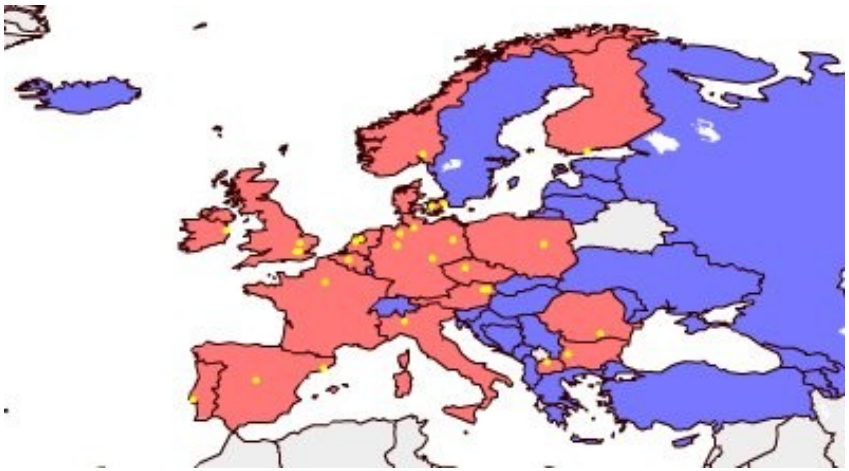
EU Data Protection and the Internet of Thigs

Andreas Krisch <andreas.krisch@edri.org>
www.edri.org

European Digital Rights - EDRi

- Association of European Digital Rights Associations
- founded in 2002
- 28 Member Organisations
- 18 European Countries



- bi-weekly newsletter EDRi-gram since 2003
- German edition since 2006 at www.unwatched.org

Agenda

- News from EU RFID data protection
  - Privacy Impact Assessments
  - Definition of personal data
- EC Internet of Things Expert Group
  - Requirements for RFID data protection
- Data breach notifications
- The EU data protection reform
  - Leaked documents

News from EU RFID data protection

2004: RFID meets society

RFID data protection

- 2007: EC RFID Expert Group (2007 - 2009)
  - On data protection and security
  - Industry, trade unions, consumer orgs, DPAs, standardisation bodies, EDRi, ...
  - Discussing requirements for RFID data protection
- 2008: RFID Logo

Quellen: FoeBuD; Informationsforum RFID

RFID data protection (2)

- 2009: EC Recommendation on RFID data protection
  - Privacy Impact Assessments
  - Retail: mandatory deactivation at POS
  - Transparency (RFID Logos; info on application)
- 2011: RFID Privacy Impact Assessment
  - Self regulation
  - Endorsed by Article 29 Working party (WP 180)
  - Signed by industry and European Commission
  - Risk assessment approach

RFID data protection (3)

- Article 29 Working Party (WP 175)
  - „if the tag is carried by a person [...], and if the tag contains a unique ID, then by definition the tag contains personal data“
  - „regardless of the fact that the “social identity” (name, address, etc.) of the person remains unknown“
  - “… even in those cases where a tag contains solely a number that is unique within a particular context, ..., care must be taken to address potential privacy and security issues if the tag is going to be carried by persons.“

