10

Ethical IoT: A Sustainable Way Forward

Maarten Botterman

GNKS Consult NV, Netherlands

10.1 Introduction

The Internet of Things (IoT) is rapidly developing, primarily driven by businesses that see opportunities for profit through new business and business models. Other key players include public administrations and non-profit institutions that see IoT as an opportunity to address societal challenges in effective ways that were not reasonably available, before. Good public use of IoT can pay off rapidly, and lead to the ability of serving citizens and businesses better, at lower costs, in more inclusive ways. The first applications in the public domain show promising results – and it is still early days.

Evolution from machine to machine technology to the growing IoT networks raises challenges at every level that can become barriers to adoption when not addressed. New masses of data are generated by our Things and then shared between objects. Smart algorithms can combine this information with masses of very diverse sources such as social media, Open Data, traffic data, etc., leading to a world where BigData are more and more used to guide our decisions.

This world with "many eyes" (all the sensors in IoT and traffic data that register what happened where when and who/what was involved) and a wealth of (Big) data that can be combined and analyzed using smart algorithms is a world in which the old methods of privacy protections often fail [1]. Many notions of privacy rely on informed consent for the disclosure and use of an individual's private data. Data has become a resource that can be used and reused, often in ways that were inconceivable at the time the data was collected.

IoT has become a real game changer in this as sensors complement the data that were already generated, stored and shared before with new data,

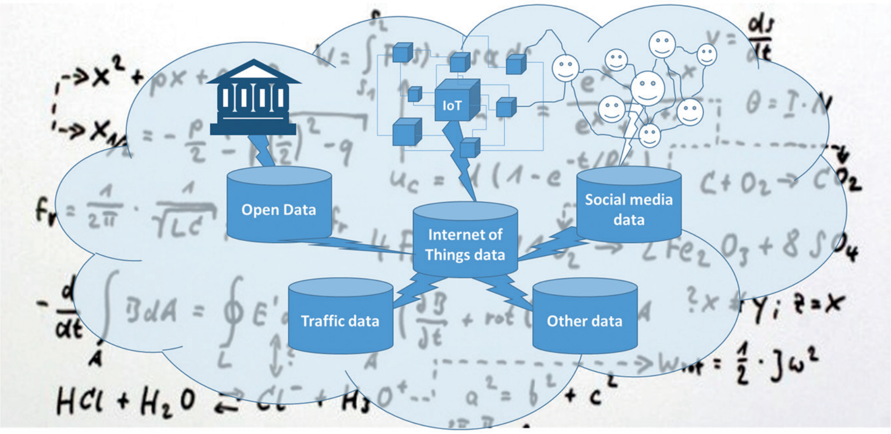

Figure 10.1 From IoT to BigData and analytics.

increasingly filling the gaps in digital representation of the (physical) world and what is happening on its surface. Not only that: IoT offers the opportunity to collect high value data – very focused on what the investing organisations want to know, and relatively well structured, as real-time as needed, and in context [2]. How do we adapt to this new reality where almost everything can eventually be captured in digital form (Section 10.2)? And what is needed most in order to create an environment that fosters positive evolution of the IoT, allowing us as businesses and society to benefit fully, without having to be afraid for the consequences (Section 10.3)? The conclusion (Section 10.4) is very much in line with the words of Commissioner Ansip: “Trust is a must”.

10.2 From IoT to a Data Driven Economy and Society

It is clear: in terms of pervasiveness, IoT has already contributed to the emergence of a society in which almost everything is or can be monitored. It is not new, nor can further roll-out be stopped. What is new, is the enormous amount of “Things” that are now connected to the Internet and that are collecting, storing and sharing information . . . and the further rapid growth of deployment of more “Things”[3] and the increasing ability of actors to access and analyze data generated by IoT and many other sources.

Now: whereas the levels of monitoring are very high and well beyond the imagination of George Orwell [4] in terms of what technically is possible, in Europe trust in government and society has remained at a relatively high level.

When Snowden revealed, starting in June 2013, some evidence reflecting the pervasiveness of monitoring through numerous global surveillance programs [5], many of them run by the NSA (National Security Agency) and the Five Eyes[1] with the cooperation of telecommunication companies and European governments, this resulted in widely expressed concern and even outrage by the general public, civil society and politicians.

This led to a global discussion making clear that monitoring is a necessity, yet should be proportional, and not take place at all costs, and a balance is yet to be found. This results in a discussion that will continue to stretch over the decades to come.

Overall, it is noted also by the European Parliament that surveillance and collection of data should be proportional and justified, noting that new legislation is underway in multiple EU member states that would allow broad collection of data and tapping of internet communications: also including IoT [6].

