Nexa Center for Internet & Society

Politecnico di Torino

Internet of Things: Hell or Paradise?

Executive Summary of the 2016 Conference of the Nexa Center for Internet & Society

Publication date: 10/01/2017

Authors: Marco Ricolfi, Antonio Vetrò, Francesco Ruggiero

Conference participants: Federico Morando, Monica A. Senor, Massimiliano Nuccio, Fabio Chiusi, Juan Carlos De Martin, Claudio Demartini

Further information on the Nexa Conference 2016 is available at the following address:
https://nexa.polito.it/conf2016

Studying the Internet, exploring its potential & experimenting new ideas

Nexa Center
for Internet & Society

Location:
Via Pier Carlo Boggio 65/A, 10129 Torino, Italia
(http://nexa.polito.it/contacts-en)
+39 011 090 7217 (Tel)
+39 011 090 7216 (Fax)
info@nexa.polito.it

Mailing address:
Centro Nexa su Internet & Società
Politecnico di Torino - DAUIN
Corso Duca degli Abruzzi, 24
10129 TORINO

Executive Summary

The term Internet of Things (IoT) refers to the network of billions of physical objects, which are provided with Internet connection and can collect and exchange data from the environment[1]. Each thing is uniquely identifiable through its embedded computing system and can be embedded with electronics, software, sensors, and actuators. Objects can be small items of common usage in everyday life (like a watch), but also home and office appliances (e.g., printers), buildings, vehicles, constructions, which are sensed and in some cases controlled remotely across existing network infrastructure. Such technological solutions create opportunities for more direct integration of the physical world into computer-based systems.

The connected Things can provide new solutions to make our everyday life more comfortable, especially in our houses (e.g., the fridge makes order of our preferred food), and even become proactive thanks to machine learning techniques (e.g., the fridge makes orders of food based on our fitness activity -which has been registered with a "smart" watch- and our diet, which is retrievable on our personal cloud storage). Bruce Schneier, expert of cryptography and computer security, suggests thinking to the objects as freed from their traditional usage, and looking at them as computers with different functions[2]: *"[...]there are now computers in everything. But I want to suggest another way of thinking about it in that everything is now a computer: This is not a phone. It's a computer that makes phone calls. A refrigerator is a computer that keeps things cold."*

The figures that describe this phenomenon are revealing: the estimated number of connected objects is estimated up to 100 billion before 2020[3]: the websites www.thingful.net and www.shodan.io are two IoT search engines that give an interesting representation of the state of the art. It is possible to model the interaction between the Things and the surrounding environment with the image of a triangulation: sensors collect data from the environment; the data are processed by algorithms (including mining or analytics techniques); based on the results, specific services or commands are executed, which are able, in turn, to operate on the environment through actuators (hence, closing the loop). The Internet permits to transfer data and commands on each of these passages, thus connecting systems, sensors and actuators (all potentially located in geographically separate areas).

---

[1] International Telecommunication Union (ITU), "Measuring the Information Society Report," ITU Report, 2015
[2] http://www.dailydot.com/layer8/bruce-schneier-internet-of-things/ , last visited on 19 Dec. 2016
[3] See https://nexa.polito.it/nexacenterfiles/Conf2016_slideVetro.pdf , pp. 22-25

