IoT Privacy, Data Protection, Information Security

It is understood, that Privacy and Data Protection on the one hand and information security on the other hand are narrowly linked areas despite of possible overlapping requirements.

This document provides a view on the challenges and objectives of IoT privacy, data protection and security, possible options and impacts.

The Issues / Challenges

As defined by CASAGRAS the Internet of Things is understood to be "a global network infrastructure, linking physical and virtual objects through the exploitation of data capture and communication capabilities. This infrastructure includes existing and involving Internet and network developments. It will offer specific object-identification, sensor and connection capability as the basis for the development of independent cooperative services and applications. These will be characterised by a high degree of autonomous data capture, event transfer, network connectivity and interoperability."

IoT is expected to enable mass participation of end users (individuals) on mission critical services (energy, mobility, legal and democratic stability). Smart objects are not only drivers for change in terms of content, and applications. Given their ability to potentially change in function because they can be digitally enhanced and "upgraded" they may acquire disruptive potentiality that could lead to serious repercussions.

It's a matter of fact that if IoT become omnipresent – everyone (individuals and enterprises) will be concerned. Also crosslinking of objects offers new possibilities to influence and to exchange. This leads to a variety of new (as well as already known) potential risks concerning information security and both privacy and data protection, which must be considered. The severity and likeliness of each risk will depend on the circumstances in which each IoT application / system is deployed.

IoT can be expected to contain huge numbers of sensors collecting and passing on data about environmental conditions, physiological measurements, and machine operational data. In addition to the computing devices that consumers use today such as laptops, games consoles and smart phones there will be many devices and appliances with embedded processors running applications (smart things) that people make use of. Many smart things will also be capable of actuation to take physical actions as a result of application control. Smart things are envisaged to provide health care, domestic functions, entertainment and many new uses not yet identified.

In a nutshell, we consider the following features for the vision in IoT:

- Four key technology areas provide the basis for IoT: pervasive identification and addressing, processing, networking and sensing
- Communication will take place at an object to object and object to person basis
- The amount of individuals' data collected and processed will increase substantially and will come from various different sources (object identifiers, sensor data etc.)
- Most communications will occur automatically objects will decide to exchange data with their environment, potentially without the user being aware of it
- Objects are heterogeneous, providing different functionalities depending on the context of their applications

Based on the features identified above, we have identified some major challenges and issues with regard to privacy & data protection and information security.

In general, we consider that privacy & data protection and information security are complementary requirements for IoT services. In particular, information security is regarded as preserving the confidentiality, integrity and availability (CIA) of information¹. We also consider that information security is perceived as a

For more information on the definition of information security, please refer to ISO/IEC 27000 "Information technology — Security techniques — Information security management systems — Overview and vocabulary"

basic requirement in the provision of IoT services for the industry, both with a view to ensure information security for the organisation itself, but also for the benefit of the citizens.

We could say that regarding information security, the general information security requirements should apply for IoT; however, since IoT is a special case and more of a vision rather than a concrete technology, we understand that it is complex to properly define all the requirements yet. From various studies already performed for identifying potential risks in such highly interconnected environments, we can note the following.

Ensuring continuity and availability in the provision of IoT-based services – a very important challenge is to ensure availability and continuity in the provision of these services, and to avoid any potential operational failures and interruptions. This directly relates to the architectural model to be followed in the provision of the IoT-based services: centralised versus de-centralised (link to the Architecture sub-group fiche, where this is also discussed). For example, considering the case of smart grids / meters; the meters can be programmed remotely by an attacker, this could cause major blackouts and it may be very difficult or impossible to resume the power supply to the home; which means that some functions may impact the availability of the grid.

It should also be reminded that not only data related to an identified person has to be considered as personal data, but that this also holds true for data related to persons whose social identity (name, address, ...) is not directly known, but might be revealed e.g. via the identification of a specific object or the combination of data from different sources.²

Design considerations for IoT technologies – Information security, privacy and data protection should systematically be addressed at the design stage. Unfortunately, in many cases, they are added on later once the intended functionality is in place. This not only limits the effectiveness of the added-on information security and privacy measures, but also is less efficient in terms of the cost to implement them. Moreover, the IoT objects do not always have enough computing power to implement all the relevant security layers / functionalities; the heterogeneity of objects becomes very challenging in this context. Similarly, the heterogeneity of privacy policies needs to be taken into account.