EC Internet of Things Expert Group

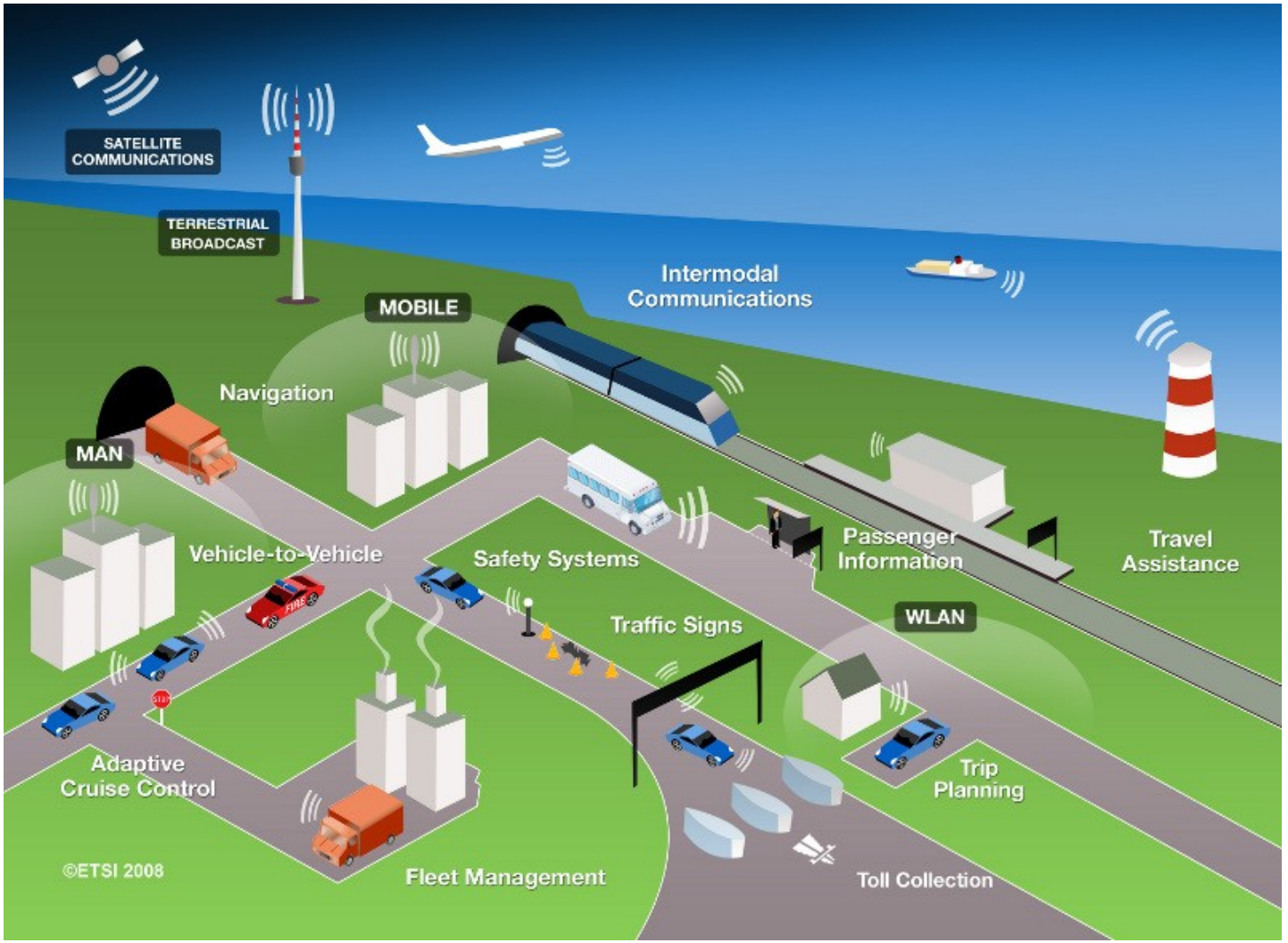
EC IoT Expert Group

- 2010 – 2012
- Stakeholder involvement
  - Industry, standardisation bodies, consumer organisations, DPAs, IT security orgs, EDRi, …
- Internet of Things
  - *… a global network infrastructure, linking physical and virtual objects through the exploitation of data capture and communication capabilities ...*
  - *… independent cooperative services and applications ...*
  - *… high degree of autonomous data capture ...*

e.g. Smart Metering

Quelle: EVB Energie AG; CC-BY-SA 3.0
http://de.wikipedia.org/w/index.php?title=Datei:Intelligenter_zaehler-_Smart_meter.jpg

e.g. Intelligent Transport Systems



Quelle: ETSI

IoT data protection: challenges

- Automatic object identification may lead to automatic identification of persons
  - Collection of information based on object IDs, sensor data, connection capabilities
  - May reveal information on individuals, their habits, location, interests, …
  - Traceability / profiling / unlawful processing, authentication and trust in the objects
- Combination of data
  - From different sources / services + data mining
  - Might create new knowledge on individuals

IoT data protection: challenges (2)

- With IoT
  - Already existing data protection problems become even more pressing
  - Due to autonomous collection, processing and communication of data
  - By “intelligent” objects with only limited computing power

IoT data protection: challenges (2)

- Data subject's rights
  - Individuals will often not be aware of IoT-systems and processing of personal data
  - How to ensure, that no unwanted processing of personal data takes place?
  - How to inform individuals?
- Data protection principles
  - How to ensure data minimisation, purpose limitation, … with autonomously operating and communicating objects?

