available at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Internet of Things – New security and privacy challenges

Rolf H. Weber

University of Zurich, Zurich, Switzerland, and University of Hong Kong, Hong Kong

Keywords:
Data protection
Internet of Things
Privacy
RFID
Security

ABSTRACT

The Internet of Things, an emerging global Internet-based technical architecture facilitating the exchange of goods and services in global supply chain networks has an impact on the security and privacy of the involved stakeholders. Measures ensuring the architecture's resilience to attacks, data authentication, access control and client privacy need to be established. An adequate legal framework must take the underlying technology into account and would best be established by an international legislator, which is supplemented by the private sector according to specific needs and thereby becomes easily adjustable. The contents of the respective legislation must encompass the right to information, provisions prohibiting or restricting the use of mechanisms of the Internet of Things, rules on IT-security-legislation, provisions supporting the use of mechanisms of the Internet of Things and the establishment of a task force doing research on the legal challenges of the IoT.

1. Internet of Things: notion and technical background

The Internet of Things (IoT) is an emerging global Internet-based information architecture facilitating the exchange of goods and services in global supply chain networks.[1] For example, the lack of certain goods would automatically be reported to the provider which in turn immediately causes electronic or physical delivery. From a technical point of view, the architecture is based on data communication tools, primarily RFID-tagged items (Radio-Frequency Identification).[2] The IoT[3] has the purpose of providing an IT-infrastructure facilitating the exchanges of "things" in a secure and reliable manner.[4]

The most popular industry proposal for the new IT-infrastructure of the IoT is based on an Electronic Product Code (EPC), introduced by EPCglobal and GS1.[5] The "things" are physical objects carrying RFID tags with a unique EPC; the infrastructure can offer and query EPC Information Services (EPCIS) both locally and remotely to subscribers.[6] The

[1] For a general overview see Rolf H. Weber, Internet of Things – Need for a New Legal Environment? [2009] 25 Computer Law & Security Review 521.

[2] RFID is a technology used to identify, track and locate assets; the universal, unique identification of individual items through the EPC is encoded in an inexpensive RFID tag.

[3] The term "IoT" has been "invented" by Kevin Ashton in a presentation in 1998 (see Gerald Santucci, Paper for the International Conference on Future Trends of the Internet, From Internet of Data to Internet of Things, at p. 2, available at: ftp://ftp.cordis.europa.eu/pub/fp7/ict/docs/enet/20090128-speech-iot-conference-lux_en.pdf).

[4] For general overviews of the technical background of the IoT see Christian Floerkemeier/Marc Langheinrich/Elgar Fleisch/Friedemann Mattern/Sanjay E. Sarma (eds), The Internet of Things, Berlin/Heidelberg 2008; Lu Yan/Yan Zhang/Laurence T. Yang/Huansheng Ning (eds), The Internet of Things, New York/London 2008.

[5] See http://www.epcglobalinc.org.

[6] See Benjamin Fabian, Secure Name Services for the Internet of Things, Thesis, Berlin 2008, 30/31; to the details of the service orientation and the context-aware computing see Davy Preuveneers/Yolande Berbers, Internet of Things: A Context-Awareness Perspective, in: Yan/Zhang/Yang/Ning, supra note 4, 288, at 296 ss.

0267-3649/$ – see front matter
doi:10.1016/j.clsr.2009.11.008

information is not fully saved on an RFID tag, but a supply of the information by distributed servers on the Internet is made available through linking and cross-linking with the help of an Object Naming Service (ONS).[7]

The ONS is authoritative (linking metadata and services) in the sense that the entity having – centralized – change control over the information about the EPC is the same entity that assigned the EPC to the concerned item.[8] Thereby, the architecture can also serve as backbone for ubiquitous computing, enabling smart environments to recognize and identify objects, and receive information from the Internet to facilitate their adaptive functionality.[9] The central ONS root is operated by the (private) company VeriSign, a provider of Internet infrastructure services.

