Internet of Things: privacy and security challenges

16 December 2015 – MILAN
IEEE World Forum on Internet of Things

Avv. Luca Bolognini
President, Italian Institute for Privacy
Founding Partner, ICT Legal Consulting
Board, Privacy Flag
THE DATA PROTECTION OF THINGS

- ART. 29 WP OPINION 8/2014 ON THE RECENT DEVELOPMENTS ON THE INTERNET OF THINGS
- DATA TRANSFER
- PROFILING
- DATA SUBJECT’S RIGHTS
- BIG DATA
- DATA PROTECTION IMPACT ASSESSMENT
- PURPOSES LIMITATION
- DATA PROTECTION BY DESIGN
- PROPORTIONALITY

ICT LEGAL CONSULTING
Privacy Flag
Istituto Italiano Privacy
And the Privacy of Things?

The IoT requires a fusion between those two rights that now are theoretically separated.

- Not just a matter of data processing
- But also a potential risk for private and family life (e.g. Home environments)
- Habeas Data (Rodotà)
Digital Subconscious: subjects ignore newborn data related to them and impacting on them

Profiling and algorithmic procedures → Monitoring Categorisation Clustering Massive analysis → Impacts on real life and human beings

DATA PROTECTION IMPACT ASSESSMENTS

In order to maintain the security and to guarantee the accountability, it must be carried out by the data controller “where a type of processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk for the rights and freedoms of individuals, such as discrimination, identity theft or fraud, financial loss, damage to the reputation, unauthorized reversal of pseudonymisation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage” (GDPR, Article 33(1)). It shall contain “at least a general description of the envisaged processing operations, an evaluation of the risk [...] the measures envisaged to address the risk including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned”.

NEED FOR AN IMPACT-BASED APPROACH, NOT FORMALISTIC

Pseudonymization or Anonymization?

Accountability principle should suggest a strong pseudonymization because impacts on individuals can derive even from anonymous data processing (the WW2 “Targeting Committee on Kyoto” case is a good metaphor).
Increase the **trust, efforts from the controller’s side**

**Data protection by design**
It consist in the controller's implementation of “technical and organisational measures appropriate to the processing activity being carried out and its objectives, such as data minimization and pseudonymisation, in such a way that the processing will meet the requirements of [the] Regulation and protect the rights of (... data subjects” (GDPR, Article 23(1))

**Privacy by Default**
Essentially, “*the controller shall implement appropriate measures for ensuring that, by default, only (...) personal data (...) which are necessary for each specific purpose of the processing are processed*” (GDPR, Article 23(2)).

**Privacy enhancing technologies**
Speaking of IoT, the respect of data protection right is not sufficient. These technologies must ensure also the safeguard of private and family life in terms of private sphere

---

**High level of details in the information notice but in a simple and user-friendly way**
Enable effective and potentially automated exercise of data subject’s rights
Application of the **right to data portability** (GDPR, Article 18)
Self(ie) Control: empower the users/data subjects

1. Crowd-privacy alerts and opinions: “unity makes strength”;
2. Automation of the self-protection (self(ie)control – e.g. Privacy Flag tools).
3. Combine the end-user awareness with the cooperation of tech-companies so as to marginalise the intervention of data protection authorities and reduce the regulation, preferring best practices (e.g. privacy by default, cybersecurity), certifications and codes of conduct.
Next “Internet of ?” challenges

- 3D DATA PROTECTION
- Internet of food, toys, jewels etc
- Internet of Blood/cells
- Nano-Internet
- Holography
- Internet of Thoughts
- Personal Effects Protection
- Expert health analytics
- IoT for financial services (borrower companies’ stocks and means monitoring)
THANK YOU!

For further questions or clarifications:

lucabolognini@istitutoitalianoprivacy.it

luca.bolognini@ictlegalconsulting.com