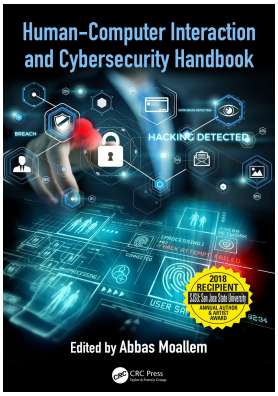

Human-Computer Interaction and Cybersecurity Handbook

Abbas Moallem

Privacy and security in the IoT—Legal issues

Publication details
https://test.routledgehandbooks.com/doi/10.1201/b22142-16
Rolf H. Weber
Published online on: 24 Oct 2018

chapter sixteen

Privacy and security in the IoT—Legal issues

Rolf H. Weber

Contents

16.1 Introduction

The legal environment in technology-exposed areas is not easy to develop and to frame as experience has shown in many cases. The rule-making processes are confronted by fast technological changes; in addition, rules must be based on the technological designs of the concerned devices and software. The case to be discussed in this chapter is the Internet of things (IoT) applications.

The Internet Society (2013, 12) defined the term *IoT*, coined by the British technology engineer Kevin Ashton, in 1999, as the development of item identifications, devices, and sensor technologies that enable everyday items to interact with the environment. The IoT adds the dimension of "any thing" to information and communications technologies that already feature "any time" and "any place" aspects of functionality (ITU 2012, 2). Thus, the IoT is "a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies" (ITU 2012, 2). A substantively wide but shortly worded definition qualifies the IoT as a network encompassing a broad spectrum of device forms used in many varying settings (Weber 2015, 618).

In the IoT field, the most commonly used technology is radio frequency identification device (RFID). RFID aims at preventing the disappearance of goods and maintaining their quality through the shipment process. Tracking parts in manufacturing processes and measuring variables (temperature and humidity) in storage facilities are other common IoT applications today.

For private use purposes, the IoT helps increase household efficiency by allowing devices to communicate and take action such as ordering items to refill the fridge or starting a washing machine. Particularly in this context, the collection of device activity data can be sensitive; consequently, data privacy becomes an issue.

A particular challenge in this respect concerns the interaction between IoT-generated data and customer data. As such, machine-produced activity data are not subject to data protection regulations, but the combination with personal data can lead to the application of data privacy laws. This consequence mainly occurs if big data analytics are applied.

Furthermore, experience shows that the effects of malfunctions (e.g., in the case of placing of an order) created by corrupted data can be substantial: If devices and/or software are not working properly, an entire production process can be interrupted or damages can be caused to a private household. On the one hand, the traditional liability regimes are applicable, but, on the other, the simultaneous disclosure of data to third persons might also cause noncompliance with data protection laws.

As mentioned, technological elements provide a framework for designing the conditions for rule-making processes; in particular, the following key elements related to different IoT applications must be taken into account when seeking to regulate this environment (Weber 2015, 618):

- The *technology* has to be "global" in order to make the same technical processes applicable all over the world; the respective industry standards should ensure interoperability and data security.
- *Ubiquity* describes the extension (scope) of the technological environment: The IoT regulatory framework must be designed to ubiquitously encompass persons, things, plants, and animals.

- *Verticality* means the potential durability of the technical environment; an IoT application needs to function long enough to enable its use in the supply chain until it reaches the final customer.
- *Technicity* is an important basis for the development of rules protecting the data; thereby, the complexity of the techniques (active and passive, rewritable, processing, and sensor-provided products) as well as the complexity of background devices must be taken into account.

In a nutshell, IoT applications can add value to individuals as well as businesses, but they also cause risks. In order to protect against such risks, the law must understand the technological features and set rules accordingly.

This contribution begins with a discussion of the normative framework applicable to IoT by taking into account the suitability of regulatory measures as well as the current state of regulation and the strategies being proposed for future regulation. Next, we discuss the privacy and security challenges in light of data protection rights and obligations before addressing specific issues in the context of IoT. These issues are based on the nature of the technology and thus require for the most part technological solutions. In conclusion, an outlook on future developments is presented.

16.2 Normative framework

16.2.1 Legal suitability and systematic structure

The normative framework governing the IoT should apply globally; it should be applicable to every device on earth. The present lack of international rules and the improbability of reaching a respective multilateral agreement require stronger leadership by the industries in establishing the relevant standards for the applications and devices. Such an approach should avoid causing a disruption between many potentially varying data protection rules across states. Harmonization processes based on standardizations of industry organizations could be a first move into the direction of legal stability.

Since IoT applications and new technological opportunities have organizational, social, and cultural implications, a simple legal framework is not easily developed. Also, different types of information used in the context of the IoT increase the difficulty of identifying single factors. Only through combinations of approaches and analytical methods will it be possible to develop a stable legal environment. Since the collection of data by IoT applications is carried out in an automated manner, the risk of being noncompliant with the applicable laws must be addressed in their design.