Within this setting, the discussion in Europe about privacy and data protection is finding its way, moving from a Directive on Data protection and privacy towards European legislation that will come into full force in May 2018. The reform is to strengthen individual rights and tackle the challenges of globalisation and new technologies, and “simplify” compliance by being applicable law in all EU member states, whereas the Data protection Directive originating from 1995 was applied by national governments in similar but not always the same way.

When the original Data Protection Directive was developed and agreed in 1995, the Internet was by far not as important as today, and nobody had even mentioned the term “Internet of Things” yet. A review of the 1995 Directive in 2009, sponsored by the UK Data Privacy Authority, already noted that new developments like IoT, data mashups and data virtualization are new challenges that had to be met [7]. The reform that led to the new General Data Protection Regulation (further: GDPR) has been under way since 2011 and culminated in a Proposal to Council and Parliament by the European Commission on 25 January 2012. This proposal was approved by the European Parliament in March 2014, and has now been finalized and ratified by Parliament and Council to come into force in May 2018.

[1] “Five Eyes”, often abbreviated as “FVEY”, refer to an intelligence alliance comprising Australia, Canada, New Zealand, the United Kingdom, and the United States that was formed. These countries are bound by the multilateral Agreement, a treaty for joint cooperation in signals intelligence.

With this, it should be noted that the work has not been completed. When this law was set up in outline in 2011, “BigData” was not yet an issue widely recognized, in that year new in the Gartner Emerging Technologies Hype Cycle.

Today, we know that BigData, and BigData analytics, fundamentally challenge the concept of “personal data” as through BigData analytics data that in isolation do not relate to persons often can be related to persons when combined with other data.

The 2014 Opinion from WP29[2] on IoT recognises the value of IoT, as well as the potential intrusions it can generate to privacy. In this Opinion, statements are made that alarmed businesses around the world now asking for guidance to the European Data Protection Supervisor, as what is suggested may put a lock on many current developments in the field.

In 2015, a Court Ruling by the European Court of Justice in the case of Maximillian Schrems versus the Irish data protection commissioner regarding the right of Facebook to transfer data to servers located in the USA under the Safe Harbour scheme further led to uncertainty about the legal situation. On 6 October 2015, the Court declared the Safe Harbour Decision invalid, as the protections under the Safe Harbour scheme provided by the US Authorities had proven to be inadequate, in particular because “*the scheme is applicable solely to the United States undertakings which adhere to it, and United States public authorities are not themselves subject to it. Furthermore, national security, public interest and law enforcement requirements of the United States prevail over the safe harbour scheme, so that United States undertakings are bound to disregard, without limitation, the protective rules laid down by that scheme where they conflict with such requirements*” and because for non-US citizens there is no opportunity to redress: “*legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, compromises the essence of the fundamental right to effective judicial protection*”.[3]

[2] The Article 29 Data Protection Working Party was set up under the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. It has advisory status and acts independently.

[3] ECJ ruling in case C-362/14 Maximillian Schrems vs Data Protection Commissioner, 6 October 2015, http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf

Currently, IoT providers such as the globally popular "Nest" smart meters and smoke detectors, owned by Google, still refer to "Safe Harbour Agreement" protection of personal data.[4] Whereas Nest explicitly commits to a number of privacy measures, it should be noted that today (2015) redress is thus not possible when a European citizen considers her or his privacy right to be violated and their data are kept in database physically outside of Europe. This is also true for companies such as Younqi (health bands) and many others that collect data and store them on US servers. The measures currently proposed by the European Commission to replace "Safe Harbour", known as "Privacy Shield", have not been accepted, yet, and await an advice from WP29. Note that the EU-U.S. "Privacy Shield" imposes stronger obligations on U.S. companies to protect Europeans' personal data and requires the U.S. to monitor and enforce more robustly, and cooperate more with European Data Protection Authorities. It also includes written commitments and assurance regarding access to data by public authorities. It should also be noted that this new agreement has not been tested in Court, yet, and until this is done and ruled to be a "valid agreement" uncertainty about this new protection remains.

Businesses are looking for guidance, as BigData is a subject of interest to many, and companies around the world are looking into the opportunities offered by BigData, data generation, collection, and analytics. IoT is a major driver in this, as "connected Things" will generated endless streams of data that will be captured and used. According to the European Data Protection Supervisor Peter Hustinx [8]: "*If BigData operators want to be successful, they should . . . invest in good privacy and data protection, preferably at the design stages of their projects*".

