ICT LEGAL CONSULTING
BALBONI BOLOGNINI & PARTNERS

*Connected Smart Cities Conference*

*Brussels – 12 January 2017*

# *ETHICS & PRIVACY ASPECTS IN SMART PROJECTS*


**Luca Bolognini**
*Lawyer, Independent Ethics & Privacy Advisor*
*President of the Italian Institute for Privacy and Data Valorisation*
*Rome, Italy*
*l.bolognini@istitutoprivacy.it*


Istituto Italiano per la Privacy e la Valorizzazione dei Dati

# Smart Citizens/IoT Subjects as ”non-users”

People's data are **key elements** in order to design effective and smart policies and services for citizens, in their own interest and for the global goods.

However, Big Data collected from cities' IoT environment can **impact** on citizens' life, freedom and rights: **ethical and privacy implications** could either be positive or negative for involved people, often unaware of ongoing data collection/processing and of any likely related consequences, acting de facto as "**non-users**".

# Some privacy/personal data/ethical risks in a smart environment

- Intruding into private life
- User identification
- Data transmission to unauthorized thir parties
- Geo-location
- Data dissemination
- Data transfer outside the EU
- Excessive data retention
- Incompatible data reuse
- Cybersecurity risks (evil use of the facility)
- Risk of losing, hacking, pirating, falsification or interception data,
- Disclosure of sensitive data (e.g. health care, sexual orientation etc.)
- Behavioural monitoring
- "Digital subconscious": data mining could generate newborn data processing, unknown and unsuspected even by data subjects
- Discriminating decisions
- Silent impacts/effects on citizens' life

Istituto Italiano per la Privacy e la Valorizzazione dei Dati

ICT LEGAL CONSULTING
BALBONI BOLOGNINI & PARTNERS

# Smart City/IoT data controllers/processors as ”non-subjects” (but ”objects”)

To complicate things… Things can automatically process, mine, exchange, analyze personal data and take decisions without human intervention.

The “**accountability of many objects**” can be challenging…

# OrganiCity and Privacy Flag: 2 interesting cases

H2020 Projects like **OrganiCity** and **Privacy Flag** are exploring interesting best practices in this sense, based on a "tridimensional approach“ to E&P, including

- crowd sourced privacy tools and assessments
- prior Ethics & Privacy Impact/Compliance Evaluations
- users/non-users self-data-protection enablers

Taking into account that personal data processing for archiving purposes in the public interest, scientific or historical research or statistical purposes can be lawful (according to Recital 156 and Section 89 GDPR) but it should be subject to appropriate safeguards for the rights and freedoms of the data subject.

# Key steps of the Ethics & Privacy Strategy in a Smart Project

1. Identify the main phases of the project, which are relevant for privacy/data protection or ethics
2. Identify the key privacy/data protection/ethics issues related to each phase of the project
3. Outline a strategy to tackle the identified issues

Istituto Italiano per la Privacy e la Valorizzazione dei Dati

ICT LEGAL CONSULTING
BALBONI BOLOGNINI & PARTNERS

# Keywords:
# Assessment, Minimization
# Awareness, Empowerement

All the possible effects (and side effects) of an advanced smart city/IoT application should be cautiously assessed, trying to minimize the risks for individuals while strengthening their awareness and empowerment. Also positive effects should be evaluated.

# OrganiCity: a (responsible) smart city facility

OrganiCity offers a new paradigm to European digital city making. OrganiCity brings software, hardware and associated human processes flexibly together into a new living city that is replicable, scalable, as well as socially, environmentally and economically sustainable. Three clusters – Aarhus (DK), London (UK) and Santander (ES) –, bring their various stakeholders together into a coherent effort to develop an integrated Experimentation-as-a-Service facility respecting ethical and privacy sensitivities and potentially improving the lives of millions of people.