The establishment and implementation of an appropriate legal framework enshrining effective rules calls for a systematic approach. Thereby, a systematization of legal problems potentially occurring should be done by coordination along certain technical axes. Reference points can, for example, be the already mentioned technological elements of globality, ubiquity, verticality, and technicity. The normative challenges of data privacy and security need to be reflected in a qualitative classification. In this context, the question that must be addressed is "how much privacy is society prepared to surrender to increase security?" Solutions should permit the understanding of privacy and security not as opposites, but as principles affecting each other.

16.2.2 Regulatory environment

16.2.2.1 Governmental initiatives

1. A multilateral agreement, similar, for example, to the World Trade Organization agreements governing international trade, does not exist in the field of the IoT. In addition, the negotiation of such an agreement is also unlikely to happen during the next few years. But even if the respective efforts were undertaken, it appears to be doubtful whether an adequate legal framework would be possible in view of the fast developing technologies and different legal regimes around the world.
2. On a regional level, the European Commission started relatively early looking into the regulatory challenges caused by the IoT. With the support of an expert group, the Commission published a detailed questionnaire that provoked many valuable inputs (European Commission 2013). Nevertheless, the Commission, which was invited by the addressees of the questionnaire to implement a multistakeholder initiative for the establishment of IoT guidelines and recommendations, has withdrawn these activities from the political agenda [for further details see Weber (2016, 29/30)].

   In March 2015, the European Commission initiated the creation of the Alliance for Internet of Things Innovation (AIOTI). This organization was invited to prepare a European IoT roadmap toward the year 2020. In October 2015, the AIOTI published 12 reports, which set forth the "Recommendations for future collaborative work in the context of the Internet of Things Focus Area in Horizon 2010." The reports address IoT applications, innovation ecosystems, IoT standards, policy issues, the smart living environment, the smart farming and food safety, wearables, smart cities, the smart mobility, and the smart manufacturing.
   In addition to Article 29—Data Protection Working Party of the EU (WP29)—consisting of representatives of the national data protection authorities, the European Data Protection Supervisor and the European Commission published its Opinion on the Internet of Things in September 2014 (WP29, Opinion 8/2014) (European Commission 2014). In this Opinion, the WP29 alerts both businesses and customers to the challenges and risks arising from the use of the IoT technologies (quantified self, home automation, and wearable computing) and proposes measures that could enhance and secure data privacy (e.g., privacy impact assessment, quality control by device manufacturers and application developers, and improvement of standardization). Finally, research groups (such as the European Research Cluster on the Internet of Things and the Dynamic Coalition on the Internet of Things) tackle normative IoT issues; however, their political impact is quite remote [see Weber (2016, 30/31)].

3. The Federal Trade Commission (FTC) in the United States has also begun to look into privacy issues in the IoT environment. The FTC in a staff report (2015) declared that IoT-specific legislation at this time would be "premature" and instead encouraged the development of self-regulatory programs for industry sectors in order to improve privacy and security issues. In May 2016, a policy paper for further research with the title "Developing and Growing the Internet of Things Act" ("DIGIT") was presented. As far as privacy issues are concerned, for obvious reasons, different levels of data protection in the United States and in the European Union (EU) create challenges in coming to a common understanding.

16.2.2.2 Self-regulatory initiatives

In view of the difficulty to develop a genuine normative environment for the IoT, as mentioned, rule-making processes should start at the technological designs of the IoT. The present lack of a global regulatory environment makes it necessary that industries producing and using the IoT devices are self-regulating by adhering to the state-of-the-art standards of the industry for such devices.

Therefore, notwithstanding the fact that the IoT will be a discussion topic for many years, the present regulatory model is still based on self-regulation through many business standards, beginning from technical guidelines and extending to fair information practices. Indeed, under the given circumstances, it appears to be appropriate that standard setting by the industry itself should be encouraged as long as this model meets the demand of the market and offers parties engaged with the IoT a choice as to the level of privacy protection they wish.

Self-regulation realizes the principle of subsidiarity, meaning that the participants of a specific community try to find suitable solutions (structures, behaviors) themselves. The legitimacy of self-regulation is to be seen in the fact that private incentives lead to a need-driven rule-making process. In addition, self-regulation is usually less costly and more flexible than governmental rules see also Schmid (2008, 199)].

Related to the concept of self-regulation, legal doctrine has developed the notion of "soft law." This term did not yet gain a clear scope or reliable content; often, it is used in parallel to self-regulation. But the word *soft law* shows the neighborhood to law usually covering certain forms of expected and acceptable codes of conduct (Weber 2010, 27/28).

The specific problem about data privacy and security consists of the acknowledgment that the applied principles are not identical in the different regions of the world, which makes the application of general principles difficult in cross border business activities.

16.2.3 Regulatory strategies and agenda

The legal framework for data privacy and data security issues of the IoT could be based on five different strategies (Weber 2010, 29; Schmid 2008, 208):

- *Right-to-know legislation:* This approach envisages keeping the customer informed about the applied IoT scenarios, i.e., the customer should know which data are collected and should have the possibility to deactivate the tags after a transaction.
- *Prohibition legislation:* This concept, corresponding to traditional atate legislation, envisages to forbid or at least to restrict the use of IoT applications in certain scenarios. The mentioned self-regulatory mechanisms, however, rather tend to introduce incentives (if at all) instead of prohibitions.
- *Information technology (IT) security legislation:* This model develops initiatives that demand the establishment of certain IT security standards; usually, respective rules are developed by the concerned market participants, but state intervention remains possible. The respective standards could develop, for example, a new-generation framework of data protection protocols allowing the setting up of stringent safeguards as to reporting and frequent audits of implemented measures.
- *Utilization legislation:* This approach intends to support the use of IoT applications under certain conditions; such a normative concept must fine-tune an appropriate balance between prohibited and utilizable approaches.
- *Task force regulation:* This model covers legal provisions supporting the technical community in investing into the research of the legal challenges of the IoT.

