Internet of Things: privacy and security challenges

2 June 2016
IoTWeek 2016 - Belgrade

avv. Luca Bolognini

President, Italian Institute for Privacy
Founding Partner, ICT Legal Consulting
Board member, Privacy Flag H2020 Project
New GDPR + Art. 29 WP Opinion 8/2014 on the Recent Developments on the Internet of Things

THE DATA PROTECTION OF THINGS

- RIGHT TO OBJECT TO PROFILING
- DATA MINIMIZATION
- PROPORIONALITY
- DATA PROTECTION IMPACT ASSESSMENT
- PURPOSES LIMITATION
- DATA PROTECTION BY DESIGN
- DATA PORTABILITY
- BIG DATA PROTECTION
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 25(1))

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 20)

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 25(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.
Increase the **power, efforts from the subject’s side**

In IoT several obstacles for traditional data protection rules:
1. Often objects «without a face» (screens, dashboards, user visual interfaces)
2. Often many data controllers/processors
3. Silent data collection and dissemination/re-use

**Digital Subconscious:** subjects are often non-users and ignore newborn data related to them and impacting on them

**NEED FOR NEW SELF-CONTROL/SELF DEFENCE TOOLS AND FEATURES FOR IOT ENVIRONMENT, DIRECTLY IN THE HANDS OF DATA SUBJECTS**
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)

**IoT:**

**Article 8: Right to respect for private and family life - ECHR**
1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

**Article 7: Respect for private and family life**
Everyone has the right to respect for his or her private and family life, home and communications.

**Article 8: Protection of personal data**
1. Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority.

**Article 12 of Universal Declaration of Human Rights**
No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks. (also Article 16, Convention on the Rights of the Child and Article 23, Convention on the Rights of Persons with Disabilities)
Next IoT “data protection” challenges

- Internet of Toys: minors smart protection
- Home cybersecurity
- Personal anti-radar/misleading tools
- Cloaks
- Objects search engines
- bloTech protection
- Sticky policies (Personal data right management linked to data sets)
- Personal Effects Protection
THANK YOU!

l.bolognini@istitutoprivacy.it

luca.bolognini@ictlegalconsulting.com