Privacy and security in the Internet of Things: challenge or opportunity

November 2014

OLSWANG

Privacy and security in the Internet of Things: challenge or opportunity

by Blanca Escribano

"As more and more of our devices become smarter and smarter, it is essential we know as much about them as they know about us – that we understand what information the devices are collecting and how it is being used or shared."

FTC Chairwoman, Edith Ramirez (November 19, 2013)

Why are privacy and security hot topics in the development of IoT-M2M?

Do you think you know your personal objects well? What do you know about your home electronics' social lives? This conversation could seem absurd, unless you were aware that objects are capable of having their own Twitter accounts[1]. A connected environment - in which every object is connected (clothes, furniture, traffic lights, cars, home security cameras, medicine boxes – even implants?) - interacts with social networks and sends data to be stored in the cloud, enabling aggregation of data from different devices and aspects of our lives, is enough to make us believe that we are reading the next volume of *Brave New World* (Aldous Huxley, 1932) or watching one of the sequels to *The Matrix* (The Wachowskis, 1999).

The extent to which the Internet of Things (**IoT**) will develop depends on how all the data potentially collected is transformed into something useful and commercially viable, and on how cloud and predictive analytics will interact with the IoT-M2M ecosystems. But in such a context, we can better understand why privacy and security are considered as one of the main downsides to IoT, being the biggest concern not only for consumers but also for service providers. That is what the EU Commission's public consultation on IoT governance and the FTC's latest debates have shown very clearly: there is a global existing need for implementing security measures that are capable of minimising the impact of a cyber-attack and unlawful profiling and surveillance of individuals.

Some of the data protection and privacy challenges raised by IoT are new, but many others are traditional, albeit amplified due to the exponential increase of data processing involved. For example:

- not all IoT-M2M products and services have a privacy component to them, but when there is one (or information is aggregated with data from other services) it can give a detailed view of all facets of a user's life (e.g. wearables, connected cars, connected homes);
- the IoT value chain is long and complex and significant number of stakeholders are involved in the data processing;

[1] Andy Piper, 2014: "Combining context with signals in the IoT"

- IoT relies on the principle of the extensive processing of data through sensors that are designed to communicate unobtrusively and exchange data in a seamless way;
- the exponential volume of data that can be collected, and its further combination, its storage in the cloud and the use of predictive analytics tools can transform data into something useful but also allow companies - and potentially malware - to have very detailed profiles of individuals; and
- the sharing and combination of data through cloud services will increase the locations and jurisdictions where personal data resides.

All of these factors raise significant privacy compliance challenges.

What are the regulators' approaches?

In the **USA**, the FTC brought its first-ever enforcement action stemming from an Internet of Things device in December 2013 against TRENDnet, the maker of a surveillance camera system with a range of uses from home security to baby monitoring. It needs to be mentioned that the ruling almost coincided with the FTC workshop on IoT. At that workshop, the FTC anticipated some best privacy practices, implementing the core principles of privacy by design, simplified consumer choice and transparency for the IoT world and announced then that its next step would be to prepare a report outlining recommended best practices for smart devices (that report is still awaited at the time of writing this article). Those best practices, together with the forthcoming bills for the Black Box Privacy Protection Act and the "We Are Watching You" Act, will probably provide much more guidance to the ecosystem.

New data protection policies are being implemented now across the different **Asian** countries and it is still early to guess how the challenges of IoT will be tackled.

In **Europe**, the EU institutions are currently in the process of negotiating a General Data Protection Regulation (GDPR 2012/0011) that will replace the existing Directive 95/46/EC) providing a more harmonised framework across the 28 EU member states The GDPR Draft is currently pending approval by the Council, before three-way negotiations between the EU institutions to reach a compromise text can begin. At the earliest, the new Regulation, if agreed by the target date of May 2015, could be in force by mid-2017. For our latest coverage of progress click here

The Draft introduces some provisions that are relevant for dealing with the IoT/M2M ecosystem and its data protection challenges, for instance, those related to data portability, privacy assessments, privacy by design and privacy by default, those related to profiling, the right to be forgotten and the new interpretation of consent. Whether or not these are the appropriate tools for this new reality of connected living is an open question.

