Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Internet of things: Privacy issues revisited

Rolf H. Weber *

University of Zurich, Switzerland

Keywords:
Data minimization
Internet of things
Quality of data
Privacy challenges
Privacy enhancing technologies
Transparency

A B S T R A C T

The Internet of Things presents unique challenges to the protection of individual privacy. This article highlights the growing need for appropriate regulatory as well as technical action in order to bridge the gap between the automated surveillance by IoT devices and the rights of individuals who are often unaware of the potential privacy risk to which they are exposed. As a result, new legal approaches for the protection of privacy need to be developed.

1. Starting point: challenges posed by the Internet of Things

1.1. *Technological background*

The Internet of Things (IoT) as an emerging global Internet-based information architecture that facilitates the exchange of goods and services is gradually gaining importance. The ITU defined the IoT as the development of item identifications, sensor technologies and the ability to interact with the environment.[1] In the meantime, the definition has been widened and it is now encompassing a broad spectrum of device forms that are used in a number of varying settings.

The most commonly known usage of the IoT is based on RFID (radio frequency identification device) technology that aims at preventing the disappearance of goods. However, other forms such as tracking parts through manufacturing processes and measuring variables such as temperature and humidity in a storage facility are common IoT applications as well. In practice, the level of sophistication and the price of RFID can be quite different, starting with the cheap passive device without a power source and limited storage to an active self-powered RFID possessing advanced storage and communication capabilities.[2]

Some of the data that are collected appear to be trivial but for example data relating to a production process could be highly valuable thus requiring appropriate protection. For private purposes, the IoT can be used to increase household efficiency by allowing the devices to communicate and take action such as place an order for goods when the fridge is empty or turn on the washing machine when electricity is cheap. The effects of malfunction created by wrong data (external and internal reasons) might be substantial in particular if a part of the decision-making process in a factory or household is automated. In such a case, the entire production line could be stopped or a customer could end up with double the quantity of goods he required. Furthermore, today all smart phones carry location sensors in them allowing the permanent tracking of their users. All these IoT devices in some form add value to individuals as well as businesses; however, they also cause risks.

* University of Zurich, Rämistrasse 74/38, 8001, Zurich, Switzerland. Tel.: +41 (44) 634'48'84; fax: +41 (44) 634'43'95.
E-mail address: rolf.weber@rwi.uzh.ch.
Chair Professor for International Business Law at the University of Zurich, Visiting Professor at Hong Kong University, Attorney-at-Law in Zurich.

[1] Definition of ITU (2005), available at <https://www.itu.int/osg/spu/publications/internetofthings/InternetofThings_summary.pdf>.

[2] RFID are classed according to their level of sophistication. Class 1 and 2 are passive RFIDs and Class 3 and 4 are active RFIDs which are commonly connected to a network and exchange data whereas Class 1 and 2 only are read by a scanner without actively collecting and submitting data on their own.

http://dx.doi.org/10.1016/j.clsr.2015.07.002
0267-3649/

1.2. *Privacy risks*

The IoT devices collect a vast amount of information and, therefore, they also carry a great potential of privacy risks in relation to the use of the data and its access. Particularly the identification of an individual and his behavioral patterns is a growing concern. As IoT devices are increasingly used in all fields of daily life, such as in the health care sector, a great amount of commonly considered private information is stored and collected.

With the growth of these technologies, new safeguards for privacy and data integrity must be created. The IoT has a limitless potential to improve the daily life, for example in health care by allowing the collection of health information (e.g. with new FitBit/Jawbone devices recording basic health information through a wristband or electronic patient chip cards) which can be used to identify disease correlations and support new treatment options as well as remotely monitor the process of the treatment, however, the chances are correlating with the challenges. Similarly, with the help of Big Data analytics the accumulated raw data are highly valuable as specific patterns can be extracted, but the privacy risks naturally inherent are immense as the IoT data could allow the identification of an individual and thus his condition.

