Building Trust in a Connected World: personal data protection in a smart environment

17 January 2019

Luca Bolognini

President, Istituto Italiano per la Privacy e la Valorizzazione dei Dati – Italian Institute for Privacy and Data Valorisation

Founding Partner, ICTLC - ICT Legal Consulting law firm

l.bolognini@istitutoprivacy.it

Istituto Italiano per la Privacy e la Valorizzazione dei Dati

SMART PERVASIVENESS WITH RESPECT TO DAILY LIFE

Smart Cities are made of: User Generated Contents, Augmented Reality, Internet of Things, Artificial Intelligence, Automation, Blockchain, Public-Private strategic technological alliances, etc…

Everything is going to be tracked.

Everybody is going to be tracked.

A smarter city necessarily implies a higher risk for private and family life, and for personal data protection.

How could we protect natural persons (not only citizens) from this new Smart Big Brother, without renouncing to facilities and useful services and tools?

Both technological and legal safeguards can be adopted.

Istituto Italiano per la Privacy e la Valorizzazione dei Dati

What are the main risks?

Profiling/monitoring without data subject's consent/awareness

Interaction between objects in order to analyze information and generate cross-profiles

Re-identification of a data subject thanks to the unique identifier assigned to the object

Auto-installing norms and algorithms taking control over the personal data/processing

Unlawful data transmission between different subjects/objects

Unauthorized access to citizens' private sensitive data, for their discrimination

Impacts on unaware data subjects and complications of objects AI ("Digital Subconscious")

Istituto Italiano per la Privacy e la Valorizzazione dei Dati

Big changes for privacy in a smart environment
#1: interactivity and accountability are transforming

BEFORE IOT -> Data subject n.1 = **active – interactive** – in principle, the GDPR (and also Directives 95/46/EC and 2002/58/EC) identifies an «interactive» data subject

AFTER -> Data subject n. 2 as a NON-USER = the IoT implies the involvement of **passive subjects** which are out of reach (in terms of information to be given and of consent to be collected)

BEFORE IOT -> Controlling/processing actors = data **controller** and data **processor** that are **active subjects**

AFTER -> NON-SUBJECTS as controlling/processing actors = data controllers and processors are also, merely, objects -> **WHAT ABOUT ACCOUNTABILITY OF THINGS?**

Istituto Italiano per la Privacy e la Valorizzazione dei Dati

Big changes for privacy in a smart environment

#2: from data protection & privacy to "data protecy"

Reconsideration of the concepts of privacy and data protection, merging them together – as the continuous processing of personal data (protected according to art. 8 of the Charter of Fundamental Rights of the European Union, "CFREU") is also by default accompanied in IoT by the invasion of what, according to art. 7 of the "CFREU", we define as private and family life. The concept of "personal sphere" has changed. It has lost its classic features, opening its doors to the first inanimate objects which now are able to act independently in terms of the information they reveal and can even talk to each other, exchange data that they have acquired. Smart "things" are objects which are precisely part of the "personal sphere" which carry risks of "interference" with respect to the individual's privacy. Thanks to the intrinsic characteristics of the IoT, we have witnessed the reunification of the rights that Articles 7 and 8 of the CFREU had divided: the Internet of things requires that data protection and privacy are fused together in order to protect the individual from the activities of connected and interconnected intelligent objects that invade the private sphere (even the human body) while processing personal data.

Privacy+Data Protection="Data protecy"= physical + virtual personal info protection

Istituto Italiano per la Privacy e la Valorizzazione dei Dati

Big changes for privacy in a smart environment
#3: DPIAs to consider also physical threatens to rights and freedoms

A good Data Protection Impact Assessment (art. 35 GDPR, art. 23 Dir. 2016/680/UE) should not only focus on data/information security

It is paramount to assess the possibile risks to freedom and rights of natural persons: **some processing activities could be perfectly lawful, legitimate, secure but, still, not safe because of some intrinsic risks implied by that specific data processing, for its very nature**

Moreover, a robust DPIA should consider also material/physical impacts on natural persons, caused by a virtual elaboration of data

Istituto Italiano per la Privacy e la Valorizzazione dei Dati

Possible solutions - 1. 3D privacy

Often we cannot choose not to be a data subject and to remain invisible to sensors of the smart object.

The protection of the personal sphere and its “material data” is becoming three-dimensional

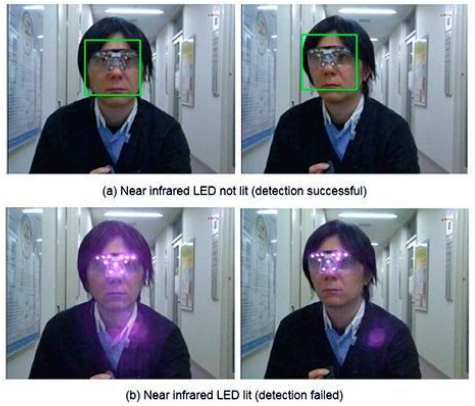
3D privacy consists in adopting also physical security measures, empowering users and non-users as data subjects with material tools in order to self-control over their information and to self-defend from data collection in IoT open environments. It is the use of other objects or other physical elements in order to avoid capture of personal information, shielding the individual from such collection,

restoring the privacy of the individual sphere and keeping the data protect.

