

European Privacy and Data Protection Commissioners' Conference
Prague, Czech Republic, 29 April 2010

"Internet of things: ubiquitous monitoring in space and time"

Giovanni Buttarelli

Assistant European Data Protection Supervisor

Dear colleagues,

I have been asked to talk about the data protection issues surrounding the Internet of Things. RFID is a building block, probably "the key" component of the future Internet of Things. Therefore, I will often refer to RFID and the Internet of Things as equivalents.

To discuss the data protection issues regarding the Internet of Things, I would like to discuss the following points:

First, I would like to give you an overview of the reality of the Internet of Things. To give you a hint of what life may look like when the Internet of Things becomes a reality

Then, I want to have a look at the steps taken by the Commission to tackle this forthcoming reality, and particularly at the legal issues. I will give you some examples of how the current data protection legal framework would apply to this reality.

Third, I will address the question of whether the Internet of Things challenges the current data protection framework. In particular, whether the current data protection framework needs to be amended to continue providing adequate protection. In this regard, I will **finalize** by suggesting some policy developments and approaches that may be necessary if we want individuals to be adequately protected when the Internet of Things becomes a reality.

I. Overview of the Internet of Things

Internet of Things will not appear in overnight. We can safely expect that islands of IoT environments will be built in dedicated and specialised locations and will be progressively connected to each other. As an illustrative example of this emerging phenomenon, the latest report of the European Network and Information Security Agency purposefully selected the area of an airport to study and assess in a prospective way the risks related to this specific IoT environment¹ i

The Internet of Things is becoming a reality due to three basic and fundamental trends which are driving the development of the Information Society and its components.

1. Even if at the level of the tag the size of the bandwidth might remain limited, the real “torrent” of data produced by the tagged objects populating the IoT will be easily transported by the network (internet or a parallel one).
2. The continuous and endless increase of storage capacity together with a huge decrease of cost production (a trend which follows the famous Moore law) offer the possibility to store all the activity of the IoT without constraint or limit; and maybe also without an additional motivation for adopting a more rigorous data retention policy In some cases it is already cheaper to keep stored data than to safely erase it.
3. Last but not least, the ambient intelligent space which is now called the IoT can exist only because all these objects will be able to be connected to the network anywhere or will even play the role of an extension node of this network.

The quote “[the Internet Society] evolves from a network of interconnected computers to a network of interconnected objects...and thus create an ‘Internet of things’ “comes from the EU communication on the Internet of Things published in June 2009² and has been built on the 2005 ITU report³. This sentence describes adequately the complex and intertwined environment the EU privacy and data protection framework will have to cope with.

¹ <http://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/flying-2.0-enabling-automated-air-travel-by-identifying-and-addressing-the-challenges-of-iot-rfid-technology-2/flying-2.0-enabling-automated-air-travel-by-identifying-and-addressing-the-challenges-of-iot-rfid-technology>

² http://ec.europa.eu/information_society/policy/rfid/documents/commiot2009.pdf)

³ http://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-IR.IT-2005-SUM-PDF-E.pdf

I.1. Internet of Things converges the digital and the off line worlds

The convergence of the real and digitized worlds⁴ is facilitated by the ever-increasing number of bridges created by both the innovative use of existing technologies and the development of new and emerging technologies. However, the proliferation of these bridges tends to blur the borders between environments which may not currently be governed by the same legal framework, and therefore creates legal uncertainties which can undermine trust and be detrimental to the development of the Information Society.

The convergence of these two worlds into a seamless space for the individual is undoubtedly creating new challenges for the EU privacy and data protection legal framework. The objective is of course to clearly reconcile the online and offline environments under a single harmonised umbrella or at least to provide an enhanced interoperability between them, in order not to jeopardise trust in this promising digital age and consolidate/preserve EU data protection principles.

I.2. A case study

A crime investigation⁵ is a very interesting case study for this forthcoming Internet of Things as it simultaneously highlights both the new capabilities offered by such environment where every single action of objects and individuals can be monitored from a time and space point of view, and the lack of "natural" limits which were preserving the privacy of the data subject so far. All the elements which are located inside the zone usually demarcated in the famous US movies by a yellow tape will be able to "speak" and contribute to the investigation. The key challenges here will be to set the limits to this powerful monitoring availability.

II. The actions of the European institutions and bodies regarding the Internet of Things

⁴ Beslay, Laurent, Hannu Hakala: Digital Territory: Bubbles. In: Paul T. Kidd (Ed.): European Visions for the Knowledge Age: A Quest for New Horizons in the Information Society, Cheshire Henbury, 2007, pp. 69-78

⁵ Beslay, Laurent, Hannu Hakala: Digital Territory: Bubbles. In: Paul T. Kidd (Ed.): European Visions for the Knowledge Age: A Quest for New Horizons in the Information Society, Cheshire Henbury, 2007, pp. 69-78

The European Commission has been involved on the issue of the Internet of Things in different ways, ranging from running on-line consultations to high level groups, etc. In March 2007, it issued a Communication on RFID, followed by RQO Recommendation on RFID and on Internet of Things in 2009.

Following the actions of the European Commission, the EDPS also contributed to the exploratory exercise of the Internet of Things and issued an opinion on the 2007 Communication in December 2007. The EDPS was also informally consulted on the draft recommendation (during the interservice consultation) and participated in a series of conferences and workshops on IoT.

You may also remember that the Article 29 Working Party issued an opinion on RFID interpreting how to apply the data protection legal framework to RFID applications.