The aforementioned approaches can also be combined; in principle, however, in the IoT environment, the IT security legislation should become the driver of a regulatory framework. The other approaches appear to be less suitable due to the limited scope and/or the unclear technological perception.

The regulatory agenda must consider the requirements of technological designs and applications [see also Nappinai (2017, 40/41)]. This awareness is crucial for the development of appropriate new rules. Therefore, based on the outlined general assessment of the normative framework governing data protection and data security issues in the IoT field, the following considerations start with a discussion of the technological topics, in particular, the devices and software requirements, the privacy and security challenges, and the privacy enhancing technologies, followed by specific new issues related to the IoT technology. For these reasons, the legal issues caused by the pertaining privacy and security threats caused by the IoT are to be analyzed hereinafter.

16.3 Specific privacy and security issues

16.3.1 Device and software requirements

During the last few years, microchips are constantly becoming cheaper to produce resulting in IoT sensor prices dropping below 50 cents per unit. The smaller devices such as RFID will be a main driver of growth in this area. In addition, cellular devices can provide an access point and a gateway for other (low-power) technologies (Weber 2015, 621).

At this moment, the technological challenge consists of the limited storage space, particularly on a simple passive RFID. An ongoing flow of information cannot be saved on an RFID tag. Therefore, the supply of the collected information must be made available through linking and cross-linking with the help of an object naming service (ONS). The ONS has some similarities with the well-known domain name system (DNS) of Internet Corporation for Assigned Names and Numbers but is not identical; nevertheless, the ONS is also authoritative in the way that the entity having change control over the information about the electronic product code (EPC) is the same entity having assigned the EPC to the concerned item (EPC Global 2008).

Depending on the IoT device, access by a third party can be made possible at any point in the technological chain. But since aggregated data are of value at the access point (router or cellular device), hackers and other interested third parties can also use the access point as main entry to the stored information. Usually, data are not encrypted at this location; encryption and anonymization are only done at a later stage on the cloud server. Consequently, privacy risks cannot be overlooked.

Recently, new standards have been designed to better deal with the various types of data. Mostly, an open-access approach is chosen. In using this method, the industry also enables criminals to profit from the accessible information. In order to avoid negative consequences, uniform security standards should be developed in order to ensure the safety of the data at every step from its collection to the processing (for the identification of criminal, see, e.g., Wynzard Group).

16.3.2 Privacy and security challenges

Obviously, the IoT devices collect a large amount of information; consequently, these devices also carry a substantial potential of privacy risks in relation to the use of the data and its access. As IoT devices are increasingly used in all fields of daily life, the identification of an individual and his/her behavioral patterns become a growing concern.

16.3.2.1 General disclosure risks

With the widespread implementation of the new technologies, better-designed safeguards for privacy and data integrity must be created. The potential of IoT for daily life needs to be balanced against the risks of undue information disclosures. For example, with the help of big data analytics, the accumulated raw data can become highly valuable (particularly in the health sector) since specific patterns can be extracted, but the privacy risks inherent are not to be neglected as the IoT data would allow the identification of an individual and his/her (health) condition [for further details on security risks, see Xiao et al. (2000)].

IoT devices often collect certain data that are aggregated with other data and sent through a router to a communication device. Such a device is then able to transfer the data to a cloud server for processing. During this procedure, various protocols and compression technologies are employed, since—as mentioned—the storage space on devices is limited. In addition, the devices often are unable to cope with the big headers used for the Internet protocol IPv6.

Technologically and practically, the interconnection between the devices and infrastructures has not yet reached the appropriate level allowing for its seamless implementation into daily life. With an increased number of services offered based on IoT technology, however, this limitation will lose importance over the next couple of years. Hence, the location points of interconnection need to be designed in a secure way.

16.3.2.2 Requirements of technical architecture

The technical design of the IoT is not without impact on the privacy and security of the involved individuals. Privacy includes the concealment of personal information as well as the treatment of the data. Many stakeholders are interested in the data; for example, private actors such as marketing enterprises, national security services, and public utility operators. Therefore, the degree of reliability must be high (Weber 2010, 24).

The following privacy and security requirements are relevant as criteria for achieving the desired goals (Fabian and Günther 2007):

- *Resilience to a tag:* The system must avoid single points of failure and should adjust itself to node failures.
- *Data authentication:* Retrieved address and object information should generally be authenticated.
- *Access control:* Information providers must be able to implement access control on the data provided.
- *Client privacy:* Only the information provider should be able to infer from observing the use of the lookup system related to a specific customer.

