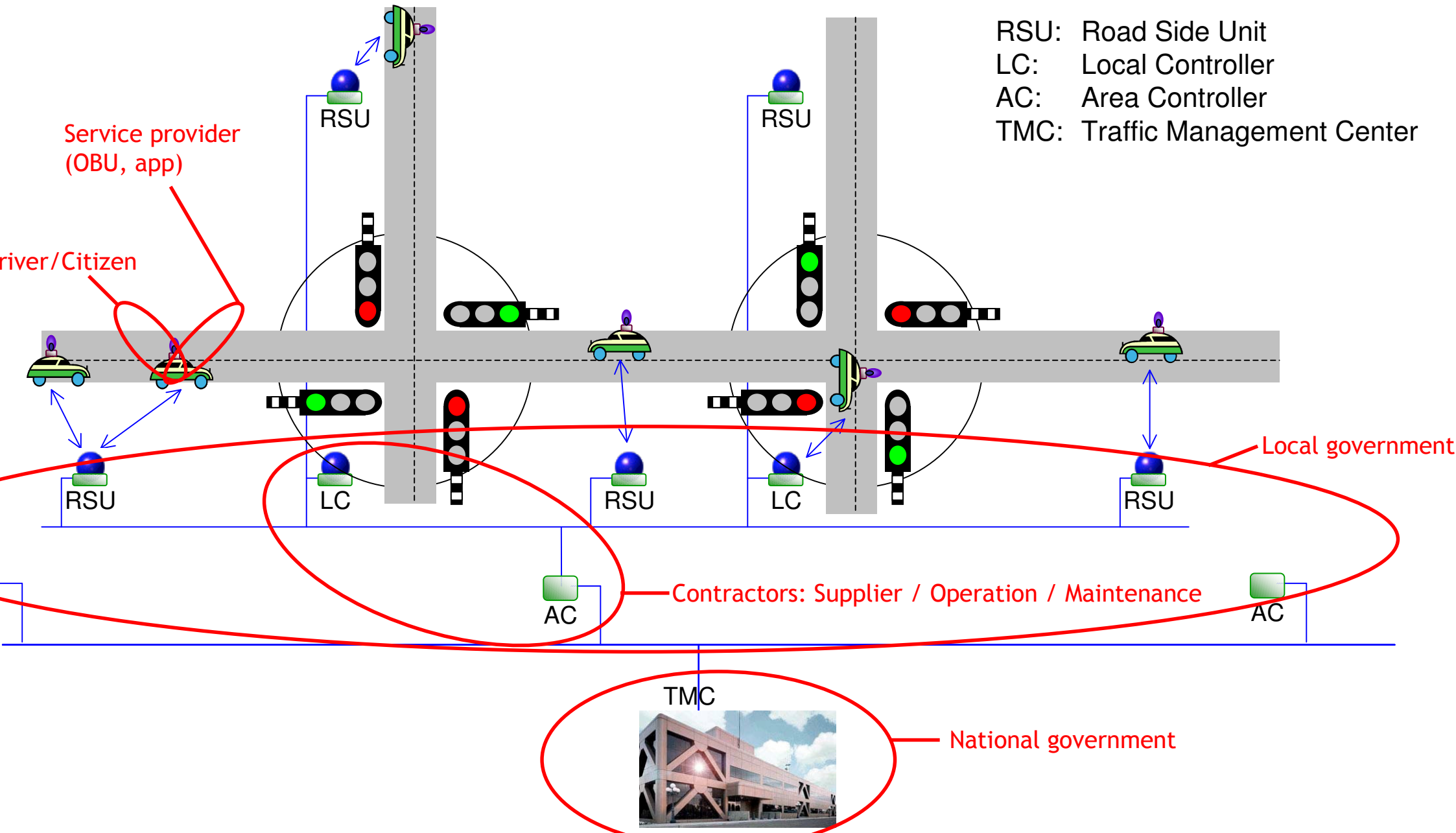
# Project Outline - Image



# [ Project Outline

- Harmonize traffic flow at intersections
  - Motivation:
    - » Better throughput / comfort / safety
    - » Environmental benefit
  - Concept:
    - » LC receives FCD from vehicles
    - » LC processes the data and builds a local map
    - » LC calculates optimal switching plan
    - » LC sends individual speed profiles back to vehicles
    - » LC forwards FCD to AC
    - » AC builds a global map
    - » AC sends LCs optimal global parameters
    - » AC archives data for analysis
    - » AC forwards aggregated data to TMC
    - » TMC archives data