III. The application of the data protection legal framework

I am convinced of the potential of the Internet of Things to bring very positive aspects to our lives. However, at the same time, the Internet of Things poses a number of problems. The issue of how to deal with privacy and security of personal information is among them.

I am convinced that the basic values and fundamental principles embodied in the Directive 95/46 are fully applicable and relevant in this context. However, we need to use our imagination to find new ways to apply these principles in the new, evolving information and communication technologies scenario.

Take for example, **the information principle** embodied in Articles 10 and 11 of the Directive, also referred to as transparency. The Internet of Things emphasizes the need for individuals to be informed. New ways of informing people will need to be found so that information is given in an efficient way. For simple RFID tags in consumer products it will be necessary, for example, to put logos on the products. In addition it will be necessary to find ways to tell people about the existence of readers and whether they are active. It will be necessary to educate consumers and find ways to communicate

effectively with them so that an average consumer understands the implications of the RFID tags attached to consumer products. At the same time, I am aware of the challenges. If we end up in a reality where we are surrounded by tags and readers, it will be very difficult to implement and enforce the information principle. In this regard, the motto for me is to look for practical and efficient ways that deliver their intended results.

The need for **legal grounds** ex Article 7 and 8 to legitimise the data processing continue to be relevant in this environment. Personal data can not be processed unless the data controller has legal grounds. In many cases, consent as defined in the Directive will be required. For example, this is the case of RFID tags in consumer products. At the point of sale, individuals should be asked whether they want to have the tag “on” after the point of sale. Opt out regimes are not likely to meet the definition of consent under the Directive. However, it may be necessary to find efficient ways to enable individuals to opt in. They should be efficient meaning that it is neither feasible nor realistic to imagine that for each item individuals will be asked whether they consent. I think that it is up to industry and stakeholders to propose solutions. Our task will be to assess whether these new ways deliver their intended and expected results. It is also important to realise that individuals may wish to revoke their consent. This may be referred to as the "silence of the chips", meaning that chips should have inbuilt the capability to be "switched off".

In this context, it is essential for those who deploy RFID applications and the much wider Internet of Things to implement *security safeguards*. It is crucial to avoid the tags being ‘read’ by other people. All the measures should be implemented to ensure that RFID tags do not reveal personal information ‘by default’. Obviously, security measures should be applied not only to the tags but also to the databases that are linked to them.

The application of the above principles, as you know, is based on the existing data protection legal framework. The principles are therefore fully applicable in this environment. However, I think that you will concur with me in saying that it will be necessary to find new ways to implement them and this is likely to be challenging.

III. The need for additional policy measures

As discussed above, clearly the EU data protection legal framework provides for safeguards to protect individuals' personal information and privacy, also in case of the Internet of Things.

This is, however, no simple matter. Although the principles of the data protection legal framework are applicable, there are some challenges when it comes to actually applying them in practice. This is because of technological developments and new global realities, which were not accounted for when the Directive was adopted. While some of such challenges may simply be solved by interpretation and flexibility, perhaps more may need to be done.

Let me just refer to a few challenges.

The first one is the question of simple item level tagging. We hear from industry that such tagging does not involve the processing of personal data and therefore there is no need for them to apply any data protection safeguards. However, it is obvious that such information may easily be 'linked' to other information that may identify individuals and more particularly may influence them. ID tags may easily be used to single out individuals. Therefore, we need to anticipate such possible 'future' linkages and take the necessary safeguards. If we do not- the risks are high.

This is connected to the need to implement measures to prevent these linkages, in other words, to prevent the use of ID tags to single out and influence individuals. This is independent of whether the tags themselves process or not personal data. In fact, it would be a measure to prevent future personal data processing.

In this context one may question whether it would be suitable to require by law that by default RFID tags, particularly in consumer products, would be put in the market in a non-active way. It is questionable whether this may be achieved under existing data protection legislation, particularly when the tag does not contain and there is no intention to link it to personal data. In my view, there are strong arguments supporting the view that additional legislation imposing "by default" RFID tags is necessary.

In this context, there is also a question related to the responsibility of designers and manufacturers of such devices in a 'privacy friendly way'. This raises the question of whether the Directive could be further reinforced with a new principle of privacy by design, a suggestion endorsed by the Article 29 Working Party to which I fully subscribe.

IV. Where do we go from here?

I would like to finalise with some conclusions:

First, I think that we can reiterate that the principles of EU law remain relevant and fully applicable the Internet of Things. However, there are some important challenges in the way these principles apply. To meet these challenges, it may be necessary to use several solutions.

Second, we need interpretation and guidance. The WP29 will need to play an active role in interpreting how to apply the existing laws and principles to the Internet of Things. This job started with the Opinion on Internet of Things. In the next Working Party 29 we will hear about the RFID privacy impact assessment proposed by industry. The Working Party opinion will be crucial.

As I said earlier, we will need to tackle these issues with an open mind and be practical without jeopardising the rights of individuals.

Third, so far, the approach used to ensure that RFID and the Internet of Things respects individuals' rights has been to rely on existing law with additional soft law instruments. This has been good so far but is probably not enough. We may need some legislative changes aimed at fixing some problems while keeping the main principles unchanged. Particularly, I see that the following may be necessary:

- A) A general principle of accountability and 'privacy by design. These two principles should give strong incentives to ensure that the Internet of Things is privacy friendly by default.
- B) It is uncertain whether general principles will be sufficient. For example, in the case of RFID tags in item level tagging, it may be necessary for the Commission to provide

for the opt-in principle at the point of sale pursuant to which all RFID tags attached to consumer products would be deactivated by default at the point of sale.

Thanks for your attention.