The OrganiCity consortium is creating a novel set of tools for civic co-creation, well beyond the state of the art in trans-disciplinary participatory urban interaction design. The tools will be validated in each cluster and integrated across the three cities. In addition to citizen-centric join of testbeds, partner technologies and enhancements, open calls allow several chosen experimenters the use of the project's facility and co-creation tools.

# Positive actions in OrganiCity

- Clear identification of roles, data controllers and data processors/sub-processors, DPO, and the relevant duties and obligations;
- Drafting of a robust Data Processing Agreement;
- Mapping and recognition of legitimate basis of personal data processing activities - and appropriate authorization of natural persons to process personal data;
- Drafting of a comprehensive and clear privacy policy/information for the open call phase (data subjects=applicants/experiment proponents);
- Correct evaluation process including Ethics and Privacy Impact assessment, both for OrganiCity facility/features and for proposed experiments;
- The stipulation of a specific data protection clause in the Agreement with Experimenters;
- First adoption of adequate security measures (including data breach reaction procedures), to be more developed following the evolution of the facility;
- Ensuring data subject's rights (including right to be forgotten), through: clear and easy contact procedures, prompt replies to data subject's requests, privacy dashboard/control panel so as to allow data subjects to keep control over their personal data.

# Further E&P steps in OrganiCity

- Continue mapping data processors/sub-processors. Focus on the collection and review of any ancillary agreements, such as data processing agreements between Partners and/or Partners and the Experimenters, and collection of the ethical and statutory written approval issued by the relevant DPAs to be obtained and submitted by Partners and experimenters;
- Performance of Data Protection/Ethics Impact Assessments for specific facility features, when needed in light of the possible risks for rights and freedom of natural persons;
- Further implementation of security measures (technical, logical, organizational) and documentation of E&P compliance activity (records, etc.);
- Deepen possibility of lawful re-use of pseudonymized data as a business model.

# THE «CROWD-PRIVACY» PROJECT FOR A CO-CREATED DEFENSE

Privacy Flag objectives:

1. Develop a highly scalable **privacy monitoring and protection solution** based on:
- Crowd sourcing mechanisms to identify, monitor and assess privacy-related risks;
- Privacy monitoring agents distributed on users' smart phones and web browsers to identify privacy threatening activities and applications;
- Universal Privacy Risk Area Assessment Methodology (UPRAAM);
- User friendly interface informing the users and raising citizen awareness on their privacy risks when using a smart phone application or visiting a website

2. Develop a **global knowledge database** of identified privacy risks with websites, smart phone applications and smart cities deployments,- together with **on-line services to support companies** and other stakeholders in becoming privacy-friendly, including:
- In-depth privacy risk analytical tool and services;
- Voluntary legally binding mechanism for companies located outside of Europe to align with and abide to European standards in terms of personal data protection;
- Services for companies/entities interested in being privacy friendly;
- Labelling and certification process and service;

3. Collaborate with standardization bodies (such as ISO, ETSI, ITU, and IEC) and actively disseminate towards the public and specialized communities, including ICT lawyers, policy makers and academics.

# Self(ie) Control: empower the user/data subjects

**1. Crowd-privacy alerts and opinions:** “unity makes strength” (e.g. collecting feedbacks via the UPRAAM tool);

**2. Automation of the self-protection** (self(ie)control – e.g. Privacy Flag tools such as the browser add-on and the smartphone application for privacy risks evaluation).

**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**.**

# Data Controllers/Processors and privacy compliance assessment

## In-depth evaluation tool

Privacy Flag will propose to SMEs and interested public entities a voluntary **in depth privacy risk and gap analysis (according to EU GDPR)** of their solutions with a report and recommendations for optimizing their practices in terms of privacy protection.

## Voluntary compliance commitment tool

Privacy Flag will enable any company or public administration in China, Japan, Korea and USA to formally and publicly commit and abide to respect the European standards (even if located outside of Europe).

# Thank you. For further requests or questions

l.bolognini@istitutoprivacy.it