The Internet of Things:

What has changed since 'IoT Council' was born

By Gérald Santucci

"In the twentieth century, computers were brains without senses—they only knew what we told them. That was a huge limitation: there is many billion times more information in the world than people could possibly type in through a keyboard or scan with a barcode. In the twenty-first century, because of the Internet of Things, computers can sense things for themselves."

(Kevin Ashton, 2015)

A Blast from the Past (the present of the past)

In August 2010 I had convinced the European Commission to set up an IoT Expert Group to debate the requirements and options for implementing the EC Communication on "Internet of Things – An action plan for Europe" (May 18th, 2009). The group held regular meetings in Brussels until November 14th, 2012.

An Internet of Nouns

At this time, the Internet of Things (IoT) was still mainly discussed within academia. The term 'Internet of Things' had been coined in 1999 by Kevin Ashton to describe a system where the Internet is connected to the physical world via ubiquitous sensors. The concept itself was not so new, and we can retrieve its roots in a number of related terms such as Pervasive Computing / Ubiquitous Computing (Mark Weiser at Xerox Palo Alto Research Center, 1988), Ambient Intelligence (Philips Research, 1998, and European Commission's Information Society Technologies Advisory Board, 2001, Ubiquitous Networking (Prof Ken Sakamura, Director YRP Ubiquitous Networking Laboratory, 2004)), Cyber Physical Systems (Dr Helen Gill, U.S. National Science Foundation, 2006), and more.

By 2012, it had become clear that against some predictions the term 'Internet of Things' would prevail outside academia, gaining adherence in industry, the public sector, and later the entire society. This was less the case for the neighboring term 'Ambient Intelligence' (Ami), which gradually evaporated outside the academic microcosm.

The discussions in the IoT Expert Group encompassed several technical issues – architectures, identification, standards – and policy / regulatory issues – privacy & data protection, security, ethics, governance.

Architectures

The main recommendations for architecture design included fair access to infrastructures across all devices, spectrum management for effective wireless connectivity, interoperability, and appropriate design of object identifiers.

Standards

Given the fragmentation of the industry, with M2M/IoT solutions mainly developed under a vertical model (application-specific developments), the IoT Expert Group was stressing the need for a common service layer that would foster reuse and interoperability between applications and devices.

Identification

The issue of Numbering / Naming / Addressing / Identification (NNAI) resources was intensively debated in the IoT Expert Group – indeed, accessing information related to an object implies the assignment of an identifier and the establishment of a network communication. An object becomes connected by getting assigned an identifier and a means to be connected to other objects or to the network.

How is the identification structured (i.e. object naming)? Who assigns the identifier (i.e. the assigning authority)? How and where can additional information about the object be retrieved, including its history (i.e. the addressing mechanism and the information repository)? How is security ensured? Which actors are deemed accountable for each of the previous questions? Which ethical and legal frameworks apply to the different actors?

Despite extensive discussions, a number of issues remained unresolved by mid-2012, e.g., should an identifier be the same as a network ID, how discovery and resolution should be handled, should unique or multiple identifiers be used, should a single global scheme be adopted (e.g., IPv6 or 6LOWPAN) or rather a solution based on different interoperable schemes using routing algorithms? The IoT Expert Group was tipping over

slightly in favor of interoperability since global identifiers are hard to manage for all types of objects and network addresses change as objects move through different domains.

Regarding the specific issue of resolution / discovery, the proposal was to use the Object Naming Service (ONS) approach and the existing Internet domain model. The IoT Expert Group thought it was important to ensure that the discovery system adopted would continue to work into the future, including being scalable up to billions of devices and efficient even for the smallest and simplest objects (e.g., individual light bulbs). Moreover, it had to be noted that different considerations could apply according to different sectors. For example, in the healthcare sector, the value is less in the connectivity than in the data.

Support for mobility was also found important, as people move around while performing a single function or role, thus requiring virtual locality. (This idea was actually quite premonitory given what happened during and after the COVID-19 period, with the rise of remote work.)