The ONS is based on the well-known Domain Name System (DNS). Technically, in order to use the DNS to find information about an item, the item's EPC must be converted into a format that the DNS can understand, which is the typical, ''dot'' delimited, left to right form of all domain names.[10] Since EPC is encoded into syntactically correct domain name and then used within the existing DNS infrastructure, the ONS can be considered as subset of the DNS. For this reason, however, the ONS will also inherit all of the well-documented DNS weaknesses, such as the limited redundancy in practical implementations and the creation of single points of failure.[11]

2. Security and privacy needs

2.1. Requirements related to IoT technology

The described technical architecture of the IoT has an impact on the security and privacy of the involved stakeholders. Privacy includes the concealment of personal information as well as the ability to control what happens with this information.[12] The right to privacy can be considered as either a basic and inalienable human right, or as a personal right or possession.[13]

The attribution of tags to objects may not be known to users, and there may not be an acoustic or visual signal to draw the attention of the object's user. Thereby, individuals can be followed without them even knowing about it and would leave their data or at least traces thereof in cyberspace.[14] Further aggravating the problem, it is not anymore only the state that is interested in collecting the respective data, but also private actors such as marketing enterprises.[15]

Since business processes are concerned, a high degree of reliability is needed. In the literature, the following security and privacy requirements are described:[16]

- *Resilience to attacks*: The system has to avoid single points of failure and should adjust itself to node failures.
- *Data authentication*: As a principle, retrieved address and object information must be authenticated.[17]
- *Access control*: Information providers must be able to implement access control on the data provided.[18]
- *Client privacy*: Measures need to be taken that only the information provider is able to infer from observing the use of the lookup system related to a specific customer; at least, inference should be very hard to conduct.

Private enterprises using IoT technology will have to include these requirements into their risk management concept governing the business activities in general.

2.2. Privacy enhancing technologies (PET)

The fulfilment of customer privacy requirements is quite difficult. A number of technologies have been developed in order to achieve information privacy goals. These Privacy Enhancing Technologies (PET) can be described in short as follows:[19]

- *Virtual Private Networks (VPN)* are extranets established by close groups of business partners. As only partners have access, they promise to be confidential and have integrity. However, this solution does not allow for a dynamic global information exchange and is impractical with regard to third parties beyond the borders of the extranet.
- *Transport Layer Security (TLS)*, based on an appropriate global trust structure, could also improve confidentiality and integrity of the IoT. However, as each ONS delegation step

[7] Fabian, supra note 6, at 33.

[8] EPCglobal, Object Naming Service (ONS) Version 1.0.1, at para 4.2, available at: http://www.epcglobalinc.org/standards/ons/ons_1_0_1-standard-20080529.pdf.

[9] Fabian, supra note 6, at 1.

[10] EPCglobal, Object Naming Service (ONS) Version 1.0.1, supra note 8, at para 5.2.

[11] For more details see Weber, supra note 1.

[12] Seda F. Gürses/Bettina Berendt/Thomas Santen, Multilateral Security Requirements Analysis for Preserving Privacy in Ubiquitous Environments, in: Bettina Berendt/Ernestina Menasalvas (eds), Workshop on Ubiquitous Knowledge Discovery for Users (UKDU '06), at 51–64; for privacy as freedom see Gus Hosein, Privacy as Freedom, in: Rikke Frank Jørgensen (ed.), Human Rights in the Global Information Society, Cambridge/Massachusetts 2006, at 121–147.

[13] Gürses/Berendt/Santen, supra note 12, at 54.

[14] See also Ari Juels, RFID Security and Privacy: A Research Survey, IEEE Journal on Selected Areas in Communications, Vol. 24, 2006, 381–394, at 383; Marc Langheinrich Marc/Friedemann Mattern, Wenn der Computer verschwindet, digma 2002, 138–142, at 139; Friedemann Mattern, Ubiquitous Computing: Eine Einführung mit Anmerkungen zu den sozialen und rechtlichen Folgen, in: Jürgen Taeger/Andreas Wiebe (eds), Mobilität. Telematik, Recht, Köln 2005, 1–34, at 18 s.

[15] Mattern, supra note 14, at 24.

[16] See Benjamin Fabian/Oliver Günther, Distributed ONS and its Impact on Privacy, 1223, 1225, available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=04288878.

[17] For RFID authentication see Juels, supra note 14, at 384 s; Rolf H. Weber/Annette Willi, IT-Sicherheit und Recht, Zurich 2006, at 284.

[18] See also Eberhard Grummt/Markus Müller, Fine-Grained Access Control for EPC Information Services, in: Floerkemeier/Langheinrich/Fleisch/Mattern/Sarma, supra note 4, at 35–49.

[19] Fabian, supra note 6, 61 s; Benjamin Fabian/Oliver Günther, Security Challenges of the EPCglobal Network, Communications of the ACM, Vol. 52, July 2009, 121–125, at 124 s.

requires a new TLS connection, the search of information would be negatively affected by many additional layers.