IoT data protection: objectives

- Effective personal data protection entailing
  - Application of legal principles
  - Accountability
  - Enforcement
- A concept or tool is needed
  - Minimize privacy-, data protection-, security-risks
  - For citizens, customers, third parties

IoT data protection: objectives (2)

- Ensure that
  - Individuals remain in control of their personal data
  - IoT systems provide sufficient transparency to enable individuals to exercise their rights
  - Information on IoT systems can also be understood by the average individual, not familiar with IoT
  - A clear and non-discriminative choice exists, where processing takes place based on consent
- Increase
  - Harmonisation and level of enforcement of DP law

IoT data protection: measures

- Privacy, data protection & security risk assessments
- Catalogue of best practices & common risks
- DP as design goal for IoT systems
- Technical measures for better data protection
  - e.g. privacy policies that can – on user level – be pushed inside the objects
- Better harmonisation of DP legislation
  - + coherent application & better enforcement

IoT data protection: measures (2)

- Bring Privacy by design to practice
  - Incl. Data minimisation & data deleting
- Enhance possibilities to exercise data subject's rights
  - Clear, easily understandable information on IoT data processing needs to be provided
  - Effective mechanisms to make individuals aware of the processing, the identity of the processor and the purposes of the processing need to be found

IoT data protection: measures (3)

- Strengthen DPAs
- Introduce significant sanctions for DP violations
- Extend data breach notifications to all areas
- Make appointment of data protection officers mandatory
- Clarify requirements for valid informed consent
- Clarify definition of personal data
- Make DP mandatory design goal in standardisation

The EU data protection reform

The EU data protection reform

- Current DP directive adopted in 1995
- EC drafts reform documents
- Leaked documents
  - General Data Protection Regulation
    http://statewatch.org/news/2011/dec/eu-com-draft-dp-reg-inter-service-consultation.pdf
  - Police and Criminal Justice Data Protection Directive
    http://www.statewatch.org/news/2011/dec/ep-dp-leas-draft-directive.pdf

The EU data protection reform (1)

- Better harmonisation
- Clarification of field of application
  - "... activities of an establishment of a controller or a processor in the Union"
  - "... where processing activities are directed to data subjects residing in the Union ..."
- Binding corporate rules
  - For processing outside of the Union
- Significant access barriers for foreign LEAs

The EU data protection reform (2)

- Data Protection Officers
  - Mandatory for companies > 250 employees if core activity is not related to processing of personal data
- Informed consent
  - Not a legal basis for processing if significant inbalance – in terms of dependency – exists between data subject and controller
- Right to be forgotten; right to deletion
- Right to data portability

The EU data protection reform (3)

- Mandatory data breach notifications
- DPAs
  - Clear(er) definition of powers & independence
  - Increased powers
  - Definition of co-operation between DPAs
  - Increased powers of Art. 29 WP → DP Board
- Increased sanctions
  - Depending on severity up to 5% of global annual turnover

EU data protection reform (4)

- Time schedule
  - 25.01.2012: Official publication of draft legislation
  - Public consultation
  - Discussion in European Parliament & council
  - Loads of lobbyism, spinning & twisting
  - Adoption probably by end of term of EP (2014)
  - Transition period: ~ 2 years

www.zeichnemit.at

Thank you for your attention!

Andreas Krisch

andreas.krisch@edri.org

www.edri.org

European Digital Rights AISBL

IBAN: BE32 7330 2150 2102

BIC: KREDBEBB