The risks are context-aware and situational – The more the individuals are involved in the process, the more privacy considerations and policies become context-aware and situational, and thus more complex to identify and assess. Concerning the identification of privacy, data protection and security risks, it depends on the context and the purpose of the objects that are considered (e.g.: health, geolocation ...). For example, in the context of smart energy management applications such as smart homes and smart grids applications: how to ensure that some principles of privacy and data protection, like informed consent and data minimisation, can survive in an automated and open environment?

Traceability / profiling / unlawful processing – The increased collection of data may raise issues of authentication and trust in the objects. In addition, it should also be noted that by using information collected about and from multiple objects related to a single person, that person may become more easily identifiable and better known.

Repurposing of data / mission creep challenge is amplified in an IoT environment – Due to the proliferation of increased amounts of data in an IoT environment, the existing challenge that data will be used for purposes in addition or other to those originally specified becomes even more serious to consider. Repurposing of data can be in the cards even before data collection begins, e.g. law enforcement authorities or intelligence agencies may seek access to data collected by others for specified purposes. This is not just in relation to the violation of individual rights to privacy but also may impact on wider social and public acceptance.

Exercising data protection rights for individuals and compliance with DP legislation for organisations – The implications of IoT on the possibilities for data subjects to exercise their data protection rights and

For the definition of personal data see Article 2 (a) of 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

questions on how to apply the data protection principles in this field, need to be considered. With IoT applications operating in the background, individuals might not even be aware of any processing of personal data taking place. Moreover, data access and controllership, permission to gather data and the optimum frequency of data collection are all issues to carefully consider and address.

Loss / violation of individuals' privacy and data protection – The natural characteristic of IoT environment is the prevalence of devices, sensors, readers, and applications which have the potential to collect a multiplicity of data types of individuals as they move through such environments. The possibilities to automatically identify objects may lead to an automatic identification of persons that are related to these objects³. The information collected based on object identifiers, sensor data and the connection capabilities of IoT systems might therefore reveal information on individuals, their habits, location, interests and other personal information and other preferences stored for ease of use in systems. In combination with data available from other services or sources data mining activities might even create new knowledge on individuals that might not be revealed by separately examining the underlying data sets. Increased concerns here relate to failure of electronic identification and identify theft. A recent example for this problem can be found in implementations of contactless credit cards, from which the name and card number can be read without any authentication. With this data it is possible for attackers to purchase goods with the identity and bank account of the card holder.

Realisation of malicious attacks against IoT devices and systems – Compromising of IoT systems due to inadequate or inappropriate information security controls in place is a very important risk, since this may lead to subsequent risks, some of them already mentioned here. The challenge is to identify these controls appropriately for the IoT systems, for which we are not yet certain how exactly they will evolve. These may also need to be defined for each system, and it also depends on the final IoT architecture (distributed or centralised). However, since it is expected that more data would be in transit than in traditional architectures, there is an increased risk of realisation of attacks and obtaining non-authorised access to data being transmitted.

User lock-in – as in the case of existing applications and technologies (e.g. cloud computing and social networking) there is an increased risk of consumers being locked-in a specific IoT service provider, making it difficult for them to migrate from one provider to the other and reduce their data portability. Such a dependency would be detrimental for users having control over their data and the right to choose providers.

Health related implications – Rapid advancement of ICTs has led to an increasing number of portable devices and sensors (Internet of Things) that enable various e-Health scenarios such as remote patient monitoring. It is expected that the "Internet of Things" will create significant impact to future delivery of healthcare. However, high dependability on the IoT technologies in e-Health creates significant security and privacy risks. In particular, there are risks with respect to patient identification and reliability of collected information. Moreover, the modern eHealth solutions based on IoT are heading towards open, interconnected environments which collect and rapidly exchange sensitive data making the problem more difficult. In addition, in some case, the physical integrity of a person (cause death, etc.) might be even at risk. For example, it could be the case of active or passive security functions used in a car (e.g. brake automatically in some circumstances) or of "things" used in the health sector (e.g. if a pacemaker can be programmed remotely and put the person at risk). The information gathered from IoT things used in a health application could also reveal that the person suffers from specific diseases and this could be used for physically attacking this person.

Loss of user control / difficulty in making decisions – Certainly automated decisions will create a perception of loss of control, but may also lead to actual loss of control, because one of the main goals of the IoT is to give some autonomy to the objects and to enable automated decisions. Both perceived and actual loss of control may have serious impact on many aspects of individual's everyday lives. On the other hand IoT could help elderly or disabled people to stay longer at home and in control of their own lives while their control of certain "fine-grained decisions" might be limited.