The European Article WP29 Opinion on IoT

And those concepts and principles in particular are the issues that the Data Protection European advisory body on data protection and privacy, the Article 29 Data Protection Working Party (**WP29**), has recently discussed in its first Opinion on IoT (Opinion 8/2014 on the Recent Developments on the Internet of

Things).[2] Indeed, despite the fact that the WP29 IoT Opinion is based on the current Directive 95/46/EC, it proposes solutions and approaches to IoT that are reflected in the Draft GDPR. So does the WP29's recently published smart metering Recommendation[3].

The WP29 Opinion focuses on three IoT developments: wearable computing, quantified self and home automation, leaving apart the specific problems of smart cities, smart transportation or M2M.

Key privacy challenges of IoT

The privacy and data protection challenges related to IoT that WP29 identifies are:

(i) **lack of control and information asymmetry** (interaction between objects that communicate automatically and by default, between objects and individuals´ devices, between individuals and other objects, and between objects and back-end systems, which will result in the generation of data flows that can hardly be managed with the traditional tools used to ensure the adequate protection of the data subjects' interests and rights);

(ii) **quality of the user´s consent** (the possibility of rejecting certain services is not a real alternative in IoT and classic mechanisms used to obtain consent may be difficult to apply, therefore, new ways of obtaining the user´s valid consent should be considered, including implementing consent mechanisms through the devices themselves as privacy proxies and "sticky" policies (conditions and constraints attached to data that describe how it should be treated);

(iii) **inferences derived from data and repurposing of original processing** (secondary uses of data, inferences from "raw" information, sensor fusion, make important that at each level IoT stakeholders make sure that the data is used for purposes that are compatible with the original purpose of the processing and that those purposes are known by the user);

(iv) **intrusive identification of behaviour patterns and profiling** (generating knowledge from trivial or even anonymous data will be made easy by the proliferation of sensors and that might enable very detailed and comprehensive life and behaviour patterns);

(v) **limitations on the possibility of remaining anonymous when using services;** and

(vi) obviously, **security risks** - weak points can occur not only at device level but also in the communication links, storage infrastructure and other inputs of this ecosystem.

[2] There are previous WP29 opinions that anticipated some of the hot topics now dealt in the IoT Opinion, such as the one on apps on smart devices, the Opinion on anonymisation techniques, the one on smart grids and smart metering and the first of its kind, the Opinion on RFID apps.

[3] Commission Recommendation of 10 October 2014 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems (2014/724/EU).

Key points from the WP29's legal analysis

The WP29 provides some guidelines on how the main data protection EU law concepts should be applied to IoT. Regarding **applicable law,** the *Google Spain* ruling has confirmed that when the establishment of the controller is outside the European Union, European law still applies if it makes use of equipment situated on the territory of a Member State. The meaning of equipment is defined by WP29 as "*all objects that are used to collect and further process the individual's data in the context of the provision of services in the IoT".*

Personal data is also interpreted broadly, because the large amount of data processed automatically in the context of IoT entails risks of re-identification. Thus, even data relating to individuals that is intended to be processed only after the implementation of pseudonymisation, or even of anonymisation techniques, may have to be considered to be personal data. In the same way, the processing of data may also concern individuals who are neither subscribers nor actual users of the IoT (the classic example is a data subject regarded/recorded by someone wearing smart glasses). For that reason, privacy icons and sticky policies are under discussion.

The application of EU data protection rules is not dependent on the ownership of a device or terminal but on the processing of the personal data itself, regardless of who the individual identified by this data is. The owner of the IoT device and the person whose data will be monitored (**data subject**) might be different people. It must be highlighted that the WP29 considers that end-users should have access to raw data registered in IoT devices in order to give them capacity to port their data to another data controller and switch services. WP29 considers **the right to portability** as part of the access right, which should also be complemented by data interoperability standards. In addition, on the data subject's right to withdraw **consent** and to object to the use of their data, the WP29 raises the issue of **the "right to be disconnected"**: "*data controllers should offer an option to disable the "connected" feature of the thing and allow it to work as the original, unconnected item […]. Data subjects should have the possibility to "continuously withdraw (their consent), without having to exit the "service provided*". But what is currently under discussion is the right to be invisible, disconnected from the "connected living" concept. As Bernard Benhamou very graphically described it, *¨the silence of the chips¨*.