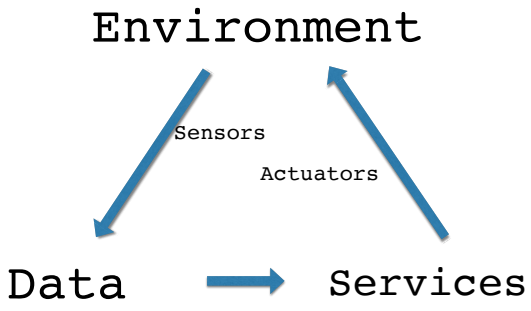

Figure 1 Triangulation of environment, data, services. Source: A. Vetrò

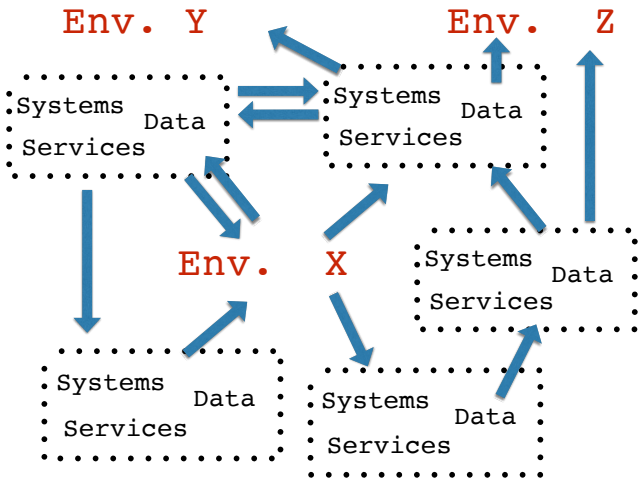

Figure 2 Connected systems, data, services. Source: A. Vetrò

Leaving aside the technical aspects - which were introduced by Antonio Vetrò-, it turned out to be useful to reflect on the nexus between IoT and circular economy (explored by Federico Morando during the conference), because the relationship between IoT and environment is tight: IoT components are often produced with a rapid obsolescence (in certain cases, even so planned and determined), which might fuel a potentially boundless consumerism, and a consequential growth of e-waste. Therefore there is a risk of negative impact of IoT on environment. However, if economic and environmental efficiency are bound together (by convenience, or regulation), the impact can turn to be positive and become a priority also for big producers: a connected thermostat can help saving money and reduce the emissions of polluting elements, especially if connected to smart grids[4]. A similar reasoning applies to car sharing solutions (on average a car in Europe spends 95% of the time in a parking lot or garage[5]), which has an impact on CO2

[4] See https://nexa.polito.it/nexacenterfiles/Conf2016_slideMorando.pdf , page 6
[5] See https://nexa.polito.it/nexacenterfiles/Conf2016_slideMorando.pdf , page 7

emissions. It should be noted, though, that the connected Things are liable to pollute less also due to the fact that they are usually managed by a central entity (in most cases, a big corporation), and that often they are used but not owned by consumers: in this way, the utilization rate increases, and so does efficiency. Decentralized systems, like the blockchain, are proposed as a solution to the centralized control, but their impact on energy consumption is deemed to be still negative.

In practice, IoT solutions with centralized control are the status quo. Such situation gives unprecedented freedom –and responsibility, too- to the big corporations, but less degrees of freedom to the citizens: impossibility of switching between services and platforms, difficulty in re-selling items with digital content stored, or impossibility of contracting the terms of use are examples of the reduction of consumers rights and protection in the IoT world. This may lead to a dysfunctional equilibrium:

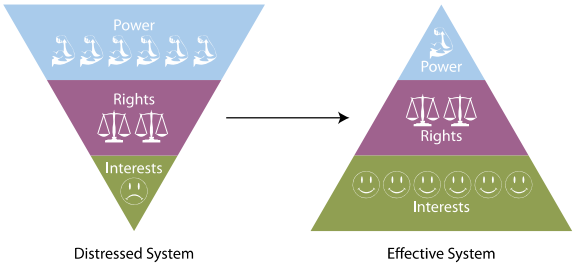

Figure 3 "Getting Disputes Resolved - Designing Systems to Cut the Costs of Conflict", Ury et al.

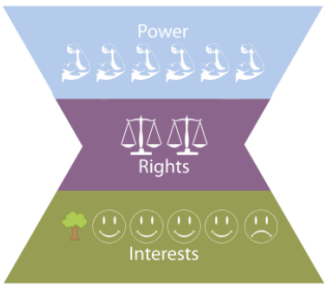

Figure 4. Risks of centralized solutions for the IoT ecosystems. Source: F. Morando.

Yet another risk - signaled by lawyer Monica A. Senor- is the pervasiveness and ubiquity of surveillance (direct or indirect), induced by IoT. Such a risk is connected to the large amount of data that are collected by the Things and then merged with data sources originated by other systems (e.g.: data of our “smart” watch connected to our social network profile, that is in turn

connected to our cloud system where a certain amount of personal data is stored). As a result we observe an un-controlled data flow, with unknown actors that have indirect and un-authorized access to personal data. With the Internet of Things, this turns out to be more than a privacy problem: it becomes a security and safety problem.

Security is an emerging problem especially regarding all those Things that have a longer duration than a smart phone (a traffic light, a car, a fridge, a thermostat) and typically do not have mechanisms for updating their access mechanisms or are placed in unprotected networks. Regulation should come to the aid of our lives: the current European law for protecting privacy, however, is not adequate in the IoT world, due to the fact that it protects only well-determined data flows, but not the undesired chains and fusions of data that are possible starting from a data source and an identity: lack of control and information asymmetry are the two most evident problems. It is therefore urgent that the Regulator protects our "digital body", which lives on our tablets, writes opinions on the social network, buys Things on online platforms: we are more than the sum of the data that we produce with connected Things (as we are more than the sum of the cells that compose our physical body). It is not a matter of digital rights, but rather of human rights declined in the *infosphere*.