These requirements are to be integrated into the risk management concept of private enterprises and government agencies. A good IT governance approach considers the concerned business activities and limits exposure.

16.3.2.3 Cybersecurity risks

The general security risks in the IoT have a further exposure in the context of cybersecurity causing new and unique challenges. In fact, recent examples such as the hacking of baby monitors have shown the vulnerability of IoT devices. A key issue consists of the increase of overall attack surface for malicious attacks, as compared to isolated (i.e., nonconnected) systems [for further details, see Weber and Studer (2016, 719/20)].

A 2015 study by Hewlett–Packard (2015) showed that 70% of IoT devices contain serious vulnerabilities stemming from the following:

- *Lack of transport encryption:* Many IoT devices are simple "unit-taskers" and have cost, size, and processing constraints, i.e., most devices will not support the processing power required for strong security measures.
- *Insufficient authentication and authorization:* The weakness is due to poor password requirements, careless use of passwords, lack of periodic password resets, and failure to require reauthentication for sensitive data.
- *Insecure web interface:* Issues in this respect include persistent cross site scripting, poor session management, and weak or plain default credentials.
- *Insecure software and firmware:* Most IoT devices are designed without the ability to accommodate software or firmware updates making vulnerability patching difficult.

In addition, digital attacks on connected devices not only pose risks in the online world, but they also create physical risks to the devices themselves and, even more critically, safety risks for IoT users [for further details, see Weber and Studer (2016, 720/721)].

16.3.3 Privacy-enhancing technologies

A number of technologies have been developed in the past couple of years to balance IT risks against information privacy goals. The best-known measures are based on the so-called privacy-enhancing technologies (PETs); the following techniques are often implemented (Fabian and Günther 2009, 124/25; Weber 2010, 24/25):

- *Virtual private networks* as extranets established by close groups of business partners
- *Transport layer security* based on an appropriate global trust structure, thereby improving confidentiality and integrity of the IoT
- *DNS security extensions* (DNSSEC) making use of public key cryptography for the signature of resource records to guarantee origin and integrity of delivered information;
- *Onion routing* encrypting and mixing Internet traffic from many different sources and channels;
- *Private information retrieval* systems assessing the customers' interest in a specific information.

Increased privacy and security can also be achieved by *peer-to-peer* (P2P) systems. These designs can achieve good scalability and performance.

Another relatively new approach addresses technical possibilities being able to integrate the data privacy safeguards into the IT devices and applications. This new notion, called "privacy by design" (PbD), requires the adherence to seven basic principles: (1) a proactive approach to protection measures, (2) privacy as default setting, (3) privacy embedded into the design of the technology, (4) full functionality, (5) end-to-end security spanning the life cycle of the device, (6) visibility and transparency allowing the stakeholders to verify the privacy claims made, and (7) respect for user privacy (Cavoukian 2009). In the meantime, PbD has become a processor's obligation according to the new EU General Data Protection Regulation (GDPR) of 2016 entering into force in late May 2018 (Article 25 GDPR).

A similar new approach is called "privacy engineering." Privacy is considered in this approach to be a nonfunctional requirement or quality attribute. Such an attribute needs

to be broken down into components that can be architected and evaluated. In this concept, the collection, processing, and storage of personal information becomes a business requirement that makes it necessary to rethink topics such as privacy policies and notices [for further details, see Finneran et al. (2014, 73–226)]. Therefore, new elements structuring data and privacy governance concepts gain importance.

16.3.4 Privacy through deletion

Privacy can be realized through the diversion or the destruction of an RFID tag or the deletion of data.

1. As far as the lifetime of RFID tags is concerned, individual tags can be disabled if it is decided that an alternative use of the tag would be preferable. The disabling can be done by putting the tag in a protective mesh of foil known as a "Faraday cage," which is impenetrable by radio signals of certain frequencies or by "killing" the tag, i.e., removing and destroying it (Eschet 2005, 317/18).

   Nevertheless, it cannot be overlooked that both approaches have certain disadvantages: Possibly, some tags are overlooked or left with the individual. In addition, the "kill" command related to a tag still leaves room for the possibility of reactivation (Weber 2010, 25). Finally, businesses may be inclined to offer clients certain incentives for not destroying tags or secretly giving them the tags.
2. Deletion rights and automatic data deletion are also an important aspect of ensuring privacy as the amount of data collected are growing exponentially [see Schwartz and Solove (2011, 1819)]. Data saved in various scattered databases make it very complicated for an individual to not only theoretically retain but also enforce the right to have the data deleted after a certain period or upon request. Looking from a general perspective, data deletion challenges merit much higher attention, exceeding the notion of the human "right to be forgotten" (Google Spain) recently acknowledged by the European Court of Justice and encompassing new technical solution for the improvement of data privacy.

16.3.5 Challenges through technological innovations

16.3.5.1 Ongoing technological developments

The regulatory framework is usually relatively slow, while technological innovations move very fast. Therefore, efforts to adjust the legal rules are often effectively nullified by new innovations. Recent technologies encompass, for example, location-based services, sensor networks, delay-tolerant networks, and the smart grids. Some legislators still try to adapt traditional telecommunications rules without taking into account that information exchange moves to other infrastructures.