- *DNS Security Extensions (DNSSEC)* make use of public-key cryptography to sign resource records in order to guarantee origin authenticity and integrity of delivered information. However, DNSSEC could only assure global ONS information authenticity if the entire Internet community adopts it.
- *Onion Routing* encrypts and mixes Internet traffic from many different sources, i.e. data is wrapped into multiple encryption layers, using the public keys of the onion routers on the transmission path. This process would impede matching a particular Internet Protocol packet to a particular source. However, onion routing increases waiting times and thereby results in performance issues.
- *Private Information Retrieval (PIR)* systems conceal which customer is interested in which information, once the EPCIS have been located. However, problems of scalability and key management, as well as performance issues would arise in a globally accessible system such as the ONS, which makes this method impractical.

A further method to increase security and privacy are Peer-to-Peer (P2P) systems, which generally show good scalability and performance in the applications. These P2P systems could be based on Distributed Hash Tables (DHT). Access control, however, must be implemented at the actual EPCIS itself, not on the data stored in the DHT, as there is no encryption offered by any of these two designs.[20] Insofar, the assumption is reasonable that encryption of the EPCIS connection and authentication of the customer could be implemented without major difficulties, using common Internet and web service security frameworks.[21] In particular, the authentication of the customer can be done by issuing shared secrets or using public-key cryptography.[22]

It is important that an RFID tag having been attached to an object can – at a later stage – be disabled in order to allow for customers to decide whether they want to make use of the tag. RFID tags may either be disabled by putting them in a protective mesh of foil known as a "Faraday Cage" which is impenetrable by radio signals of certain frequencies or by "killing" them, i.e. removing and destroying them.[23] However, both options have certain disadvantages. While putting tags in a special cage is relatively safe, it requires that every tag from every single product is put in that cage if a customer desires so. Chances are that certain tags will be overlooked and left with the client and that he/she could still be traced. Sending a "kill" command to a tag leaves room to the possibility of reactivation or that some identifying information could be left on the tag. Furthermore, businesses may be inclined to offer clients incentives for not destroying tags or secretly give them tags.[24] Instead of killing tags, the dissolution of the connection between the tag and the identifiable object could be envisaged. The information on ONS is deleted to protect the privacy of the owner of the tagged object. While the tag can still be read, further information with potential information concerning the respective person, however, are not retrievable.[25]

Moreover, transparency is also needed for non-personally identifiable information retrieved by RFID. An active RFID can for example trace movements of visitors of an event real time without identifying the persons as such who remain anonymous; nevertheless, the question remains whether such information not covered by traditional privacy laws might be collected without any restriction.[26]

2.3. *Legal course of action*

The European Commission is aware of the security and privacy issues related to the RFID and the IoT. In a Recommendation of May 12, 2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification[27] the European Commission invites the Member States to provide for guidance on the design and operation of RFID applications in a lawful, ethical and socially and politically acceptable way, respecting the right to privacy and ensuring protection of personal data (No. 1). In particular, the Recommendation outlines measures to be taken for the deployment of RFID application to ensure that national legislation is complying with the EU Data Protection Directives 95/46, 99/5 and 2002/58 (No. 2). Member States should ensure that industry in collaboration with relevant civil society stakeholders develops a framework for privacy and data protection impact assessments (PIA; No. 4); this framework should be submitted to the Article 29 Data Protection Working Party within 12 months. Industry and civil society stakeholders are in the process of establishing the requested framework PIA until late 2009. The objectives of the PIA are designed to identify the implications of the application on privacy and data protection, to determine whether the operator has taken appropriate technical and organizational measures to ensure respective protection, to document the measures implemented with respect to the appropriate protection, and to serve as a basis for a PIA report that can be submitted to the competent authorities before deployment of the application. Presumably, the framework should serve to determine a common structure and content of reports. In particular, RFID application description and scope, RFID application governing practices, accountability and analysis and resolution seem to be of importance. Furthermore, operators are asked to conduct an assessment of the implications of the application implementation for the protection of

[20] Benjamin Fabian/Oliver Günther, Distributed ONS and its Impact on Privacy, 1225, available at http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=04288878.
[21] Fabian/Günther, supra note 19, at 123.
[22] Fabian/Günther, supra note 20, at 1227.
[23] Gal Eschet, Protecting Privacy in the web of Radio Frequency Identification, Jurimetrics, Vol. 45, 2005, 301–332, at 317 s.
[24] Eschet, supra note 23, at 137 ss.
[25] Jürgen Müller/Matthias Handy, RFID als Technik des Ubiquitous Computing – Eine Gefahr für die Privatsphäre?, at 17, available at: http://www.imd.uni-rostock.de/veroeff/handy_bamberg05.pdf.
[26] See Weber/Willi, supra note 17, at 245 ss; Viola Schmid, Radio Frequency Identification Law Beyond 2007, in: Floerkemeier/Langheinrich/Fleisch/Mattern/Sarma, supra note 4, 196–213, at 196; Benjamin Fabian/Oliver Günther/Sarah Spiekermann, Security Analysis of the Object Name Service, at 1 ss, available at http://lasecwww.epfl.ch/~gavoine/download/papers/FabianGS-2005-sptpuc.pdf.
[27] COM (2009) 3200 final.