Governance

Protracted discussions on IoT governance never reached a common satisfactory point. The IoT Expert Group was split between some experts recommending regional bodies and other organizations and the other experts holding that it was not necessary to create new governance bodies since the existing ones were well suited for the purpose. This failure reflected the difference of perception regarding the relationship between IoT and the Internet in general. For a first group of experts, the Internet was simply a part of IoT (actually, this was my view, taking a long-term perspective with several billion devices talking with each other, with humans, and with different networks), for a second group of experts IoT was just an Internet application, and for a last group IoT was just formed by a range of different applications.

Data protection, privacy, and security

No need to go into details here about the specifics of the discussions, since these issues continue to occupy the top of the policy agenda today at institutional, international, regional and national levels. Let's just mention the General Data Protection Regulation (GDPR), which was significantly influenced during the relevant policy making process by some of the discussion elements that had been addressed within the IoT Expert Group – Data Protection Impact Assessment (instead of Privacy Impact Assessment), Right to Erasure ('Right to be Forgotten'), Privacy by Design, Right to Data Portability.

When the IoT Expert Group was disbanded in November 2012, the General Data Protection Regulation (GDPR) did not exist, it was only under discussion behind curtains, and my goal while holding frequent contacts with European Commission colleagues in DG JUST and DG ENTR was to persuade them of the necessity, as soon as the policymaking process on the revision of the 1995 Data Protection Directive would take on momentum, to buy-in some of the new concepts discussed in the IoT Expert Group.

I never thought that a distinct legislation should be developed for IoT privacy, data protection, and security, but I had strong expectations that concepts such as "privacy impact assessment", "right to the silence of the chips" and "ethics-by-design" would fuel the upcoming political discussions on a general new data protection legislation. In other words, I was looking for a Recommendation to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions on the governance of the Internet of Things that would emphasize the role and useful impact of self-regulation and co-regulation, thus allowing the general provisions of the future data protection legislation to be further developed for the Internet of Things. In this respect, success has exceeded my expectations.

Metaphorically, I sowed pebbles like Tom Thumb, in the form of almost invisible threads that eventually connected policymakers in the European Commission to the right options for designing the new data protection legislation.

Ethics

I contemplate writing a detailed article later on IoT Ethics, but I can't hide my satisfaction for what the IoT Expert Group achieved in the early 2010s when it gave utmost importance to an issue which today, whether for IoT, Artificial Intelligence and other digital technologies and applications, is regarded almost everywhere as inescapable.

Since the topic was new, the discussions were blooming in all directions, encompassing data protection, social justice, trust, separation (i.e. the boundaries between contexts and social spheres), discourse framing (i.e. adequateness of IoT metaphors), agency, informed consent.

Moreover, the idea of creating a social contract between people and objects was also heavily debated. This was because the issue of objects agency questions current understandings of the social contract between people and the (smart) objects surrounding them. When people use the things in the IoT, they effectively delegate actions to objects. It is therefore important that the actions being taken by IoT technology are actually intended by

its human users. Of further importance are the algorithms being used as part of the IoT: profiling algorithms may be blind towards the special needs of individuals and therefore assurance is needed that they are morally proper.

A recent trend in IoT ethics concerns the dataification of the world. Should we collectively impose scientific and/or ethical limits to what I would call the *quantified-selfication* of the human being and the emergence of Human Digital Twins – near-live digital representations of our bodies in data for tracking, measuring, and monitoring our activities, our movements, and our key health indicators for health, fitness, and wellness.

Another challenging issue is data monetization, i.e. how far should we collectively accept that personal data can be traded on markets by individuals acting as allegedly free actors? In other words, should personal data be considered as a commodity? Is this fair? Is this worthy from an ethical point of view?

The Future Begins Today (the future of the present)

After I moved to another DG CNECT Unit in July 2012 (Knowledge Sharing), the IoT Expert Group was unfortunately left without clear and strong guidance, which resulted in November of the same year in a tense meeting and its definitive disbanding. I always considered, sadly, that I missed 6 months to complete the work I had in mind with a strong consensus that would have maintained the leadership of Europe in IoT policy development.

More than a decade after the closure of the IoT Expert Group, the question that comes to my mind is the following: outside the issues that have been mentioned above, which are still relevant (e.g., identification, privacy) or which sometimes are being addressed today in a different perspective (e.g., governance), what are the fundamental changes that have occurred and are likely to drive the IoT in the coming years?