Nevertheless, expectancy of control will be a key foundation to build individual's trust on IoT.

3

See for example "Show me how you move and I will tell you who you are", Gambs et al, 2010, http://licit.inrialpes.fr/apvp2010/slides/APVP_ADEPT_Gambs.pdf

Decisions taken automatically by devices or applications, based on this huge set of sensed data might not be transparent to the data subjects and therefore create the sense of loss of control. Moreover these decisions will be difficult to understand for individuals as especially information collected via sensors is often only subconsciously recognized by individuals.

Applicable law – Given the global nature of the IoT another problem is, that individuals and companies are confronted with a number of national / regional data protection laws providing different levels of protection. When data controllers of IoT systems and individuals affected by these systems are based in different countries (within or outside the EU) this potentially leads to lots of different applicable laws.

Objectives to be attained

Based on the context above, the main objectives should be effective personal data protection which entails the application of the legal principles, as well as effective information security (confidentiality, integrity, availability) of services, with a view to provide better IoT services for the citizens.

Another interesting element is the issue of universality of personal data protection which is going to be very relevant in an IoT environment. Apart from the obvious legal problems, the issue of scope of users' choices and data portability also needs to be considered.

Due to the international / global nature of the Internet of Things it is important, to increase the level of harmonisation of data protection legislation and to ensure a high level of enforcement.

It can reasonably be forecast, that if IoT is not designed from the start to meet suitable detailed requirements that underpin

- ★ the right of deletion
- ★ the right to be forgotten
- ▲ privacy and
- ▲ data protection principles

then we will face the problem of misuse of IoT systems and consumer detriment.

Policy options for reaching the objectives

Two general principles should be carefully considered in the IoT policy making:

- ▲ The IoT shall not violate human identity, human integrity, human rights, privacy or individual or public liberties.
- A Individuals shall remain in control of their personal data generated or processed within the IoT, except where this would conflict with the previous principle.

In accordance with these principles the following options should be considered:

Privacy, data protection and information security risk management – Appropriate and relevant technological safeguards can only be identified if a sound privacy, data protection and information security risk management is conducted. To this effect, such a process would need to be defined at the EU level and be based on existing risk management frameworks. The RFID Privacy Impact Assessment framework seems to provide for an appropriate prototype for a risk management-based approach for the IoT case, as well. This concept should be accompanied by effective and efficient means of data protection enforcement, to ensure a proper and widespread implementation. It has to consider at least the study of the context, the unwanted events, the threats, vulnerabilities and risks to determine the appropriate measures to be taken to mitigate the risks.

Several technological safeguards are commonly discussed or implemented: data minimization, encryption, access control, technologies giving the individuals enhanced control over their personal data, the way it is exchanged and their privacy. But technological aspects are only one factor in the equation. As in a proper analysis of the risks and impacts one shouldn't only focus on the technological aspects. It is also of utmost

importance to look into e.g. organisational / procedural / "softer" and legal / regulatory measures.

This methodology should ensure that the data protection principles (data minimisation, purpose limitation, ...) are included as design goals for IoT systems and that best practices (such as the use of temporary identifiers, audit logging, data aggregation, the definition of deletion-dates for personal data, privacy-friendly default settings etc) are used to reduce the identified risks; in this context a catalogue of best practices and common risks could be established.

Challenges addressed with this option:

- A Ensuring continuity and availability in the provision of IoT-based services
- ▲ The risks are context-aware and situational
- A Traceability / profiling / unlawful processing
- Loss / violation of individuals' privacy and data protection
- A Realisation of malicious attacks against IoT devices and systems
- Loss of user control / difficulty in making decisions

Options:

Do nothing:

The fundamental rights to data protection and privacy as well as information security are often not considered at the design stage. This is especially true with the development of new technologies, where the focus is at core technical challenges. It is therefore unlikely that these issues will be properly addressed by the market without regulation.

Soft law / Self regulation:

Keeping in mind the international dimension of IoT, the resulting need for interoperability, the importance of an harmonised internal market and last but not least the universality of the fundamental rights to privacy and data protection as enshrined in the Charter of Fundamental Rights of the European Union, it would be inadvisable to allow divergence at a member state level of key methodologies to ensure the development of fundamental rights compliant IoT technologies and applications.

Co-regulation:

Policy providing guidance towards a harmonised Privacy, Data protection and Information security risk management methodology may in the long term be sufficient to achieve the desired goal. However the development of such methodologies might on the one hand take too long and on the other hand lack the necessary enforcement components that are needed to ensure a proper implementation.