All these new technologies have caused additional risks to privacy and security. In order to minimize such risks, data collection devices should be designed to include basic privacy protection features from the beginning. In fact, the new so-called G2 RFID technology allows the user to hide a part or all the memory of the tag and the ability to read or alter the data depending on the proximity to the tag. Thus, such new technologies will ensure that the control over the data is given back to the data subject (Weber 2015, 623).

However, more and more devices used in daily life create additional challenges. These emerging risks include (i) automatically generating data that are not necessary for providing a service and its collection could potentially have severe privacy implications, (ii) private data

scattered across large distributed systems leads to a loss of control, and (iii) deanonymization results from the linking of data collected across an ever-growing number of devices.

The issues of (i) the quality of data and (ii) the quality of context add a new critical dimension of data privacy and security discussions. These phenomena play an increasingly important role in IoT debates and, therefore, are discussed in more detail in the following sections.

16.3.5.2 Quality of data

The quality of the data collected is increasing with any further information added. Location and environment information leads to a better usability of the data. Thus, the aggregation of data is a quality-improving activity.

The collected data are in most cases not encrypted, as its face value is low. The risks emerge when the automatically collected unencrypted data from various sources are combined and aggregated into one database. Therefore, automated processes should be implemented in IoT devices to ensure privacy by encrypting and anonymizing data.

The quality of the data can be achieved by taking the environment in which it is collected into account. A context attribute may be unknown as long there is no information about it. It may also be ambiguous and/or imprecise when the reported information is correct but not provided with a sufficient degree of precision (Weber 2015, 623).

16.3.5.3 Quality of context

The quality of context raises new issues of confidentiality. The quality of context refers to the embedment of information into the life sphere of an individual and not to the process or the hardware components that possibly provide the information. Up to now, quality of context issues have not been sufficiently discussed even as these phenomena play an increasingly important role in privacy debates [see, for example, Machara Marquez et al. (2013) and de Montjoye et al. (2013)].

A context data may be unknown if there is no information available about it, leading to incomplete context information and wrong interpretations (Weber 2015, 624). It may also be ambiguous or imprecise in case of contradictory information from different context sources. As context data are by nature dynamic and heterogeneous, they tend to be erroneous (i.e., an exact reflection of the real state of the modeled situation is not given).

However, even low-quality context data are useful for data mining algorithms. In addition, the reliable quality of context information is improving the efficiency of such algorithms. Legally, the quality of context data encompasses sensitive information since its value and the potential effects of such data relate to individuals. The combination of parameter values may be used to infer what the operating system of remote machines is because different operating systems, and different versions of the same operating system, set different default values for these parameters (Weber 2015, 625).

16.4 Specific challenges of the IoT for privacy and security

16.4.1 Types of privacy infringements

Data privacy can be infringed in the IoT context at various stages (Miorandi et al. 2012): The first stage concerns the access to the collected data by third parties; the second stage is the use and distribution of data by the data collector; and the third stage encompasses the risks that the data is combined with other data. Individuals are especially unaware of the third case when using IoT devices supplying the data. Such kind of combinations

with other data allows the creation of new information about a person or a situation being potentially of high commercial value.

As mentioned, a particular issue is the quality of context. Information surrounding the collection of the primary data such as the status and attributes of the data-collecting device can lead to a personality profile. The aggregation of a large amount of data (for example, power usage of a household and travel patterns from mobile phone location data) causes the formation of sensitive data collections. Such a development is not compliant with the data minimization principle of data protection laws requiring the limitation of data collection to the furthest extent possible (Weber 2015, 624).

The automated data collection does not necessarily lead to a higher level of trust than in the case of manually collected human data. Therefore, adverse judgments affecting a person based on such data collected by whatever devices should be prevented not only through appropriate technical safeguards but also through regulatory restrictions on the data use (Weber 2015, 624).

16.4.2 Enforcement of the transparency and the data minimization principle

Data collection and data storage must be transparent. Individual rights can be effectively exercised only if the concerned person is aware of the data processing entity and the contents of the databases. Therefore, awareness should be generally created in the society as to the many privacy implications IoT devices can have on an individual.

Transparency tools have been addressed for a few years. Usually, these tools intend to improve the users' understanding and control of their data profiles. Transparency was particularly acknowledged as an important element of privacy in the "Mauritius Declaration on the Internet of Things," proclaimed by the Data Protection and Privacy Commissioners (2014) of more than 100 countries on October 14, 2014: "Transparency is key: those who offer Internet of Things devices should be clear about what data they collect, for what purposes and how long this data is retained."

Four basic characteristics that transparency tools should possess appear to be important in the long run (Weber 2015, 625):

- Provide information about the intended collection, storage, and/or data processing
- Provide an overview of what personal data have been disclosed to what data controller under what policies
- Provide online access to the personal data and how they have been processed by the data controller
- Provide counterprofiling capabilities helping the users to anticipate how their data matches relevant group profiles, which may affect future opportunities and threats

Transparency in the privacy context is also important with respect to technical safeguards. Only if people understand the functions of PETs can they use them efficiently or decide on the implementation in an automated fashion. Transparency might even gain importance in view of the next IoT-based distributed systems compared to the present web-based ubiquitous applications, since users can no longer control the data coming from terminals with which they directly interact (laptop, smartphone, etc.). However, they will have to handle the control of the data automatically produced by the connected devices (Weber 2015, 626).