personal data and privacy and take appropriate technical and organizational measures to ensure the protection of personal data and privacy (No. 5), and a person within a business needs to be designated for the review of the assessments and the continued appropriateness of the technical and organizational measures. In addition, Member States are invited to support the EU Commission in identifying those applications that might raise information security threats with implications for the general public (No. 6). Additional provisions of the Recommendation concern the information and transparency on RFID use, the RFID applications used in the retail trade, the awareness raising actions, research and development as well as follow-up actions (Nos. 7–18).

In its specific Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the Internet of Things (an Action Plan for Europe), the EU Commission again points to the importance of security and privacy in the IoT framework.[28] The particular Line of Action 2 encompasses the continuous monitoring of the privacy and the protection of personal data questions; as part of Line of Action 3 the EU Commission is envisaging to launch a debate on the technical and the legal aspects of the ''right to silence of the chips'' and expresses the idea that individuals should be able to disconnect from their networked environment at any time.

3. Milestones of an adequate legal framework

The implementation of the IoT architecture and the use of RFID pose a number of legal challenges; the basic questions of the agenda can be phrased as follows[29]:

Is there a need for (international or national) state law or are market regulations of the concerned businesses sufficient?

If legislation is envisaged: Would existing/traditional legislation be sufficient or is there a need for new laws?

If new laws are to be released: Which kind of laws are required and what is the time frame for their implementation?

These legal challenges need to be embedded into the human rights and constitutional framework. Insofar, the decision of the German Supreme Court of 27 February 2008 constituting an independent fundamental right of confidentiality and integrity related to info-technical systems merits attention.[30]

3.1. *Systematic approach*

The establishment and implementation of an appropriate legal framework[31] calls for a systematic approach[32] in relation to the legislative process. Thereby, the following aspects should be taken into account:[33]

- Facts about RFID using scenarios are to be systematically developed; only under the condition that the facts are sufficiently known, adequate legal provisions can be drafted.
- A systematization of the legal problems potentially occurring can be done by coordination along the below discussed four technical axes, namely globality, verticality, ubiquity and technicity.
- The legal challenges of security and privacy issues related to the IoT and RFID are to be qualitatively classified.

In particular, the question must be addressed how much privacy the civil society is prepared to surrender in order to increase security. Solutions should be looked for allowing considering privacy and security not as opposites, but as principles affecting each other.[34]

In light of the manifold factual scenarios, it appears to be hardly possible to come to a homogenous legal framework governing all facets of the IoT and RFID. Moreover, a heterogeneous and differentiated approach will have to be taken into account. Thereby, the technical environment can be crystallized along the four axes, representing the most important challenges to the establishment of regulation:[35]

- *Globality* is based on the fact that goods and services in the IoT context will be globally marketed and distributed. The RFID technology is also ''global'' in the sense that the same technical processes are applied all over the world. Consequently, business and trade would be heavily complicated if differing national laws would be in place. If the RFID-tagged products are available on a global level, the legal systems need to be synchronized.
- *Verticality* means the potential durability of the technical environment. In particular, it is important for the life of the IoT that RFID-tagged products are lasting long enough to not only use them in the supply chain until the final customer, but also for example in the waste management. For the time being, this requirement is not sufficiently met in the EPC traffic.
- *Ubiquity* refers to the extent of the RFID-tagged environment; technically, RFID could indeed be used ubiquitously encompassing persons, things, plants, and animals.

[28] COM (2009) 278 final.

[29] Schmid, supra note 26, at 200.

[30] See Decision 1 BvR 370/07 and 1 BvR 595/07; to this decision see Rolf H. Weber, Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität, digma 2008, 94–97; Thomas Stögmüller, Vertraulichkeit und Integrität informationstechnischer Systeme in Unternehmen, CR 2008, 435–439; Bernd Holznagel/Pascal Schumacher, Auswirkungen des Grundrechts auf Vertraulichkeit und Integrität informationstechnischer Systeme auf RFID-Chips, MMR 2009, 3–8.

[31] A general overview in respect of the globalization developments which confront privacy issues is given by Herbert Burkert, Globalization – Strategies for Data Protection, Weblaw-Jusletter, 3 October 2005, at nos. 11–25.