The Internet of Things and Nostradamus

In 2010, IoT stakeholders were struck by the stunning prediction, made almost at the same time by Ericsson and Cisco, that the world would have 50 billion connected devices by 2020. Remarkably, those predictions weren't even close to the highest of the time, made by IBM that forecasted 1 trillion connected devices by 2015! Frankly, I tended to believe in these preposterous projections. Since then, I prefer not to look at any sky-high projections of this kind for IoT growth and profits…

It was also the time when some experts of international renown were warning entrepreneurs and policymakers that without the

extensive global adoption and deployment of IPv6 as the primary version of the Internet Protocol, the IoT would never be possible. When the first internet protocol, Internet Protocol Version 4 (IPv4), was released for public use, we were told, it only allocated enough address spaces to accommodate for just over 4 billion devices. Therefore, Internet Protocol Version 6 (IPv6) was obviously the perfect solution for the IoT as it can extend the number of address spaces to roughly 340 undecillions (10^{66}). I have nothing against IPv6, on the contrary, but this argument, continually repeated at every conference, also taught me the lesson that before panicking it was much wiser to give time to time, sit down, and discuss, if possible with a beer in hand.

After development, where is deployment?

IoT is no longer confined in academia, it is actually well installed in industry. However, the IoT industry, we are told frequently, is not thriving.

Yet, Small and Medium Enterprises (SMEs), which represent about 90% of global business and more than half of employment worldwide, are steadily embracing the potential of the IoT for innovation that can help them stand out among stiff competition. However, if disruptive and incremental innovation comes mainly from SMEs, it is then captured by larger companies – as Henk Koopmans, President Advisory Board at CROSS-SILO B.V., explained to me in a conversation, "*SMEs are on the losing end because their political lobby has not the financial power of the market leaders to keep on lobbying politicians worldwide, in the EU and its Member States.*"

Moreover, after several decades of existence of the IoT, companies are often disappointed that their Return on Investment (ROI) expectations have not been met on the market. As Francisco Maroto, CEO and founder at OIES Consulting, an IoT consulting and business development company, has recently explained on LinkedIn, companies tend to believe that their investment in building an IoT infrastructure – in a smart city, a smart factory, a smart building, or a smart home – has not been justified by the actual ROI, which is somewhat unfair since they should rather consider that success in IoT requires time, i.e. patience, and that the choice of business cases upfront is a critical moment that must be paid the heaviest attention. "*Don't expect miracles on your IoT investments*", says Maroto, "*but don't quit halfway.*"

This IoT Day 2023 (between 3,000 and 6,000 results on Google over the last few days, which *en passant* is an excellent search engine score, without any existing SEO or SEA strategy!) has allowed to show that IoT is today everywhere – Rob Tiffany, a top voice in IoT and Digital Twins, recorded many use cases

during his IoT Coffee talk sessions, for example Smart Cities, Smart Home, Smart Spaces, Agriculture, Education, Oil & Gas, Security, the UN Sustainable Development Goals (Water & Sanitation, Poverty, etc.), and he managed lively discussions on the growing confluence of IoT with other technology developments such as Artificial Intelligence (AI), Blockchain, Cellular, Digital Twins, Edge Computing, LoRaWAN… The potential of IoT sensors for mitigating Climate Change and Natural Hazards, such as flood prediction and prevention, has been stressed by several participants in the conversations.

Therefore, there is no sensible reason why we should expect a bleak future for IoT.

There are several "Big Trends" that we could summon to provide a glimpse of the future of the IoT. Here are three such Big Trends which, for me, are both irresistible and necessary.

Big Trend 1: From the Cloud to the Edge

Along with AI, 5G/6G, and Big Data, the IoT is at the center of the digitalization of the world. With processing moving to the edge, communication and storage costs are drastically reduced while AI and Machine Learning (ML) allow to identify data patterns that have an impact on physical processes. The data collected from IoT sensors is obviously essential for monitoring their environment and gaining insights, instigating an action, or responding to other remotely situated connected objects.

Given the rise of connected devices, the logical evolution of the dominant Cloud Computing model is Edge Computing where the processing moves from a centralized point to the IoT device itself, i.e. the edge or periphery of a network. Edge Computing allows (i) to avoid the transfer of mission-critical data to the Cloud, (ii) to support resilience, real-time operations, security, privacy and data protection, and (iii) to reduce energy consumption and the human carbon footprint.