With this, he recognises the important of "soft law" at this point [9]. Investing in good privacy and data protection should be core in the innovation, development and deployment of IoT, and probably a pre-condition for European (co-)sponsored research. A way forward could include the habit/obligation of a Privacy Impact Assessment in every stage of design of new IoT products and services.

In his published Opinion on Digital Ethics [10], the European Data Protection Supervisor (EDPS) refers to Article 1 of the EU Charter of Fundamental Rights: '*Human dignity is inviolable. It must be respected and protected.*' From that position he further explains that: "*In today's digital environment, adherence to the law is not enough; we have to consider the ethical dimension of data processing*."

[4] https://nest.com/legal/privacy-statement-for-nest-products-and-services/

It is in line with this that some projects funded by the European Commission are looking very carefully at the issue of privacy protection and the idea of limiting the amount of information available to each entity. In general, the key issue to take into account while discussing privacy has to do with the integration of information from different sources. While a single stream of data might not contain enough information to invade the privacy of the user, it is recognized that the correlation and concurrence of information at an entity can lead to privacy considerations that were unthinkable only looking at the individual sources.

While the user is ultimately responsible for the data it allows to escape in the open, a modern individual that works and lives with current technologies cannot keep up with the types and amount of information being "leaked" by applications and websites. It is, therefore, for an individual virtually impossible to design privacy policies that are permissive enough to allow for services to work, while at the same time, restrictive enough that the privacy of the user is not compromised. Any specific harm or adverse consequence is the result of data, or their analytical product, passing through the control of three distinguishable classes of actor in the value chain [11]:

1. Data collectors, who may collect data from clearly private realms, from ambiguous situations, or data from the "public square," where privacy – sensitive data may be latent and initially unrecognizable;
2. Data analyzers, who may aggregate data from many sources, and they may share data with other analyzers creating uses by bringing together algorithms and data sets in a large – scale computational environment, which may lead to individuals being profiled by data fusion or statistical inference;
3. Users of analyzed data generally have a commercial relationship with analyzers; creating desirable economic and social outcomes, potentially producing actual adverse consequences or harms, when such occur.

As the complexity increases through technology, we will depend on technology to deal with it. It is crucial that automated and self-configuring solutions are offered that analyze the type and amount of information given away for a specific user and configure the appropriate number of policies to ensure that the level of security and privacy desired by the user is kept untouched. This goes beyond mere regulatory actions and requires robust and flexible technology solutions that work under very different conditions, and that are backed by legislation to ensure that abuse of technologies or data is subject to redress and legal action.

10.3 Way Forward with IoT

The Internet of Things and its underlying data streams shape an important part of that transformation by collecting and sharing data from a rapidly increasing amount of objects that are digitally connected in our lives, ranging from our cars to smart TVs, smart homes to smart cities, as well as natural disaster warning systems and air quality sensors network.

Drivers for IoT introduction include the need to address societal challenges in efficient ways, and to grab business opportunities that often come with new business models. There is no way back: the "promises" of IoT make further development unstoppable. Data generated and shared by objects connected through the Internet, combinable using smart algorithms, lead to a world in which privacy is getting a new meaning and where good security is more important than ever. IoT, in combination with BigData and data analytics in particular as an enabler of high quality real-time data provider, has become a real game changer.

Governments at all levels are confronted with this, and need to find responses, soon. Societal challenges need to be dealt with effectively, using less money and relying more on active participation of citizens and businesses, yet this cannot go at cost of a society we want in terms of trust.

IoT is currently mainly driven by business opportunity considerations and technology push, yet it is clear that people are waking up and become concerned on where this takes us. Consumers and citizens have to become involved in developing a "future we want" in which there is "respect for human dignity" as well as individual choice.

During meetings within the European IoT and Future Internet research community and the recently launched public private partnership *Alliance for Internet Of Things Innovation* (AIOTI), and in global forums such as the Internet Governance Forum's *Dynamic Coalition of the Internet of Things* (IGF DC IoT) and EuroDIG, these issues have been at the center of a dialogue between public, private, and civil sector stakeholders. There is an ongoing need to protect the public interest as well as to create space for innovation and experimentation using IoT products and services within the current and developing legal frameworks. To find this balance requires the active, well informed involvement of public authorities.

IoT can be used for many different things in many different ways, and practical experimentation in an ecosystem in which all stakeholders are involved will help understand the impacts of the IoT more profoundly than its technological specifications alone. In order to be "trusted" by its users, IoT will need to offer:

- Meaningful transparency – what is happening;
- Clear accountability – who takes responsibility;
- Real choice – "all or nothing" is not good enough.