From a legal point of view, one of the most sensitive issues in IoT is the allocation of legal responsibilities among **data controllers** based on the specifics of their respective interventions (device manufacturers, social platforms, third-party applications, device lenders or renters, data brokers or data platforms). In other words, is your smartphone operating system liable for your connected car accident?

Practical recommendations

Finally and most interestingly, the WP29 lists a number of **recommendations** that the WP29 deems useful in order to facilitate the application of EU legal requirements to the IoT. It provides some common recommendations to all stakeholders and other specific ones for the different stakeholders across the value chain (OS and device manufacturers, application developers, social platforms, IoT device owners and additional recipients and standardisation bodies and data platforms). See the table below. The recommendations common to all stakeholders are:

- the performance of **Privacy Impact Assessments** prior to the launch of any new IoT application;

- stakeholders must **delete** raw data (if possible at the nearest point of data collection) as soon as data required for data processing is extracted;
- **privacy by design and privacy by default** principles should be applied;
- the **user should be in control** of the data at any time and for that purpose, offering a right to refuse/request consent should be made as user-friendly as possible (understandable and not hidden in a general privacy policy); and
- devices and applications should be designed so as to **inform** users and non-user data subjects.

For the specific stakeholders, most of the recommendations have been mentioned above, but those addressed specifically to OS and device manufacturers are also worth mentioning. These include that OS and device manufacturers should:

- **inform users** about type of data collected and processed and they should inform other stakeholders in the value chain as soon as the data subject withdraws its consent or opposes data processing;
- **offer granular choices** when granting access to applications as for instance, a "do not collect option" to schedule or quickly disable sensors;
- data (including aggregated data) should be stored and exported in a structured/commonly-used/standardized format allowing **data portability**;
- **security by design** should be followed;
- ensure that devices are capable of distinguishing between **different users** using the same device, and enable local control of data through personal privacy proxies; and
- **work together with standardisation bodies and data platforms to sup**port **common protocols** for preferences with regard to data collection/processing.

A few words on security

There is an understandable general concern about the risk of cyber-attacks on IoT devices or networks, as these could lead to catastrophic events. Security breaches can entail significant privacy risks for the individuals whose data are processed.

The potential targets may include new endpoints such as smart homes, cars, buildings or cities. If we think about a virus or a hacker attacking endpoints like a traffic management big data centre, a medical device, or even a toaster, we can imagine consequences like city traffic chaos and car crashes, a hospital power failure, or even a fire caused by a malicious extension of cooking time in a toaster.

The need to protect crucial electronic infrastructure against terrorism and other threat vectors has increasingly manifested itself internationally in recent years. In the EU, the European Programme for Critical Infrastructure Protection (2006), followed by the Critical Infrastructure Directive 2008/114/EC[4], the subsequent Critical Information Infrastructures package and its recently proposed cyber-security strategy, which included a proposed Network and Information Security Directive[5] (NISD), have triggered the

[4] Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

[5] Network and Information Security Directive (2013/0027(COD).

implementation of different legal instruments across the different Member States. While the Critical Infrastructure framework aims to protect general societal interests, the Security framework focuses more on combating specific criminal incidents.

But IoT is not formally defined in current legal initiatives, and it is therefore not unambiguously covered or exempted under existing legislation, including the Critical Information Infrastructure Directive and the proposed NISD. In order to trigger the mandatory protection through the existing mechanisms, it would need to be specifically mentioned as one of the sectors/infrastructures to be protected. At the time this was written, there is still uncertainty on the final scope of infrastructure to be caught by the NISD and therefore, on the impact on the IoT front.

The IoT value chain is long and complex and security should be monitored across all the components in the chain, in a way that makes it easier to detect liability in the event of a data breach or infringement of the security protocols. A security breach might originate from any one of multiple stakeholders, especially when considering M2M environments based on exchange of data among devices.