[32] See also Pieter Kleve/Richard De Mulder, Privacy protection and the right to information: in search of a new symbiosis in the information age, in: Sylvia Kierkegaard Mercado (ed.), Cyberlaw, Security and Privacy, Beijing 2007, 201, at 205/06.

[33] Schmid, supra note 26, at 201 s.

[34] Kleve/De Mulder, supra note 32, at 207.

[35] For more details see Schmid, supra note 26, at 204 ss.

- *Technicity* is an important basis for the development of rules protecting privacy objectives. Several differentiations can be taken into account, namely (i) the complexity of the tag (active and passive, rewritable, processing and sensor provided products), (ii) the complexity of background devices (reader or other linked media) and the maximum reading range which is particularly designed to cover transparency demands.[36]

These four requirements have to be taken into account when establishing a legal framework binding all participants of the IoT. Resulting from these four requirements, the framework to be established has to be global, i.e. established by an international legislator, and applicable to every object on earth from its becoming until its destruction. The ubiquity needs to be addressed in particular if various objects are put together to form a new ''thing''.

This new ''thing'' can either be attributed with a new tag, or the creation can carry multiple tags. While the first scenario is more practical, this solution may leave businesses with the problem that individual parts cannot be traced back to their origin. A solution may be that the one tag attached to the object makes reference to the different sources of all individual parts. A global consensus needs to be found, which is then generally applied. The question raised is also connected to the fourth requirement, technicity. If composed objects keep all the tags of integrated parts, tracing all relevant information concerning that object becomes extremely complex and difficult. As this discussion demonstrates, determining an appropriate legal framework raises various technical questions. Therefore, the inclusion of technical experts in the process-making seems inevitable. Furthermore, the discussion also shows that the framework needs to be established at an international level and address all fundamental issues. Otherwise, the IoT becomes impractical and cannot be used efficiently.

The following conclusion for a potential legislation can be drawn from the mentioned systematic approach[37]: A unique strategy will not be suitable to satisfactorily cope with the privacy challenges of the IoT. Inevitably, legislators have to make good use of several of them. In particular, due consideration of technicity seems to be of major importance. Furthermore, data protection and privacy need communication strategies establishing an effective platform for dialogue between state legislators, non-governmental organizations, public interest groups and the international private sector.

3.2. *State law or self-regulation*

The establishment of an adequate legal framework for the protection of security and privacy in the IoT is a phenomenon giving rise to the question of the appropriate legal source. Various regulatory models are available in theory: Apart from the possibility of no regulation at all, which cannot be considered as a real ''solution'', the choice is principally between traditional national regulation, international agreements and self-regulation.[38] As mentioned, national regulation has the disadvantage of not meeting the globalization needs of an adequate legal framework in view of the fact that transactions through the IoT are usually of a cross-border nature.

(i) So far, the regulatory model in the IoT is based on self-regulation through manifold business standards, starting from technical guidelines and leading to fair information practices. In particular, the EPC-Guidelines[39] rely on components like ''Consumer Notice'', ''Consumer Education'' and ''Retention and IT-Security Policy''. Consequently, the compliance with the EPC-Guidelines is driven by a self-control strategy.[40] This self-regulatory model follows the well-known principle of subsidiarity, meaning that the participants of a specific community try to find suitable solutions (structures, behaviors) themselves as long as government intervention has not taken place.[41] The legitimacy of self-regulation is based on the fact that private incentives lead to a need-driven rule-setting process. Furthermore, self-regulation is less costly and more flexible than State law.[42] In principle, self-regulation is justified if it is more efficient than state law and if compliance with rules of the community is less likely than compliance with self-regulation.[43]

The theoretical approaches to the self-regulatory model show a multi-faceted picture[44]: In many cases, self-regulation is not more than a concept of a private group, namely a concept occurring within a framework that is set by the government (directed self-regulation or audited self-regulation). This approach has gained importance during the last decade: if the government provides for a general framework which can be substantiated by the private sector often the term ''co-regulation'' is used. The state legislator does not only set the legal yardsticks or some general pillars of the legal framework, but eventually the government remains involved in the self-regulatory initiatives at least in a monitoring function supervising the progress and the effectiveness of the initiatives in meeting the perceived objectives.