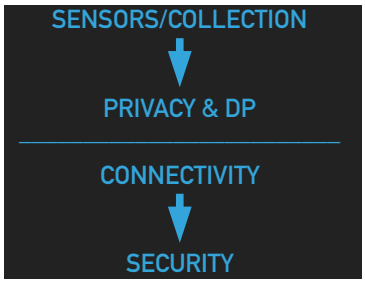

Figure 5. From privacy to safety and security. Source: M.A. Senor

Privacy by design and risk assessment are urgent, if still preliminary, steps to adopt in order to not bump into the infernal scenarios depicted by journalist Fabio Chiusi, whose consideration originated from the DDoS (distributed denial of service) attack witnessed by American people on 21st October 2016. The attack has been conducted through the botnet Mirai, which is composed of about half million Things connected to the Internet and whose passwords were retrieved with surprising ease from registers shared on the Web[6]. With a similar procedure, it would be possible

[6] Default company passwords or commonly used passphrases are listed in these registers.

to shut down the Internet or launch a world cyber war from a connected toaster.

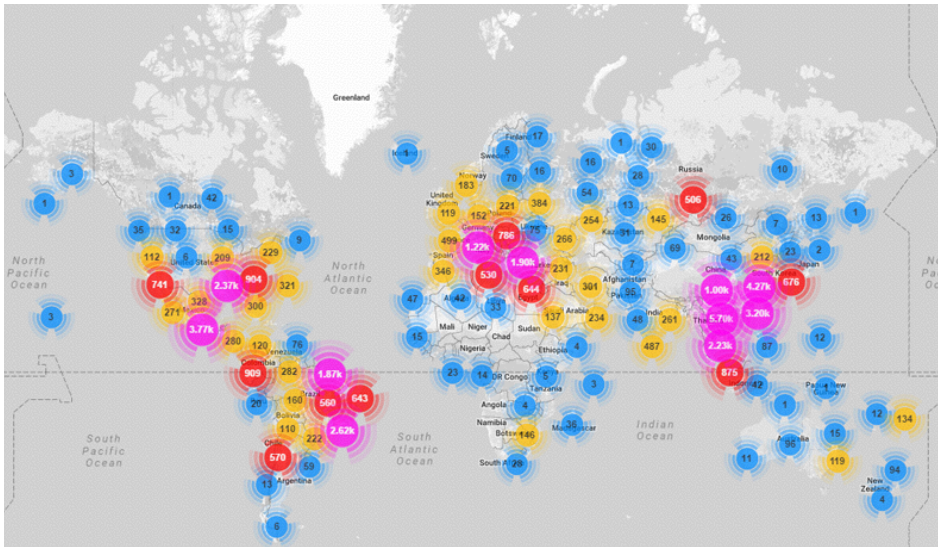

Figure 6. A visualization of the spread of Mirai. Source: Malware Tech

The main reason for such paradox is that innovation has been exponential and therefore much faster than regulation and enforcement of information security measures. In addition, interconnection makes unsecure also Things that have been harmless for human beings so far: it already happened that fridges sent 750000 spam e-mails, smart TVs can send records of our family conversations, cars can be controlled remotely with a laptop, traffic lights commanded by drones, and advertising boards hacked[7]. While waiting for a better regulation of the security measures, simple actions can keep at bay the "hell": for example producers shall permit automatic updates of the software, and consumers should change default passwords of their Things. In addition, security and privacy should be among the goals of the entire products supply chain: from the producer to the seller, until the customer.

Following the dichotomy hell-paradise, Massimiliano Nuccio presented two economic visions. The positive one lays its foundations in the fact that Internet has reduced transactional and search costs, favoring the meeting between demand and offer. The result is a dynamic market where reputation and brand have less importance than in the past: this situation should support SMEs. However the reality has turned out to be different, because few big corporations right now operate in multiple markets, competing among them with different services or products. SMEs are confined in a (hopefully long) tail of the demand of very sectorial –and often highly customizable- products and services.