Binding law:

In order to ensure a harmonised high standard of privacy, data protection and information security, the development of a common binding European Data Protection Impact Assessment Framework for IoT seems to be appropriate. This should be accompanied by effective and efficient means of data protection enforcement, to ensure a proper and widespread implementation.

(Research on) Privacy by Design and Privacy by Default – Usually it is not the technology *per se* that increases the risks for privacy, data protection and security, but the way it is developed and applied. The negative consequences of this practice for privacy, data protection and security will significantly increase, if applied to IoT systems. Therefore mechanisms are needed to ensure that no unwanted processing of personal data takes place and that individuals are informed of the processing, its purposes, the identity of the processor and of how to exercise their rights. At the same time processors need to comply with the data protection principles as data minimisation, purpose limitation etc., which might be especially challenging in an IoT environment, where automatic communication without human intervention between objects and between objects and persons is at the core of the system.

On a technical level an appropriate process to protect personal data should be defined. For example, privacy policies (at the user level) that can be pushed / built inside the objects (and translated according to the technical specificities of each object) and finally be enforced by the object with appropriate mechanisms to

ensure data protection. The technical challenge is however, to enable objects with limited processing power and / or memory to receive and respect such policies.

The possibilities for individuals to exercise their data subject rights need to be enhanced. It needs to be ensured that clear, easily understandable information on the data processing of IoT systems, their objects, functions and purposes, is provided to individuals. Mechanisms need to be found to make individuals aware of the processing and to provide information on the processor, the purpose of the processing and possibilities to exercise data subject rights, as most IoT applications are expected to operate in the background, invisible to and unrecognised by the individual.

Information on how to build privacy-friendly applications needs to be provided to IT engineers, system designers and standardisation bodies, to ensure that the concepts of Privacy by design and Privacy by default settings get implemented in practice. Data protection officers might have an important role here, provided that defined minimum requirements ensure that they themselves are sufficiently trained.

Educating individuals throughout all levels of the educational system needs research into pragmatic didactic course material and a theoretical pedagogic framework.

Challenges addressed with this option:

- △ Design considerations for IoT technologies
- ▲ The risks are context-aware and situational
- ▲ Traceability / profiling / unlawful processing
- A Exercising data protection rights for individuals and compliance with DP legislation for organisations
- Loss of user control / difficulty in making decisions

Options:

Do nothing:

As already described above it is unlikely, that the privacy, data protection and information security will be addressed properly by the market without any regulation.

Soft law / Self regulation:

Considering the privacy, data protection and information security problems existing under the current legal framework there seems to be no indication, that these challenges will be overcome in the area of IoT based on self regulation. In the contrary it can be stated that even current binding legislation is not sufficient to ensure a fundamental rights compliant development of information technologies.

Co-regulation:

See section "Standards" below.

Binding law:

See the following section.

Data protection legislation: harmonisation / coherent application / enhanced enforcement – On a legal level it is important to increase the level of harmonisation of data protection legislation, to ensure a coherent application of this legislation and to ensure a high level of enforcement. To this end the above discussed principle of "Privacy by design" should be mandatory, including principles of data minimization and data deleting.

At the same time the data protection authorities should be strengthened, their powers clarified and harmonised and they should be empowered to enforce all relevant rights and obligations, not only selected ones. Significant sanctions for violations of data protection obligations should be introduced and the concept of mandatory personal data breach notifications should be extended to all areas of personal data processing.

In order to ensure a consistent and professional implementation of data protection legislation, the role of data protection officers has to be considered. In addition to ensuring a high level of compliance data protection

officers also can serve as multipliers and provide data protection education to the staff and management of their respective companies. They therefore could also play an important role in the design of IoT systems by providing expert knowledge on data protection to the relevant actors.

It should be ensured, that individuals remain in control of their personal data and that IoT systems provide sufficient transparency to enable individuals to effectively exercise their data subject rights. This also involves, that in cases where data processing takes place based on consent, a clear and non-discriminative choice must exist to refuse consent. Furthermore it should be clarified, under which circumstances the consent of individuals to certain data processing activities should be considered to be valid. Especially in the case of IoT, individuals will often lack the necessary understanding of the technical functioning and therefore of the consequences of their consent. Clear rules on the conditions that need to be met for consent to be valid, should be defined.

On the definition of personal data, the concept of indirectly identifiable data needs to be strengthened and clarified, as in practice data processors often face uncertainties especially with regard to unique identifiers.