In this context, the legal doctrine has developed the notion ''soft law'' for private commitments expressing more than just policy statements, but less than law in its strict sense, also possessing a certain proximity to law and a certain legal relevance.[45] Nevertheless, the term ''soft law'' does not yet have a clear scope or reliable content. Particularly in respect to the enforceability of rules, law is either in force (''hard law'') or not in force (''no law''), meaning that it is difficult to distinguish between various degrees of legal force. Generally, it can only be said that soft law is a social notion close to law and that it usually covers certain forms of expected and acceptable

[36] Schmid, supra note 26, at 205 s.
[37] See also Burkert, supra note 31, at nos. 21–23.
[38] Rolf H. Weber, Shaping Internet Governance: Regulatory Challenges, Zurich 2009, at 10 s.
[39] See http://www.epcglobalinc.org/public/ppsc_guide.
[40] Schmid, supra note 26, at 199.
[41] Weber, supra note 38, at 18.
[42] Eschet, supra note 23, at 322 s.
[43] Weber, supra note 38, at 18.
[44] For further detail see Weber, supra note 38, at 18 s with further references.
[45] Weber, supra note 38, at 20.

codes of conduct.[46] This concept of self-regulation cannot overcome the lack of an enforcement strategy if compliance is not done voluntarily.[47] Therefore, the involvement of the legislator seems to be inevitable.

While self-regulation has gained importance during the last years, there are still critics thereof, pointing out that self-regulatory mechanisms only regulate those motivated or principled enough to take part in them as market pressure is not yet strong enough to oblige everyone to adopt the respective rules. Furthermore, it is argued that self-regulation is only adopted by stakeholders to satisfy their own interests and is therefore not effective in the protection of privacy.[48]

(ii) Therefore, even if the manifold merits of self-regulation are to be honoured, some pillars of the legal framework in the context of security and privacy need to be set by the legislator. Such law would have to be introduced on an international level. Contemporary theories addressing international law aspects tend to acknowledge a wide definition of international law, according to which this field is no longer limited merely to relations between nation states but generally accepts the increasing role of other international players such as individual human beings, international organizations and juridical entities.[49] Since customary rules can hardly develop in a fast moving field such as the IoT, the main legal source is to be seen in the general principles of law, such as good will, equal treatment, fairness in business activities, legal validity of agreements etc.[50] These general principles can be illustrated as ''abstractions form a mass of rules'' which have been ''so long and so generally accepted as to be no longer directly connected with state practice''.[51] To some extent, basic legal principles are considered to be an expression of ''natural law''; practically, general legal principles may be so fundamental that they can be found in virtually every legal system.[52]

The specific problem in view of security and privacy, however, consists in the appreciation that privacy concerns are not identical in the different regions of the world which makes the application of general principles difficult in cross-border business activities. Therefore, a basic legal framework should be introduced by an international legislator; however, the details of the legal rules for the protection of security and privacy needs are to be developed by the private sector.

The IoT being a new system itself, the idea of entrusting a body with its legislation and governing that is new, too, is not far-fetched. A new body would be in the position to take into account all the characteristics of the IoT. Furthermore, considering the complexity of the IoT, this body could be construed in a way to dispose of the necessary capacities. The alternative to the creation of a new body is to integrate the task of international legislator for the IoT in an existing organization. Bearing in mind the globality of the IoT, this organization has to have a certain scope of territorial application. Furthermore, the organization should have a structure that allows for the inclusion of a body only responsible for the IoT. Finally, legislation and governing of the IoT should be encompassed by the overhead responsibilities of the organization to be appointed. When considering these requirements, the World Trade Organization (WTO) and the Organization for Economic Co-Operation and Development (OECD) come to mind. A special Committee responsible for rule-setting and supervision in the IoT could be established as an answer to the question of an international legislator. This Committee would be made up of representatives of WTO or OECD member States, thereby assuring an international approach. The Committee could, after deliberations, issue formal agreements, standards and models, recommendations or guidelines on various issues of the IoT.

This evaluation coincides with the experiences made in the field of Internet governance in general. An internationally binding agreement covering privacy and data protection does not yet exist. Even if international human rights instruments usually embody the essence of privacy, at least to a certain extent, the protection cannot be considered as being sufficient; only ''extreme'' warranties are legally guaranteed, such as the respect for private life or the avoidance of exposure to arbitrary or unlawful interference.[53] Therefore, it is widely accepted that co-regulation is needed to secure the implementation of effective principles of privacy in the online world. Possible elements of a self-regulatory scheme may include codes of conduct containing rules for best practices worked out in accordance with substantive data protection principles, the establishment of internal control procedures (compliance rules), the setting-up of hotlines to handle complaints from the public, and transparent data protection policies.[54] Many international instruments, such as the Guidelines of the OECD and Art. 27 of the EC Directive on the Protection of Personal Data (1995),[55] mention self-regulation as an appropriate tool.[56]

Nevertheless, security and the protection of privacy is not a matter to be addressed exclusively by a legislator. Research and development in the field of information technology should also consider ethical consequences of new inventions.[57]