In the future, data could be scattered across a large distributed system while facing issues such as heterogeneity and scalability of processes. So far, neither experts nor

regulators have undertaken much research in this field notwithstanding the importance of the arising privacy-related topics.

Apart from transparency, the general principle of data minimization is enshrined in practically all data protection laws, such as, in Article 5 of the EU GDPR 2016. This principle aims at limiting the collection and processing of personal data to the amount necessary for the concerned businesses. Again, the legal requirement of data minimization needs to be supported by technical measures. Possible implementation approaches are (Weber 2015, 626) as follows:

- *Encrypted aggregation techniques:* Data are collected only to the extent to which they add value for the intended use.
- *Perturbation:* Data gets systematically altered using a perturbation function (e.g., adding random numbers).
- *Obfuscation:* This concept replaces a certain percentage of data by random values (e.g., change of code in order to make reverse engineering difficult).

In particular, the data minimization principle aims at deleting data from the IoT device or supporting systems when the data are no longer relevant and when continued storage is not justified. Nevertheless, in the IoT context, the data minimization principle must be balanced against the demands of civil society and businesses for more functionality. Thus, the problem (to be solved) arises to what extent and under what circumstances technical possibilities exist for putting back "deleted" data in its original state, if at a later stage, a new need to read the information should occur.

16.4.3 Confidentiality and anonymity challenges

Confidentiality is a legal notion that has been relevant in public and private law for centuries. Under certain circumstances, information is only disclosed to a small circle of persons. Its content should not be available to persons other than the specific addressees. For example, in governments and administrative agencies, certain data are classified as confidential information; typically, this is the case for federal and state investigating authority inquiries (e.g., the Federal Bureau of Investigation, the Department of Justice, and the police). In the private law, similar protections exist, for example, the attorney–client privilege or the medical doctor–patient secrecy in the healthcare sector.

The new technologies allow an improvement of the framework for confidentiality interests. Particularly, the PETs (cf. Section 16.3.3) can protect data from unauthorized access by third persons. Privacy measures can support confidentiality requirements by providing solutions for anonymizing the collected data (including the communications).

The "anonymity of data" [see Weber and Heinrich 2012)] can be indexed by cryptographic measures. Such measures are designed to reflect properties such as (i) unlinkability (two information items or two actions of the same person cannot be related), (ii) undetectability (a third person is not able to ascertain whether an information item exists), (iii) unobservability (it is not possible to detect whether a system is being visited by a certain user), and (iv) communications content confidentiality (Weber 2015, 622).

During recent years, new technologies have been developed allowing a disclosure of information to a third person but protecting the anonymity of the person from whom the data were collected while still retaining its value. The best-known model is called *k*-anonymity, which is aimed at reducing the risk of reidentification by linking datasets. The *k*-anonymity model addresses the problem of directly matching externally available

data and claims that an individual cannot be identified within a set of k users. Therefore, protection is provided if the information for each person is not distinguishable from at least $k - 1$ individuals whose information is also contained in a given data set (Sweeney 2002). Thus, this approach requires a structuring of the data, which protects against the identification of an individual.

However, the *k*-anonymity model is susceptible to background knowledge and homogeneity attacks (Machanavajjhala et al. 2006). As a consequence, a further refined variant has been developed, namely, the L-diversity model; a block of data is L-diverse if it contains at least L well-represented values for the sensitive attribute S (Wang and Wang 2013). So far, this approach has mainly been effective in cases of static data, but due to increased research efforts, the L-diversity method is now also applicable to incremental data disclosure (Wang and Wang 2013).

Normative frameworks from competent regulatory authorities come into play in this context, since legal rules must define under which circumstances the noncompliance with anonymity requirements constitutes a data breach. The relevant term is called *differential privacy*, which is aimed at providing means to maximize the accuracy of queries from statistical databases while minimizing the risks of identifying its records (Dwork and Roth 2014).

Anonymity in communications has the objective of protecting traffic data by avoiding disclosure of who talks to whom. Even if the content of a communication is kept confidential (or anonymous), sensitive information can still be gained by analyzing the leaked traffic data, namely, the respective data can include locations and identities of the parties in the communication, time, frequency, and the volume of the information exchange (Weber 2015, 623). Therefore, privacy laws also need to protect such kind of data.

16.4.4 Cybersecurity regulations in particular

As mentioned, cybersecurity issues play a role in the data security context of the IoT. Apart from the quite outdated and not globally applicable Cybercrime Convention (CETS 185) of the Council of Europe (Budapest Convention) of November 2001 [for further details, see Weber and Studer (2016, 722/23) and Nappinai (2017, 43)], only a recent regional legal instrument is available, namely, the Network and Information Security (NIS) Directive of the EU of May 2016. Based on the preparatory work of the 2004 established European Network and Information Security Agency, the NIS Directive has the objective of implementing a culture of network and information security for the benefit of citizens, consumers, businesses, and public sector organizations in the EU [for further details Weber and Studer (2016, 723)]. The NIS concept encompasses the ability of networks and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity, or confidentiality of stored or transmitted or processed data or the related services [for the United States, see Shackelford et al. (2016)].