[7] See https://nexa.polito.it/nexacenterfiles/Conf2016_slideChiusi.pdf , pp 14-26

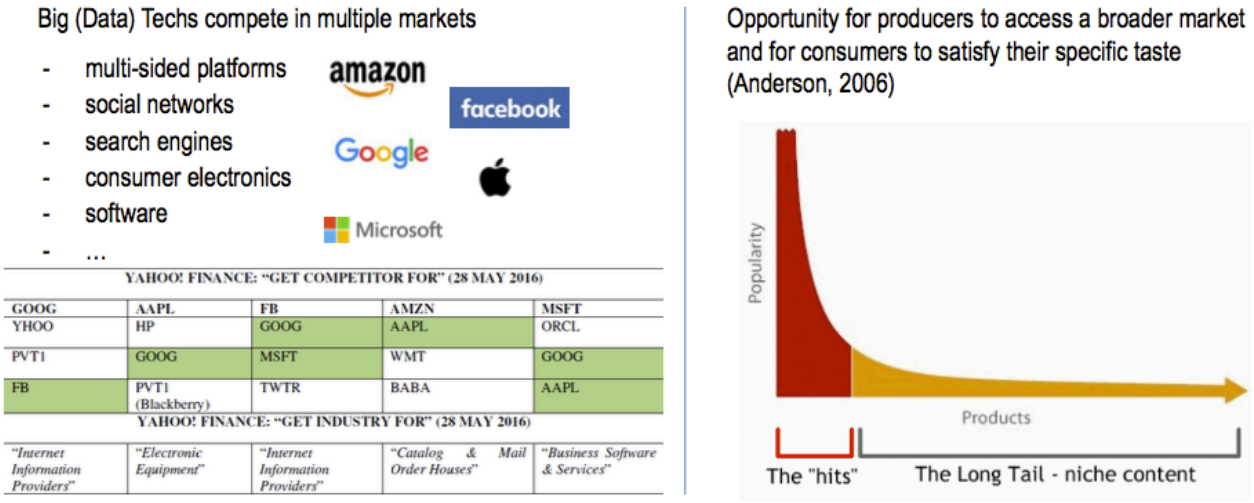

Figure 7. Oligopolies and long tail in the IoT economy. Source: M. Nuccio

Further negative aspects concern also the technological barriers for collecting, analyzing and transforming data: theoretically open source, multi-homing and data portability can balance such asymmetry, giving the possibility of using consumers data to a multitude of actors, preventing thus the consolidation of an access economy.

Marco Ricolfi concluded the conference with an overview of the research priorities in the path ahead. In *primis*, researchers and policy makers should reflect on the effects of IoT on employment, which –so far- has been negative due to the impact of connected automated systems on the quantity and quality of labor input for product unit; also the ongoing redistribution to the top quartiles of income tends to depress aggregate demand. Regulation should step in soon at both levels (employment and income distribution), but a big question arises: at which level can intervention be imagined? Ex-ante solutions should be identified at specific levels: national State, bodies of the European Union (e.g., Antitrust), International Organizations, multi-stakeholder governance structures. Each level can have a different effect, depending on the service, the product and the type of data involved. The intervention of global governance entities might be necessary, due to a current geo-political context in which multi-stakeholder governance has proved problematic, and still Internet decentralization has emerged as a priority. This is even more urgent in light of the fact that only three States[8] own most of the geostationary satellites: they are, in fact, the ultimate source of control of every-Thing connected. As a consequence, the IoT could become a system potentially dangerous for the whole humanity (think to drones or tanks): as A. Vetrò underlined in the introduction, IoT is not only about sensors, but also about

[8] USA, Russia and China

actuators. Considering that satellites are also vulnerable to destruction or hacking, the hellish scenarios makes a disquieting shift in the macro scale.

Research and policy makers, as underlined by Co-director Juan Carlos De Martin in the introduction and by Claudio Demartini (Head of Automatics and Informatics Department at the Politecnico di Torino) in his closing remarks, should focus on these risks, in order to help governments and civil society recovering the gap between them and the technological progress, and understanding what should be done to avoid the hell of connected Things.

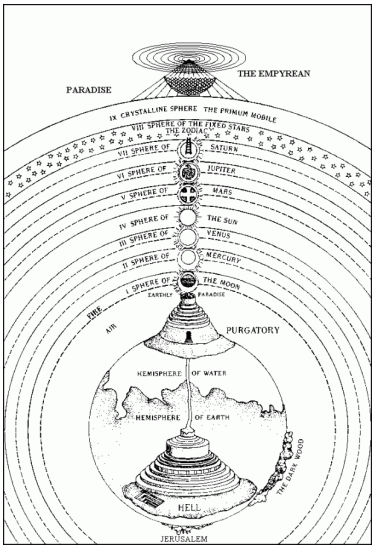

Figure 8 A representation of Dante's vision of Paradise and Hell. Source: http://www.florenceinferno.com