Dialogues at global level have led to the insight that IoT needs to "go ethical". What this means exactly, and how it can work is still to be determined, with all stakeholders around the table. One thing is clear: we cannot continue to count on "adherence to the law". A good first step has been made with the draft declaration by the *2015 IGF Dynamic Coalition on Internet of Things Good Practices Policies* which can be found on the website of the IGF.[5]

10.4 Conclusions

It is clear that IoT and BigData have changed our ability to protect data to be related to individuals. At the same time, this doesn't mean we should give up on the right to privacy. To quote the EDPS: "*there are deeper questions as to the impact of trends in data driven society on dignity, individual freedom and the functioning of democracy*." And to quote the US President's Council of Advisors on Science and Technology [11]: "policy focus primarily on whether specific uses of information about people affect privacy adversely. It also recommends that policy focus on outcomes, on the "what" rather than the "how," to avoid becoming obsolete as technology advances. The policy framework should accelerate the development and commercialization of technologies that can help to contain adverse impacts on privacy, including research into new technological options. By using technology more effectively, the Nation [USA] can lead internationally in making the most of BigData's benefits while limiting the concerns it poses for privacy."

As Commissioner Ansip stated in his speech (spoken word) during the Net Futures conference in Brussels on 20 April 2016: "Trust is a must" for whatever we do on our way forward.

No stakeholder can do this alone. Businesses need to invest, governments need to protect the public interest which includes protection, ensuring redress and choice, the technical community needs to design and develop new and better approaches, and users need to be aware and "steer" investments and developments through conscious use.

Time to make technology work for us in a way that people can trust these technologies is now. Let's make sure we reflect our awareness of and

[5] http://review.intgovforum.org/igf-2015/dynamic-coalitions/dynamic-coalition-on-the-internet-of-things-dc-iot-4/

commitment to this ethical side in every step we do when developing and deploying new technologies and services that collect, store, share, protect and act on data.

For those of us who have read Asimov's book "*I, Robot*" [12]: remember the Three Laws of Robotics which in fact could relate to all intelligence developed, and apply them to whatever connected intelligence you work on – no harm to be done to people. Indeed, Isaac Asimov, describes the three laws that set the way forward for robots: 1st Law: A robot may not injure a human being or, through inaction, allow a human being to come to harm; 2nd Law: A robot must obey the orders given it by human beings except where such orders would conflict with the First Law; 3rd Law: A robot must protect its own existence as long as such protection does not conflict with the First or Second Laws.

References

[1] Helen Rebecca Schindler, Jonathan Cave, Neil Robinson, Veronika Horvath, Petal Jean Hackett, Salil Gunashekar, Maarten Botterman, Simon Forge, Hans Graux. *Europe's policy options for a dynamic and trustworthy development of the Internet of Things*. Report for the European Commission under SMART 2012/0053. June 2013.

[2] Tableau Software. *Top 8 Big Data trends for 2016*. Report.

[3] Maarten Botterman. *Opening towards a new reality*. Policy paper on IoT Future Technologies for the European Commission DG CONNECT. Rotterdam, April 2015.

[4] George Orwell. 1984. *Secker and Warburg*. June 1949.

[5] Glenn Greenwald, Ewen MacAskill and Laura Poitras. *Edward Snowden: the whistleblower behind the NSA surveillance revelations*. the Guardian, June 2013, http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.

[6] Niels Muiznieks. *Europe is Spying on you*. NY Times http://www.nytimes.com/2015/10/28/opinion/europe-is-spying-on-you-mass-surveillance.html?_r=0, October 2015.

[7] Neil Robinson, Hans Graux, Maarten Botterman & Lorenzo Valeri. *Review of the EU Data Protection Directive*. prepared for the Information Commissioner's Office, TR-710-ICO. Cambridge, May 2009.

[8] Mark Say. *Big data needs big guidance*. Financial Times. Retrieved http://www.ft.com/cms/s/0/fab4bae8-7f88-11e4-86ee-00144feabdc0.html#axzz3O8I1GAvc on 2015.01.07, December 2014.

[9] RAND. *Europe's policy options for a dynamic and trustworthy development of the Internet of Things*. June 2013.

[10] European Data Protection Supervisor. Opinion 4/2015. *Towards a new digital ethics: Data, dignity and technology*. EDPS, September 2015.

[11] Executive Office of the [USA]. *Big Data: Seizing Opportunities, Preserving Values*. President PACT report. May 2014.

[12] Isaac Asimov. I, Robot. Gnome Press December 1950.