The NIS Directive sets forth the following main topics and measures to realize the desired level of information security:

- *Improved national cybersecurity capabilities:* A national cybersecurity strategy should be developed and adopted designing a policy and a regulatory environment for information security as well as establishing adequate institutional capacities.
- *Improved EU-level cooperation:* Strategic cooperation and exchange of information must be secured.

- *Security and incident notification requirements:* The respective requirements are differently designed for operators of essential services and digital services providers [for further details, see Weber and Studer (2016, 714)].

The NIS Directive has been subjected to critical assessments; mainly, the weakening of certain provisions during the legislative process (relatively low level of "minimum" harmonization) is debated. Furthermore, some requirements imposed on digital operators are subject to an open interpretation. Nevertheless, this new legal instrument has at least the chance to adapt the regulatory environment to new cybersecurity needs by obliging a wide range of industries and other players to pay more attention to the challenging issue of information security.

16.4.5 Interoperability and connectivity requirements

With the increased availability of IoT applications, challenges in respect to the interoperability and connectivity of the new services also increase. An added value for users (civil society and businesses) depends on the possibilities to bring different networks and services "together" as was done in the case of different Internet protocols some 30 years ago. Interoperability and connectivity requirements have been known for decades from telecommunications markets; in the IoT field, the problems are not substantially deviating but technically often more complicated.

The Open Interconnect Consortium (OIC) was founded in July 2014 to improve interoperability and connectivity. The efforts of the OIC go in the direction of defining a common communications framework based on industry-standard technologies to wirelessly connect and intelligently manage the data flow among emerging IoT devices, regardless of form factor, operating system or service provider. The OIC assembles leaders from a broad range of industry vertical segments, from smart home and office solutions to automotive and more. As an objective, OIC specifications and open-source implementations should support businesses in the design of products that intelligently, reliably, and securely manage and exchange data under changing conditions, power, and bandwidth, even in the case of lack of an Internet connection (Broadcom 2014).

At first instance, interoperability and connectivity facilitate the execution of business transactions. But the respective technical requirements can also uphold privacy standards; if the respective instruments are in place and enable the smooth "transfer" from one system to another system, technically encrypted, and thereby, privacy-protecting data do not risk being disclosed during a transmission chain.

16.5 Outlook

The IoT opens up a world of opportunities because it is applicable to a wide range of sectors and markets, including logistics and transportation management, connected furniture and appliances, agricultural monitoring systems, smart clothes and accessories, toys, entertainment, and art. The steadily growing number of IoT products and devices will make life easier for individuals while creating privacy risks by targeting individuals unknowingly at the same time.

Nevertheless, based on the technical and regulatory complexity of IoT, the future of digital privacy will strongly depend on the willingness of the IoT industry to implement its own standards. These standards must consider the nature and context of the collected data and offer tailored solutions as part of the technological backbone.

Furthermore, efforts must be made to negotiate international standards which are based on an international agreement and have binding effect, providing both enforceable rights against the suppliers of IoT technology as well as the providers of the ancillary software environment. So far industry standards as to security have been very effective. However, data protection and privacy require a much broader foundation that is based on both technical standards and an appropriate legal framework.

The ultimate solution to complex issues raised by IoT may be the combination of law and technology together with a universally agreed industry standard. Any such legal–tech solution must allow for both an efficient technical process and a data protection policy conform use of the collected IoT data. In doing so, such a toolset could also address many of the issues that create uncertainty in the market such as the application of the controller or processor definition to IoT device manufacturers. If they are part of a broader solution, they will not need to rely on ambiguous interpretations of the GDPR to be compliant. Furthermore, such tools would facilitate the documentation of the collected data and the use by third parties, thereby allowing for more transparent processing and facilitating of the enforcement of data subject rights. Such a PbD approach would mitigate most of the data protection and security issues that arise in most IoT settings.

In summary, many challenges lie ahead: security and privacy issues, product energy and maintenance needs, new product–person relationship models, product–user–manufacturer relationships, as well as new business models reflecting this duality. To facilitate the seamless implementation process of both privacy and security frameworks, a coordinated approach on both the international and national levels is necessary and warranted.

References

Broadcom (2014), *Industry Leaders to Establish Open Interconnect Consortium to Advance Interoperability for Internet of Things*, Press Release, July 9, 2014, Broadcom, San Jose, CA, available at http://www.broadcom.com/press/release.php?id=s858114.

Cavoukian A. (2009), *Privacy by Design, 7 Foundational Principles*, available at https://www.privacybydesign.ca/index.php/about-pdb/7-foundational-principles/.

Data Protection and Privacy Commissioners (2014), *Mauritius Declaration on the Internet of Things*, 36th International Conference of Data Protection and Privacy Commissioners, available at http://www.privacyconference2014.org/madia/16596/Mauritius-Declaration.pdf.

de Montjoye Y., Hidalgo C.A., Verleysen M., and Blondel V.D. (2013), Unique in the crowd: The privacy bounds of human mobility, *Nature Scientific Reports* 3, 1376.