The IoT devices usually collect certain data that are often aggregated with other device data and thereafter sent via a router to a communication device (Wi-Fi or cellular) that transfers the data to a cloud server for processing. During this procedure various protocols and compression technologies are employed as the storage space on the devices is extremely limited and cannot cope with the big headers which for example are used for the Internet Protocol IPv6. Currently, providers attempt to filter data as closely as possible to the device that created it since this method avoids unnecessary transmissions and reduces safety risks.

Notwithstanding the fact that discussions about the normative framework governing the IoT are going on for the last five years[3] available legal assessments are still not stable. Furthermore, technologically and practically the interconnection between the devices and infrastructures has not yet reached a level that would allow its application in real life to a broad extent. However, this situation is changing with more and more services being offered based on IoT technology.

1.3. *Need for legal stability*

In view of the large range of IoT applications it is obvious that the new technological opportunities have organizational, social, and cultural implications. At the same time, various legislative instruments place limits on the IoT and its use in daily life; therefore, a single legal description cannot easily be developed. Moreover, data protection laws and privacy laws related to specific types of data must be considered. From a general perspective, the EU Data Protection Directive (DPD) is influencing the processing of data if the data collected are qualified as personal data. Other sector-specific regulations in particular in the USA (e.g. Health Insurance Portability and Accountability Act [HIPAA]) also have an effect on the data collection and the privacy of the data.

These regulations target at certain types of information, however, in the context of the IoT the definitions used are not sufficient because the IoT raw data are not "personal" on its face as it does not identify an individual. Only through combination and analytical methods can the identity of the individual as subject of data protection regulation be ascertained, which then could potentially submit the data collection to the EU DPD. As the collection by IoT devices is carried out in an automated manner, the risk of being non-compliant with these laws is inherent in their design. Nevertheless, IoT services' providers as well as consumers do not have a clear picture of the available legal provisions; such kind of normative uncertainty is detrimental to the business.

Therefore, in light of the vast technological developments over the last decade new rules are necessary for the IoT. Even if the IoT applications are quite different causing problems in the harmonization processes, the regulation of a global technology requires a worldwide approach in order to be most effective. In light of the difficulties associated with reaching an agreement on basic data protection and privacy issues, this solution is unlikely to be realized in the near future. Rather a more nuanced approach taking into account technological standards as enablers of data protection as well as national data protection regulations is the more likely scenario.

1.4. *First regulatory efforts by the EU*

The first supranational organization having dealt with the business and legal environment of the IoT, namely the European Commission, appointed a large group of experts to examine the relevant aspects of a possible IoT normative framework;[4] however, these activities have come to an end. Nevertheless, not only the expert reports are available but also the results of a public consultation that collected about six hundred responses to a broad questionnaire identifying IoT challenges.[5]

As far as privacy and data protection are concerned, the public consultation showed diverging results regarding the issues raised in the questionnaire. The industry was of the opinion that the current data protection framework would be sufficient, whereas a large majority of interested citizens and consumer organizations claimed that a greater focus on privacy and data protection in the context of the IoT would be needed. New instruments such as data protection impact assessments have been largely welcomed.[6] This reflects a common understanding that enterprises wish to expand their business operations whereas consumers still value their fundamental privacy rights and seek a choice as to what information enterprises can use and collect.

According to the public consultation, special emphasis must be placed on user consent as well as on the right of the

[3] For an early overview see R.H. Weber, Internet of things – New security and privacy challenges, CSLR 26 (2010), 23–30 causing the present title "revisited"; see also R.H. Weber/R. Weber, Internet of Things – Legal Perspectives, Zürich 2010.

[4] European Commission, Internet of Things, Reports, January 16, 2013, available at <https://ec.europa.eu/digital-agenda/en/news/conclusions-internet-things-public-consultation>.

[5] For an overview see also R.H. Weber, Internet of Things – Governance quo vadis? CLSR 29 (2013), 341, 342/43.

[6] Reports (supra note 4), 3.