Data controllers should perform security assessments of systems as a whole, including assessments at component level and applying principles of composable security. In the same way, use of certification for devices as well as the alignment with internationally recognised security standards could improve the overall security of the IoT ecosystem and minimise legal exposure. As mentioned above, in applying the "privacy by design principle", most importantly, security should be built-in from the very outset and be on top of standards.

Summing up, privacy and security find a challenging field in the IoT. There are some jurisdictions, like the US and the EU, where regulators have already given some thought to finding the right approach and solutions to ensure that the IoT ecosystem doesn't find itself road-blocked. However, given that the IoT is global, there are still many open questions and problems that need further thinking and harmonisation. As a final remark, and again paraphrasing the FTC Chairwoman "*The difficulties will be exponentially greater with the advent of the IoT, as the boundaries between the virtual and physical worlds disappear*".

Consumers' fear of potentially intrusive new technologies is one of the main barriers to the adoption of the Internet of Things. Stakeholders who can demonstrate privacy compliance and ethical practices will be best placed to win consumers' trust and gain competitive advantage in this brave new (connected) world.

What are the obligations on players in the IoT value chain?

The following table aims to provide an overview of the different obligations which arise under each of the main data protection principles that are applicable generally to all stakeholders in the IoT value chain.

	All players in the IoT value chain	Device manufacturers	App developers	Social platforms	Device owners and additional recipients	Data platforms/ standardisation bodies
Privacy Impact Assessments	Prior the launch of any app	✓	Special attention to sensitive personal data	✓	✓	Standardisation bodies to develop encryption and communication protocols
Privacy by design and default	✓	Disable wireless interfaces when not used and use random identifiers	Minimise the amount of collected data	-Default settings of apps should ask users to review/edit/decide before publication -Information should by default not become public/indexed by search engines	✓	✓
Control by the user	✓	Provide tools to modify data before transferred	User friendly	✓	-Not economic penalization or service degradation when not use a service/device -Access and opposition rights should be enabled to any user/non-user data subject (with or without contractual relationship)	✓
Transparency	User friendly (not in general PPs on websites	-By design (as to inform users and non-user data subjects) -Communicate value chain when consent is withdrawn -Offer granular choices on type/frequency of collection -Distinguish between users -Enable local control/storage of data (not at the manufacturer)	-By design (as to inform users and non-user data subjects) -periodically notify recording mode	✓	Non users data subjects should be informed of the presence of IoT devices/type of collected data	✓
Portability	✓	-Store/port standardized format. -Aggregated data -work with platforms and	Raw and aggregated data in a standard and usable format	✓	✓	-Clear and self-explanatory data formats for portability and interoperability -Certified standards
Minimisation	Deletion of raw data after extracting required data (at the nearest point of collection)	✓	Not access aggregated data if row is sufficient for purpose	✓	✓	-Format for raw and aggregated data -Few strong identifiers as possible to facilitate anonymisation

Contacts

Blanca Escribano
Partner, Madrid
+34 91 187 1924
blanca.escribano@olswang.com

Purvi Parekh
Partner, London
+44 (0)20 7067 3524
purvi.parekh@olswang.com

Ross McKean
Partner, London
+44 (0)20 7067 3378
ross.mckean@olswang.com

Anthony Waller
Partner, London
+44 (0)20 7067 3461
anthony.waller@olswang.com

Andreas Splittgerber
Partner, Munich
+49 89 206 028 404
andreas.splittgerber@olswang.com

Sylvie Rousseau
Partner, Brussels/Paris
+32 2 641 1272
sylvie.rousseau@olswang.com

Rob Bratby
Partner, Singapore
+65 9832 2898
rob.bratby@olswang.com

Matt Hunter
Associate, Singapore
+65 9827 8711
matthew.hunter@olswang.com

OLSWANG

Berlin	+49 (0) 30 700 171 100
Brussels	+32 2 647 4772
London	+44 (0) 20 7067 3000
Madrid	+34 91 187 1920
Munich	+49 89 206 028 400
Paris	+33 17 091 8720
Thames Valley	+44 (0) 20 7067 3000
Singapore	+65 67208278

www.olswang.com

18789565