Dwork C., and Roth A. (2014), The algorithmic foundations of differential privacy, *Theoretical Computer Science* 9 (2014), 211–407.

EPC Global (2008), *Object Naming Service (ONS) Version 1.0.1*, EPC Global, Lawrenceville, NJ, available at http://www.gs1.org/sites/default/files/docs/epc/ons_1_0_1-standard-20080529.pdf.

Eschet G. (2005), Protecting privacy in the web of radio frequency identification, *Jurimetrics* 45 (2005), 301–322.

European Commission (2013), *Public Consultation on the IoT Governance*, European Commission, Brussels, available at https://ec.europa.eu/digital-single-market/en/news/conclusions-internet-things-public-consultation.

European Commission (2014), *WP29 (Article 29 Data Protection Working Party): Opinion 8/2014 on the Recent Developments on the Internet of Things* (September 16, 2014), European Commission, Brussels available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf.

Fabian B., and Günther O. (2007), Distrubted ONS and its impact on irivacy, *IEEE Communications 2007*, Institute of Electrical and Electronics Engineers, Piscataway, NJ, available at http://ieeexplore.ieee.org/document/4288878.

Fabian B., and Günther O. (2009), Security challenges of the EPC Global Network, *Communications of the ACM* 52 (2009), 121–125.

Finneran Dennedy M., Fox J., and Finneran T.R. (2014), *The Privacy Engineer's Manifesto*, Apress Media, New York.

FTC (Federal Trade Commission) (2015, January) *Staff Report, Internet of Things: Privacy and Security in a Connected World*, FTC, Washington, DC, available at https://www.ftc.gov/system/files/documents/reprts/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-of-things-privacy/150127iotrpt.pdf.

Hewlett–Packard (2015), *Hewlett–Packard Internet of Things Research Study*, Report 2015, Palo Alto, CA, available at http://www.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf.

Internet Society (2015), *The Internet of Things: An Overview*, Internet Society, Reston, VA, available at https://www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151014_0.pdf.

ITU (International Telecommunications Union) (2012), *ITU-T Recommendation Y.2060, Overview of the Internet of Things (6/2012)*, ITU, Geneva, available at http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11559.

Machanavajjhala A., Gehrke J., and Kifer D. (2006), L-Diversity: Privacy beyond k-anonymity, *Proceedings of the 22nd International Conference on Data Engineering, Los Alamitos*, IEEE Computer Society, Washington, DC, 24–35.

Machara Marquez S., Chabridon S., and Taconet C. (2013), Trust-based Context Contract Models for the Internet of Things, UIC/ATC 2013, 557–562, available at https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6726259.

Miorandi D., Sicari S., de Pellegrini F., and Chlamtac I. (2012), Internet of things: Vision, Applications and Research Challenges, *Ad Hoc Networks* 10 (2012), 1497–1516.

Nappinai N.S. (2017), Dark side of IoT, *CRi* 2 (2017), 39–45.

Schmid V. (2008), Radio frequency identification law beyond 2007, in Floerkemeier Ch., Langheinrich M., Fleisch E., Mattern F., and Sarma S.E. (eds.), *The Internet of Things*, Springer, Berlin, 196–213.

Schwartz P., and Solove D. (2011), The PII problem: Privacy and a new concept of personally identifiable information, *New York University Law Review* 86/6 (2011), 1814–1894.

Shackelford S.J., Russell S., and Hunt J. (2016), Bottoms up: A comparison of voluntary cybersecurity frameworks, *UC Davis Business Law Journal* 2016, 217–260.

Sweeney L. (2002), k-Anonymity: A model for protection of privacy, *International Journal on Uncertainty, Fuzziness and Knowledge-Based Systems* 10 (2002), 557–570.

Wang P., and Wang J. (2013), L-diversity algorithm for incremental data release, *Applied Mathematics & Information Services* 7 (2013), 2055–2060.

Weber R. H. (2010), Internet of things—New security and privacy challenges, *Computer Law & Security Review* 26 (2010), 23–30.

Weber R. H. (2015), Internet of things: Privacy issues revisited, *Computer Law & Security Review* 31 (2015), 618–627.

Weber R. H. (12016, Governance of the Internet of things—From infancy to first attempts of implementation? *MPDI Laws* 5 (2016), 28–39.

Weber R.H., and Heinrich U. 2012, *Anonymization*, Springer, London.

Weber R.H., and Studer E. (2016), Cybersecurity in the Internet of things: Legal aspects, *Computer Law & Security Review* 32 (2016), 715–728.

Wynzard Group, Advanced Crime Analytics, The fastest way to reveal actionable intelligence hidden in your data, available at https://wynyardgroup.com/crime_analytics.php.

Xiao Q., Gibbons T., and Lebrun H. (2000), *RFID Technology, Security Vulnerabilities, and Countermeasures*, 357, in Huo Y. (ed.). Supply Chain the Way to Flat Organisation seq., available at http://cdn.intechopen.com/pdfs-wm/6177.pdf.