# Stakeholder Analysis



# [ What Else

- ITS Directive
- EDPS Opinion on BAT
- eSecurity - Article 29WG joint meetings
- CVIS framework, architecture, ecosystem

# PIA Screening

1 Does the project apply new or additional information technologies that have substantial potential for privacy intrusion?

- **Yes:**
  - » Application uses GPS for the vehicle location;
  - » Communication between vehicle and roadside systems;
  - » Storing data for improving the systems.

2 Does the project involve new identifiers, re-use of existing identifiers, or intrusive identification, identity authentication or identity management processes?

- **Yes: Vehicle ID for short range tracking of vehicles.**

3 Might the project have the effect of denying anonymity and pseudonymity, or converting transactions that could previously be conducted anonymously or pseudonymously into identified transactions?

- **Yes, it might.**

4 Does the project involve multiple organisations, whether they are government agencies (eg in 'joined-up government' initiatives) or private sector organisations (eg as outsourced service providers or as 'business partners')?

- **Yes: public authorities, service providers, maintenance organisations.**

5 Does the project involve new or significantly changed handling of personal data that is of particular concern to individuals?

- **No. Processed data is not of class 'sensitive personal data' (racial, ethnical, ...).**

# PIA Screening

6 Does the project involve new or significantly changed handling of a considerable amount of personal data about each individual in the database?

- No, this application does not deal with a considerable amount of personal data.

7 Does the project involve new or significantly changed handling of personal data about a large number of individuals?

- Yes, data will be processed for every vehicle passing (and the appropriate OBU installed).

8 Does the project involve new or significantly changed consolidation, inter-linking, cross-referencing or matching of personal data from multiple sources?

- No, the project scope does not consider this.

9 Does the project relate to data processing which is in anyway exempt from legislative privacy protections?

- No, the project deals with traffic management and is not involved with law enforcement.

10 Does the project's justification include significant contributions to public security measures

- No, there is no relation with public security.

11 Does the project involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable privacy regulation?

- No, the selected contractor will be subjected to the national privacy regulation.

[ Full PIA is needed?

# [ *Next Screening Steps*

- *Privacy law compliance check*
- *Data protection compliance check*
  - *Template is based on the UK law*
  - *More appropriate for the data controller*
  - *Not for the supplier (he can second guess)*

# [ PIA

- Preliminary Phase
- *Preparation Phase*
- Consultation and analysis Phase
- *Documentation Phase*
- *Review and Audit Phase*

# [ Preliminary Phase

- *Review preliminary phase*
- *Update project outline*
- *Resource planning*
- *Preliminary discussion*
- Preliminary analysis of privacy issues
  - Vehicle ID
  - Tracking location, speed
  - Using electronic communication
  - Store data for offline research

# [ Preparation Phase

## ■ Consultation plan

- Local government (cities);
- Traffic management companies (traffic light operation, maintenance);
- National government (TMC);
- Service provider OBU;
- Drivers?

# [ Consultation and analysis Phase

- *Re-consider the design options*
- **Select a design**
  - Anonymisation / pseudonymisation (FCD data)
  - Data minimisation (FCD data)
  - Logical access control (systems)
  - Encryption (communication)
  - Policy enforcement for storing data
- *Provide the design features to the*
  - *PCG (PIA Consulting Group)*
  - *Project team*

# [ Documentation Phase

- *Final document*
- *PIA report*
- *Make PIA available to PCG*
- *Publish PIA report*
  - *Could add the privacy law compliance study*
  - *Could add the data protection act compliance study*

# [ Review and Audit Phase

- *Undertake review*
- *Prepare review report*
- *Present report to PCG*
- *Make report public*

[ Thanks