3D privacy = a type of data protecy self-enforcement

Istituto Italiano per la Privacy e la Valorizzazione dei Dati

3D privacy: examples



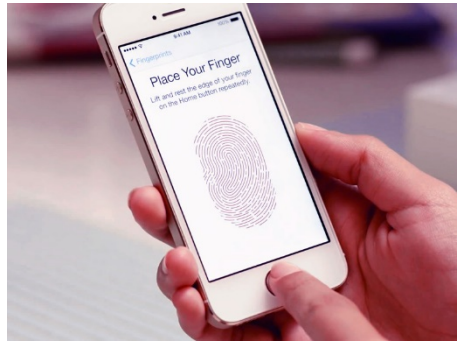
Privacy visors

Anti-paparazzi foulard

Personal antiradar

Privacy screen

Biometric passwords



iPhone press-code

Istituto Italiano per la Privacy e la Valorizzazione dei Dati

Possible solutions - 2. Crowd-privacy

Privacy Flag H2020 Project: to enable users in order to exchange information/awareness and to organize self-defense measures from cyber/privacy threats on line and in IoT environments

UNITY MAKES STRENGHT

Crowdsourced tools to monitor and check Smart and IoT systems in terms of security and privacy

Istituto Italiano per la Privacy e la Valorizzazione dei Dati

Possible solutions - 3. A “Food&Drug approach” and ADS/targeting labelling

Thinking about the impacts -> Disclosing what data processing was behind a targeted conten

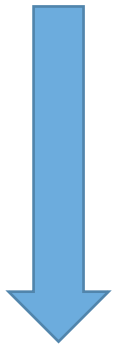
Like food&drug labelling, detailing ingredients and preservatives, users should be enabled to discover and understand why they are receiving a specific ads

Online users deserve the max possible **transparency** when receiving online "food for thoughts", such as ADS and other contents. Users shall know what they are taking and why, understanding criteria which are behind a digital content targeting. It would be possible to adopt a **code of conduct** according to Article 40 of the GDPR, combining it with a web-based **label-add-on**, to improve both the **accountability** of the digital content-providers and the **users’ awareness over IoT Big Data-driven impact** on their life.

Istituto Italiano per la Privacy e la Valorizzazione dei Dati

Possible solutions - 4. Blockchains for objects-accountability

Blockchain can help tracking – in a trustless way – all data processing transactions between things. Tampering of material objects (typically off-chain) could be detected and tracked through IoTized seals

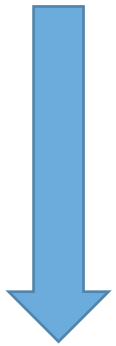


Possibility to make smart objects and non-human automated algorithms more accountable from a GDPR perspective

Istituto Italiano per la Privacy e la Valorizzazione dei Dati

Possible solutions - 5. Automated GDPR audits and certifications for smart environments

Art. 42 GDPR will allow new kinds of certification models and schemes, adopting «automated probes» to audit in real time privacy and security compliance levels in smart deployments



Possibility to make Smart Cities and other intelligent applications more accountable and trustable

Istituto Italiano per la Privacy e la Valorizzazione dei Dati

More in general: how to protect fundamental rights in a smart world?

"**Rule of law by design**" risks to become obsolete and weak against "***auto-installing norms***"

Today, that democracy-defending formula would need to be expanded upon and better specified: "**rule of human law by default**". We should in no way accept the idea of subjecting ourselves to rules, regulations, laws, decisions and codes that are automated and artificially created. No public law should ever be generated from an inhuman algorithm. No robot and no other form of artificial intelligence should be designed without an ON/OFF button that can be controlled only by humans and not by other machines – meaning that for each robot or form of artificial intelligence there should be at least one human super-admin and definitely no artificial super-admin. Also the robots, like the kings (and the mayors), have to be held accountable to human law. And each super-admin, or remote-Commander-in-Chief, in turn, should also be subject to the rule of human law.

Istituto Italiano per la Privacy e la Valorizzazione dei Dati

Thank you!

Luca Bolognini

President, Istituto Italiano per la Privacy e la Valorizzazione dei Dati –

Italian Institute for Privacy and Data Valorisation

Founding Partner, ICTLC - ICT Legal Consulting law firm

l.bolognini@istitutoprivacy.it