The next generation IoT will need a strong computing capacity at the edge and a computing continuum between far edge devices and the Cloud.

I believe that the ongoing Transatlantic Digital Cooperation should consider to include this aspect.

Big Trend 2: From Local Mobility to Global Connectivity

A second 'big trend' concerns the mobile industry. The Mobile Network Operator (MNO) model, based on branded, proprietary SIM cards, is doomed to collapse. The reason is that MNOs are inherently regional companies that operate in limited (mostly national) geographies and control their own slice of bandwidth with limited unused capacity.

This model works indeed for smartphones, where people typically live in one country and can get flexible international roaming options for international travel. But it doesn't work in a context where enormous quantities of devices need to be shipped all around the world. Therefore, we are already today witnessing the gradual replacement of SIMs in favor of eSIMs, with as a consequence the end of the vendor lock-in of customers.

The search for increased flexibility and choice is going to change the dynamics of the mobile industry, giving a unique opportunity for the global digital platforms, up to now situated in the U.S. and China, to use their scale and power to provide turnkey solutions. MNOs will be gradually forced to adapt their business models by offering next generation Mobile Virtual Network Operator services, integrated with digital platform offerings to offer switch services between networks according to local and international needs.

If this happens, as I believe it will, the IoT market will scale up rapidly while the industry will become more concentrated around the largest companies.

Big Trend 3: From IoT to IoTforGood

Over the last few years we have seen the number of IoT use cases and business cases developing and growing, from Smart *Whatever* (City, Home, Building, traffic etc.) to Healthcare, Water & Sanitation, Logistics & Supply Chains, Environmental Monitoring, and so forth.

We are faced today with a systemic sustainability crisis caused by multiple interrelated forces which exploit and destroy nature. This is the result of a protracted failure of policies, institutions and markets taken together to change course and address the source of the problem at systems level. We are moving from the Holocene geological epoch to the Anthropocene one. (Even if scientists largely disagree on when this transition began.)

What matters, I believe, is not to consider the use cases in isolation, according to the specific needs of customers or opportunities of vendors, but to realize that they all together belong to those IoT applications that are essential to realize the vision of what I would call the "Economy of Life", i.e. the world of tomorrow where priority investments, both private and public, will target areas that benefit the resilience of our planet and the wellbeing of human beings: Security; Healthcare; Natural hazards, asset tracking of hazardous materials; Climate Change; biodiversity loss; broken land-use and water cycles.

In this context, our role – and responsibility is to alert policymakers to the urgent need of using IoT and associated technologies, in particular AI, for fostering such an Economy of

Life. Here, the purpose of humanity aligns with the purpose of the planetary system itself: we are looking to continuously improve through feedback loops, learning, and adaptation toward ever-increasing levels of diversity, resilience, beauty, and abundance, for example.

Conclusion (or not)

More than a decade after the disbanding of the European Commission IoT Expert Group, several issues that were intensely debated there have found their way into policymaking and public space. Others were left orphan, but the market played its full role and picked up the winning options. Meanwhile, new issues have emerged – Interoperability, MVNOs, Ethics, or the confluence of IoT and related disruptive technologies like AI, Edge Computing, 5G, Blockchain.

No doubt the IoT Council has a major role to play in raising awareness about these new issues, debating requirements an policy options, insisting on the focus to be given to the Economy of Life, calling for enhanced cooperation between institutions, countries and regions, fostering the exchange of knowledge and information amongst its members and towards all stakeholders who share its purpose and values, writing well-thought reports targeting policymakers, etc.

Taking now some distance from reality, I would like to conjure up a conversation I had recently with Peter Friess, a former European Commission colleague who worked with me on the IoT. At a time when experts discuss in particular the role of IoT in the development of the Metaverse, i.e. how to map data from real life, in real-time, into a digital reality, Peter stressed for me the concept of "Otherverse", inspired by the German idea of a *Wunderkammer* – a concept of the Renaissance and Baroque periods – with IoT and AI opening up new possibilities for future research (by providing collective knowledge) and future creation (by proposing a machine-thinking inspired recombination of ideas).

As Ted Kennedy said once: "*To strive, to seek, to find, and not to yield (…) The work goes on, the cause endures, the hope still lives, and the dream shall never die.*"

12/04/2023