3.3. *Legal categories and scenarios*

Future legislation encompassing privacy and data protection issues of the IoT and RFID could have five different goals[58]:

[46] Weber, supra note 38, at 20, with further references.
[47] Schmid, supra note 26, at 199.
[48] Michael Froomkin, The Death of Privacy?, Stanford Law Review, Vol. 52, 2000, 1461–1543, at 1524 ss.
[49] Weber, supra note 38, at 12.
[50] Weber, supra note 38, at 15.
[51] Ian Brownlie, Principles of Public International Law, 7th edition Oxford/New York 2008, at 19.
[52] Weber, supra note 38, at 15.
[53] Weber, supra note 38, at 239.
[54] Weber, supra note 38, at 240.
[55] For an evaluation see Yves Poullet, The Directive 95/46/EC: Ten years after, Computer Law and Security Report, 2006, 206–217.
[56] For further detail see Rolf H. Weber, Regulatory Models for the Online World, Zurich 2002 at 165 ss.
[57] Langheinrich/Mattern, supra note 14, at 142.
[58] Schmid, supra note 26, at 207.

- Right-to-know-legislation;
- Prohibition-legislation;
- IT-security-legislation;
- Utilization-legislation;
- Task-force-legislation.

The different categories of future legislation should be evaluated in the light of the objectives of privacy and personal data protection depending upon the use of RFID which can concern the following aspects, namely[59]:

- Monitoring products (EPC),
- Monitoring animals (real-time authentication and monitoring of animals),
- Monitoring persons (real-time authentication and monitoring of persons),
- Collecting data for profiling purposes (aggregation).

In the context of the IoT, the EPC scenario concerning products is practically the most important application. Theoretically, EPC does not directly trace relational personal data, however, a person carrying an RFID-tagged item discloses to the organization using the RFID system certain data or gives at least the opportunity to collect information.

A specific legislative aspect concerns the term ''person''. The EU Directives as well as many national laws only consider individuals (''natural persons'') as objects of privacy laws. In particular, in the context of the IoT, this understanding is too narrow. Legal persons (e.g. corporations) do also have privacy interests; as for example in the Swiss legislation, the scope of application of data protection law needs to be extended to legal persons.[60]

(i) The right-to-know-legislation has the purpose to keep the customer informed about the applied RFID scenarios. In other words, the customer should know which data are collected and should also have the possibility to deactivate the tags after a purchase. In the United States, several attempts have been take to realize such kind of legislation.[61]

(ii) The prohibition-legislation introduces provisions which envisage to forbid or at least to restrict the use of RFID in certain scenarios.[62] Such an approach is traditional in state legislation if the public community dislikes a certain behavior; enforcement of prohibition is possible (at least in the books). Self-regulatory mechanisms rather tend to introduce incentives (if at all) instead of prohibition.

(iii) IT-security-legislation encompasses initiatives that demand the establishment of certain IT-security standards which should protect that application of RFID from unauthorized reading and rewriting.[63] Such kind of provisions can be introduced by the state legislator, but also by self-regulatory mechanisms; typically, industry standards are developed by the concerned market participants, having therefore the chance to be observed by the respective developers. Technologically, a new ''fourth generation'' framework of data protection protocols should be developed allowing the setting-up of stringent safeguards as to reporting and frequent audits of the measures.[64]

(iv) Utilization-legislation intends to support the use of RFID in certain scenarios.[65] Insofar, this approach stands contrary to the prohibition-legislation; it envisages making the RFID available in the relevant identification documents. Therefore, the legislative approach has to fine-tune an appropriate balance between prohibited and utilizable approaches.

(v) The task-force-legislation covers legal provisions supporting the technical community to invest into the research of the legal challenges of RFID[66]; the purpose of this approach consists in a better understanding of the relevant problems.

3.4. *Evaluation of the European legislative approach*

The Recommendation of May 12, 2009, of the European Commission is a framework approach to legislate in the field of Internet security. The Recommendation provides guidance to Member States which then have to enact specific rules. While the Recommendation makes reference to EU Data Protection Directives, it does not stipulate any specific provisions itself. The European Commission furthermore introduces a framework privacy and impact assessment, established by the industry and the relevant civil society stakeholders, and the publication of an information policy for applications should also be ensured by Member States.

