available at www.sciencedirect.com
ScienceDirect
www.compseconline.com/publications/prodclaw.htm
Computer Law & Security Review

Internet of things – Need for a new legal environment?

Rolf H. Weber [a,b]

[a] *University of Zurich, Switzerland*
[b] *University of Hong Kong, China*

Keywords:
Internet of Things (IoT)
ONS and DNS
European Regulatory IoT-Initiatives
Root System
Self-Regulation
Governance Principles for the IoT

ABSTRACT

The Internet of Things as an emerging global, Internet-based information service architecture facilitating the exchange of goods in global supply chain networks is developing on the technical basis of the present Domain Name System; drivers are private actors. Learning from the experiences with the ''traditional'' Internet governance it is important to tackle the relevant issues of a regulatory framework from the beginning; in particular, the implementation of an independently managed decentralized multiple-root system and the establishment of basic governance principles (such as transparency and accountability, legitimacy of institutional bodies, inclusion of civil society) are to be envisaged.

1. Notion and concept of the internet of things

In the ongoing process of Internet growth a new development is on its way, namely the evolution from a network of interconnected computers to a network of interconnected objects (Internet of Things, IoT)[1].

1.1. *Notion of IoT*

The term IoT, first used by Kevin Ashton in a presentation in 1998[2], describes an emerging global, Internet-based information service architecture. Technically, the architecture is based on data communication tools, primarily RFID-tagged items (Radio Frequency Identification).[3] The purpose of the IoT consists in the facilitation of information exchanges about, among other things, goods in global supply chain networks, i.e. the IT-infrastructure should provide information about ''things'' in a secure and reliable manner.[4] Extending the initial application scope, the IoT might also serve as backbone for ubiquitous computing, enabling smart environments to recognize and identify objects, and retrieve information from the Internet to facilitate their adaptive functionality.[5]

1.2. *Technical background of IoT*

The most popular industry proposal for the new IT-infrastructure of the IoT is based on an Electronic Product Code (EPC). In the respective network, established by EPCglobal and GS1,[6] the ''things'' are physical objects carrying RFID tags with a unique EPC; the infrastructure can offer and query EPC

[1] I would like to thank my research assistant Ulrike I. Heinrich for her valuable support in the preparation of this article.
[2] 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.
[3] 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.
[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 in general Benjamin Fabian, Secure Name Services for the Internet of Things, Thesis, Berlin 2008, at p.1.
[6] See http://www.epcglobalinc.org.

0267-3649/$ – see front matter
doi:10.1016/j.clsr.2009.09.002

Information Services (EPCIS) both locally and remotely to subscribers.[7] Instead of saving all information on a RFID tag, however, a supply of the information by distributed servers on the Internet is achievable through linking and cross-linking with the help of an Object Naming Service (ONS).[8]

The ONS does not contain actual data about the EPC, but it can return a list of network accessible service endpoints that pertain to the EPC in question.[9] 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.[10] The central ONS root is operated by the (private) company VeriSign, a provider of Internet infrastructure services.

1.3. *ONS and DNS heritage*

The ONS is based on the well-known Domain Name System (DNS), i.e. the DNS-based ONS as hierarchical tree-like architecture[11] locates the information sources relevant for a given object. 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.[12] Since the main design idea is to first encode the EPC into a syntactically correct domain name and then to use the existing DNS infrastructure to query for additional information, it can be said that the ONS is a subset of the DNS.[13]

The ONS and the DNS have the following similarities:

- *Structure:* Based on the distributed DNS-tree both the ONS and the DNS are grounded on the same database structure.
- *Service architecture:* Both the ONS and DNS use the architectural client-server model and the same Internet communication protocols.

The following differences are given between the ONS and the DNS:

- *Standardisation processes and bodies:* The ONS uses the standards development process by EPCglobal, a user driven standards process for the development of technical standards whereas DNS applies the RFC (Requests for Comments) series, a standardisation process published by the Internet Engineering Task Force (IETF).
- *Naming schemes:* The domain names in the DNS usually consist of two or more alphanumeric parts (labels) with only a few technical limits, e.g. each label can contain up to 63 octets, but the whole domain name may not exceed 255 octets. The ONS uses the Tag Data Standard, a deterministic choice based on the EPC structure.[14]
- *Use models:* The DNS is based on an extensible and multipurpose Internet-based public infrastructure; the ONS uses a private infrastructure that is specific to RFID-related business activities/partners.

Since ONS is based on DNS use,[15] it will also inherit all of the well-documented DNS weaknesses. For example, DNS suffers from limited redundancy in practical implementations.[16] Furthermore, the small number of servers for a given zone information and their limited redundancy create single points (or small areas) of failure. In addition, root and top-level domain (TLD) servers might suffer from strong load imbalance induced by the architecture. In a nutshell, the DNS weaknesses in robustness, configuration complexity and security need to be overcome if the IoT should become a reliable system.

Apart from the technical issues, governance aspects remain crucial. Criticism has been levied against ICANN as governing body of the (traditional) Internet, for example in respect of the "thin" legitimacy and the lack of sufficient transparency and accountability.[17] The same question arises in the IoT environment; who should reasonably control and operate the root and TLD servers?

Since the IoT is not only a mere extension of today's Internet, but rather a complex netting of independent but interoperable systems, implemented in a symbiosis with new services and different modes of communication, the traditional Internet Governance concepts are not anymore suitable to identically be applied, but the development of decentralized architectures and the promotion of a shared network of multistakeholderism governance for the IoT is needed.

2. EU-activities

The need to tackle regulatory issues of the IoT governance has been recognized by the EU Commission already in 2006, particularly at the occasion of a workshop entitled "From RFID to the Internet of Things[18]. Comparatively, the EU efforts in studying the regulatory needs for the IoT are further advanced than the efforts of any other institutional body.

2.1. *Staff paper and replies*

(i) As its further contribution to the increasing public debate and for reaching mutual understanding about the IoT and its relationship towards the future Internet the EU

[7] Fabian, supra note 5, at p. 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, at p. 288, 296 ss.
[8] Fabian, supra note 5, at p. 33.
[9] EPCglobal, Object Naming Service (ONS) Version 1.0.1, para 4.2, available at: http://www.epcglobalinc.org/standards/ons/ons_1_0_1-standard-20080529.pdf.
[10] EPCglobal, Object Naming Service (ONS) Version 1.0.1, supra note 9, at para 4.2.
[11] Fabian, supra note 5, at p. 33.
[12] EPCglobal, Object Naming Service (ONS) Version 1.0.1, supra note 9, at para 5.2.
[13] Fabian, supra note 5, at p. 36 refers to a "secondary dependence".
[14] Fabian, supra note 5, at p. 37.
[15] To the DNS in general see Rolf H. Weber, Looking ahead: more harmonization in the domain name system? International Journal for Intercultural Information Management 2007, at p. 74 ss.
[16] See also Fabian, supra note 5, at p. 50.
[17] To the respective discussion extensively Rolf H. Weber, Shaping Internet Governance: Regulatory Challenges, Zurich 2009, at p. 105 ss.
[18] See ftp://ftp.cordis.europa.eu/pub/ist/docs/ka4/au_conf670306_buckley_en.pdf (final report).