Note: Some of the options discussed in this section are also addressed in the recently published proposals on the reform of the EU data protection legislation. An analysis of these reform documents still needs to be carried out.

Challenges addressed with this option:

- △ Design considerations for IoT technologies
- ▲ Traceability / profiling / unlawful processing
- A Repurposing of data / mission creep challenge is amplified in an IoT environment
- Loss / violation of individuals' privacy and data protection
- ▲ User lock-in
- ▲ Applicable law

Standardisation – Generally speaking, standards could provide presumption of conformity with the legal requirements and could be used for certification; in addition, they could provide definitions for clear information to individuals on how to exercise their data protection rights, mindful that clear information is a prerequisite for informed consent.

On the other hand standards are voluntary and non-binding. Therefore the tool might possibly be too "weak" for the intended outcome. Other regulatory measures which are more binding might also be needed. A recommendation could be envisaged and committology procedures could be launched to build a European privacy risk management tool (methodology + best practices).

In order to make Privacy by design and Privacy by default a reality, the consideration of data protection requirements should become a mandatory design goal in standardisation, as standards can serve as a multiplier for privacy friendly application design.

In the context of the Internet of Things, standards should be elaborated specifically on the aspects of good application design, user application interfaces (usability / accessibility) and on tools for individuals to play their part in security, data protection and privacy for the Internet of Things for people ("empowerment").

Challenges addressed with this option:

- Lexercising data protection rights for individuals and compliance with DP legislation for organisations
- ▲ User lock-in
- Loss of user control / difficulty in making decisions

Potential impacts of each policy option

"Building trust in the online environment is key to economic development. Lack of trust makes consumers hesitate to buy online and adopt new services, including public e-government services. If not addressed, this lack of confidence will continue to slow down the development of innovative uses of new technologies, to act as an obstacle to economic growth and to block the public sector from reaping the potential benefits of digitisation of its services, e.g. in more efficient and less resource intensive provisions of services. This is why data protection plays a central role in the Digital Agenda for Europe, and more generally in the

Europe 2020 Strategy."4

This statement is especially true in the area of new technologies like the IoT, which will only be able to develop their full economic potential, when individuals trust and adopt these technologies.

Furthermore Article 8 of the EU's Charter of Fundamental Rights enshrines data protection as a fundamental right, which reinforces the necessity to ensure the implementation of high standards for data protection, privacy and information security.

Main goals of any regulatory approach should therefore be

- to ensure full compliance of IoT technology and applications with the Charter of Fundamental Rights
- to minimise potential barriers for the adoption of IoT technology in order to benefit of it's full economic potential

With regard to the policy options described above the potential impacts might be the following

Do nothing:

"[P]ersonal data today may be processed more easily and on an unprecedented scale by both private companies and public authorities, which increases the risks for individuals' rights and challenges their capacity of keeping control over their own data (...). Moreover, there are wide divergences in the way Member States have transposed and enforced the Directive, so that in reality the protection of personal data across the EU **cannot be considered as equivalent today**."⁵

IoT technology will lead to an by far increased amount of personal data being processed. The very nature of IoT technology, to autonomously process and communicate data without human intervention increases the need for not only harmonised technical standards but also legal requirements.

Doing nothing might reinforce the adverse effects and seems to be the least preferable option.

Soft law / Self regulation:

Especially in the area of developing technologies self regulation might not lead to satisfying results, as solving the core technological problems will likely be given preference over addressing requirements as properly considering privacy, data protection and information security aspects, as soft law lacks sufficient enforcement features.

As a result, binding regulatory actions that might be taken later in order to compensate existing weaknesses will cause higher costs, as then already existing technologies will need to be changed in order to be compliant rather than being designed according to the requirements, which usually is the significantly cheaper option in IT development.

Co-regulation:

As standards are voluntary and non-binding, the tool might possibly be too "weak" for the intended outcome. However standards can be used to support the intended developments and lead the way in the desired direction.

Ibid, page 11.

Impact Assessment Accompanying the document Regulation of the EuropeanParliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, European Commission, 25.01.2012, SEC(2012) 72 final, page 4.

Binding law:

Binding law in combination with increased level of data protection enforcement seem to be the most promising option to achieve the goals to ensure a fundamental rights compliant and trustworthy development of IoT technology. As IoT technologies are in a very early stage of development, it also seems to be economically preferable to provide clear binding requirements already at this stage of the development. This allows for designing technology according to these requirements, rather than having to change already existing technology later on.