Artificial Intelligence or Artificial Insanity?
Challenges for Privacy and Data Protection in an A.I.-driven and IoTized world

2018

Luca Bolognini

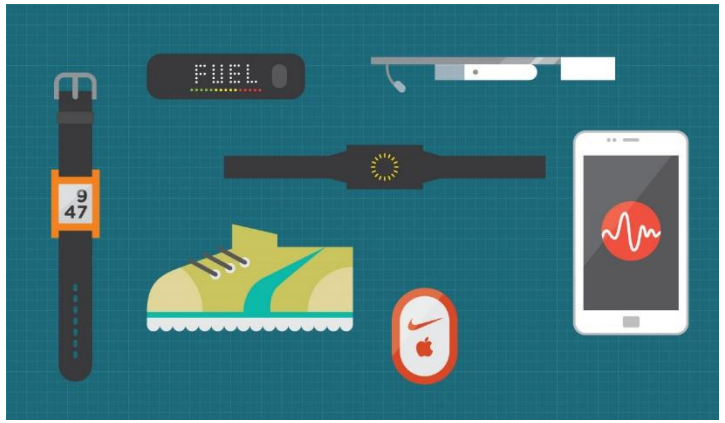
President, Istituto Italiano per la Privacy e la Valorizzazione dei Dati – Italian Institute for Privacy and Data Valorisation

Founder, ICT Legal Consulting

l.bolognini@istitutoprivacy.it

Istituto Italiano per la Privacy e la Valorizzazione dei Dati

IOT PERVASIVENESS WITH RESPECT TO DAILY LIFE



Wearable computing

Waiting for Internet of Blood?

Smart home

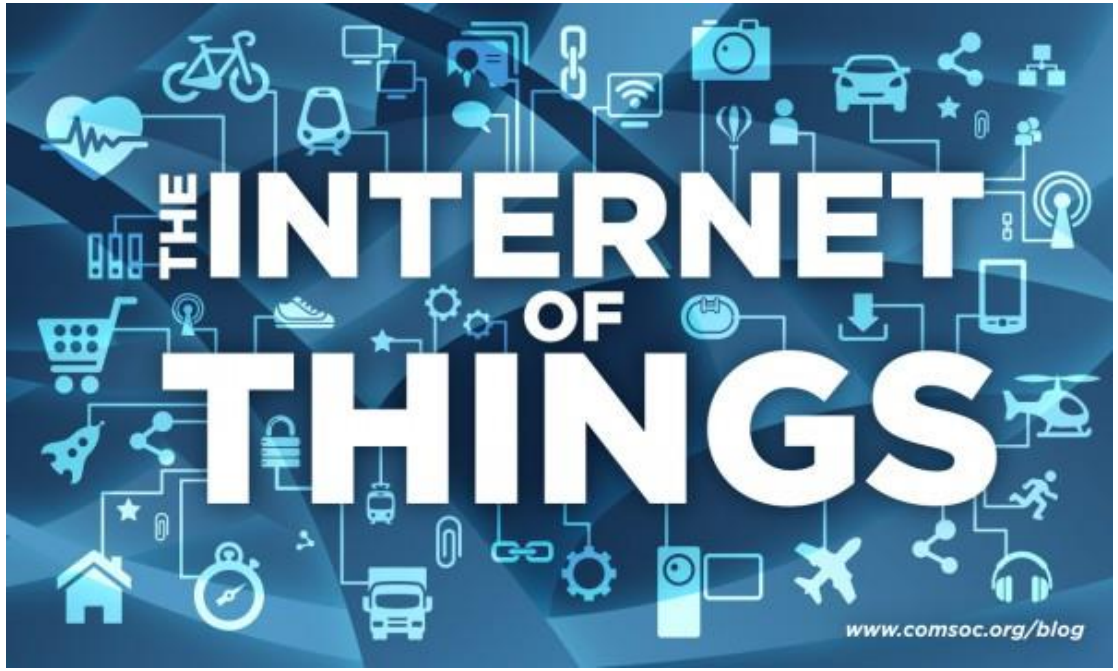
Istituto Italiano per la Privacy e la Valorizzazione dei Dati

Non-human social engineering

Big Data Collection

Material effects

A.I. driven decisions



Environmental sensing

Real time Profiling/ Monitoring

Identity fragmentation

Intersubjective and interobjective data transfer

Istituto Italiano per la Privacy e la Valorizzazione dei Dati

What are the main risks/threats?

Profiling/monitoring of data subjects without their 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

Impacts on unaware data subjects and newborn data generation ("Digital Subconscious")

Unlawful data transmission between different subjects/objects

Istituto Italiano per la Privacy e la Valorizzazione dei Dati

IoT players: a new dimension

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?**

“Data protecy”, not only a legalese neologism

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.

Data protecy =

physical + virtual personal info protection

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

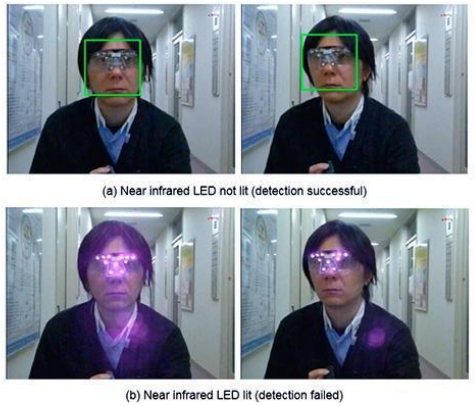
3D privacy consists in adopting also physical security measures, empowering users and non-users as data subjects with material tools in order to self-control over their information and to self-defend from data collection in IoT open environments. It is the use of other objects or other physical elements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

Personal antiradar

Anti-paparazzi foulard

Objects search engines

Privacy screen

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, to organize self-defense measures from cyber/privacy threats on line and in IoT environments

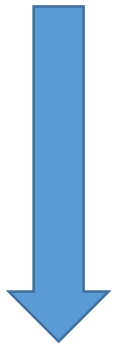
UNITY MAKES STRENGHT

Crowdsourcing tools to monitor and check IoT security and privacy

Istituto Italiano per la Privacy e la Valorizzazione dei Dati

Possible solutions - 3. Blockchain for objects-accountability

Blockchain can help tracking – even in a trustless way – all data processing transactions between things



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 - 4. A “Food&Drug approach” and ADS labelling

Thinking about the impacts -> Disclosing what data processing was behind a targeted banner or DEM

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 - 5. Seals and Certifications

An example: Privacy Flag H2020 Project and the new EuroPrivacy scheme (and more schemes will come in the future from the application of articles 42-43 GDPR and from the new EU Cybersecurity Package)

KEY TO PROMOTE:
CONSISTENCY AND INTEGRATION BETWEEN DIFFERENT CERTIFICATION SCHEMES (GDPR, CYBERSECURITY, ETC.)
NEW MIX OF AUDITING METHODOLOGY (INCLUDING REAL TIME – ALGORITHMIC AUDITING)
SPECIALISATION, FOCUSING ON USE CASES/DEPLOYMENT SCENARIOS

New best standards can be valid also for non-EU controllers/processors and tech producers

Istituto Italiano per la Privacy e la Valorizzazione dei Dati

Artificial Intelligence or Artificial Insanity? How to protect fundamental rights in an A.I.-driven world?

"**Rule of law**" 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**". 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 other governors, 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

Founder, ICT Legal Consulting

l.bolognini@istitutoprivacy.it

Istituto Italiano per la Privacy e la Valorizzazione dei Dati