EPCglobal and industry are currently establishing the requested framework (Private Impact Assessment, PIA). Even if its details are not known as of early November 2009, it can be said that the objectives of the PIA are designed to identify the implications on privacy and data protection, to determine whether the operator has taken appropriate technical and organizational measures to ensure respective protection, to document the implemented measures, and to serve as a basis for a PIA report to the competent authorities. Important aspects concern the RFID application description and scope, the RFID application governing practices, the accountability challenges, as well as analysis and resolution aspects. Finally, while the European Commission provides for this framework, Member States are strongly encouraged to support the Commission in identifying threats to information security.

The regulatory approach of the European Commission consists in vague framework guidelines which address many aspects without considering the merits of the self-regulatory models and industry standardization. The framework is formulated in an open way and thereby ensures that technical principles such as verticality, ubiquity and technicity can be

[59] Schmid, supra note 26, at 206.
[60] Art. 2 para. 1 of the Federal Act of 19 June 1992 on Data Protection, SR 235.1.
[61] Schmid, supra note 26, at 208, with further references.
[62] See also Schmid, supra note 26, at 208.
[63] Schmid, supra note 26, at 208.
[64] See Gehan Gunasekara, The ''Final'' Privacy Frontier? Regulating Trans-Border Data Flows, International Journal of Law and Information Technology, Vol. 17, 2009, 147–179.
[65] Schmid, supra note 26, at 209.
[66] Ibid.

taken into account. However, being established by the European Commission, it is only applicable for Member States in Europe and not globally. Moreover, the fact that it is up to Member States should establish more detailed regulation is even more prejudicial to the principle of globality.

Nevertheless, the recent Recommendation and Communication by the European Commission attest that privacy and data protection problems in the field of the Internet of Things are taken seriously and that there is a strong will to establish mechanisms to ensure that those do not become accurate once the Internet of Things operates large-scale.

4. Outlook

With the emergence of an Internet of Things, new regulatory approaches to ensure its privacy and security become necessary. In particular, attacks have to be intercepted, data authenticated, access controlled and the privacy of customers (natural and legal persons) guaranteed. The nature of the IoT asks for a heterogeneous and differentiated legal framework that adequately takes into account the globality, verticality, ubiquity and technicity of the IoT.

Geographically limited national legislation does not seem appropriate in this context. However, self-regulation as it has been applied up to now may not be sufficient to ensure effective privacy and security, either. Therefore, a framework of substantive key principles set by a legislator at the international level, complemented by the private sector with more detailed regulation seems to be the best solution. Through such a framework, general pillars of regulation could be set for everyone, which are then suitable to be supplemented by the individuals concerned in a way that suits their current needs. Furthermore, the inclusion of an international legislator in the process also ensures the continued involvement of the public sector, contributing at least by monitoring the process.

The approach chosen by the European Commission goes in that direction. However, it would be preferable to have an international (not European) legislator setting the framework; such an approach would better adapt to the needs stemming from the globality of the IoT. Furthermore, if a more detailed regulation should be established by the private sector, lessons can be drawn from Internet governance in general, where the private sector has already marked presence in the rule-setting.[67]

The content of the respective legislation has to cover the right to information, provisions prohibiting or restricting the use of mechanisms of the Internet of Things, rules on IT-security-legislation, provisions supporting the use of mechanisms of the Internet of Things and the establishment of a task force doing research on the legal challenges of the IoT.

While according mechanisms still need to be developed, the early recognition of eventual problems and suggestions for their encounter leaves hope that effective regulation can be established before the Internet of Things is in full operation.

Prof. Dr. Rolf H. Weber *(rolf.weber@rwi.uzh.ch) is professor at the University of Zurich and a visiting professor at the University of Hong Kong.*

Rolf H. Weber *studied at the University of Zurich and at the Harvard Law School. Since 1995 he is chair professor at the University of Zurich and since 2006 a visiting professor at the University of Hong Kong, teaching and publishing in civil, commercial and European law with special topics in Internet, media and competition law, international finance and trade regulation. He is director of the European Law Institute and the Center for Information and Communication Law at the University of Zurich; in addition he is member of the directory of the Postgraduate Studies in International Business Law and the MBA-Program at the University of Zurich. Since 2008 Prof. Dr. Rolf H. Weber is member of the Steering Committee of the Global Internet Governance Academic Network (GigaNet) and since 2009 he is member of the High-level Panel of Advisers of the Global Alliance for Information and Communication Technologies and Development (GAID). Besides, he is engaged as an attorney-at-law and as a member of the editorial board of several Swiss and international legal periodicals.* *A first version of this contribution has been published in Sylvia M. Kierkegaard (ed.), Legal Discourse in Cyberlaw and Trade, 2009, 1–14. The author expresses his gratitude to lic. iur. Romana Weber for her valuable research support.*

[67] Weber, supra note 38, at 17 ss.