Available online at www.sciencedirect.com

SciVerse ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

# Internet of things – Governance quo vadis?

*Rolf H. Weber*

*University of Zurich, Zurich, Switzerland*

*Keywords:*
Competition law
EU policy
International regulators
Particularities of IoT
Regulatory approaches
Substantive governance principles

ABSTRACT

The Internet of Things (IoT) as an emerging global Internet-based information architecture facilitating the exchange of goods and services is gradually developing. While the technical aspects are being discussed in detail a legal framework does not exist so far. The first supranational organization trying to work out an IoT governance framework has been the European Commission by appointing a large group of experts to examine the relevant aspects of a possible IoT governance regime. In the meantime, however, the activities have been degraded. Nevertheless, even if the differences between the IoT and the Internet have been overestimated at the beginning, many elements of the IoT differ in part from the corresponding problems in the Internet. Therefore, an analysis of the major IoT governance issues (legitimacy, transparency, accountability, anticompetitive behavior) seems to be worthwhile to conduct.



## 1. Introduction

For the time being, an authoritative definition of the Internet of Things (IoT) does not exist, notwithstanding the fact that several efforts have been taken to define the IoT. A commonly acknowledged definition stems from the ITU (2005), arguing that the development of item identifications, sensor technologies and the ability to interact with the environment will create an IoT.[1] In the IoT physical objects are seamlessly integrated into the information network and the physical objects can become active participants in business processes (in the form of interaction with "smart objects" over the Internet); 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.[2]

The development of a new information infrastructure raises the question of its "governance", understood as the design of institutions and the structure of authority to allocate resources and coordinate or control activities in the society. According to a definition of the World Bank governance "includes (i) the process by which those in authority are selected, monitored and replaced, (ii) the capacity of the governing body to effectively manage its resources and implement sound policies, and (iii) the respect of citizens and the state for the institutions that govern economic and social interactions among them".[3] In the context of Internet governance, the Working Group on Internet Governance has referred to the "development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet".[4]

Several elements of the governance of the Internet are highly disputed; amongst others, the central role played by ICANN in the domain name allocation regime has caused concerns in the eyes of many countries.[5] With the IoT in its

[1] http://tinvurl.com/v614sor; see also European Commission (ed. by H. Sundmaeker/P. Guillemin/P. Friess/S. Woelfflé), Vision and Challenges for Realising the Internet of Things, Brussels, March 2010, p. 43; G. Lee, The Internet of Things – Concept and Problem Statement, IRTF, available at http://tools.ietf.org/html/draft-lee-iot-problem-statement-00.

[2] R. H. Weber/R. Weber, Internet of Things – Legal Perspectives, Zürich/Berlin 2010, p. 1 with further references.

[3] http://geo.worldbank.org/MKOGR258V0.

[4] Report of the Working Group on Internet Governance, June 2005, p. 4, available at http://www.wgig.org/docs/WGIGREPORT.pdf.

[5] A detailed description of these concerns would be outside of the scope of this article; for an overview see R.H. Weber, Shaping Internet Governance: Regulatory Challenges, Zurich 2009, pp. 106–148.

0267-3649/$ – see front matter 
http://dx.doi.org/10.1016/j.clsr.2013.05.010

infancy, similar questions about governance have taken place in the political debates.

The European Commission has been the first supranational body trying to work out an IoT governance framework. Apart from some internal efforts, a large expert group was appointed and asked to study the relevant aspects of a possible IoT governance regime. Since the European Commission recently changed its focus and degraded the importance of the IoT project, an analysis of the given situation seems to be worthwhile to conduct.

## 2. IoT issues – EU perspectives

The group of experts on the Internet of Things has analyzed in sub-groups several issues of importance in connection with the IoT, namely architecture, identification, privacy and security, standards, governance as well as ethics. Based on the respective analyses, the European Commission initiated a public consultation between April and July 2012. About 600 persons, associations and various groups from academics, industry and civil society responded to the consultation. The objective of the questionnaire was to identify those areas where public intervention would be required to allow the relevant benefits to materialize while maintaining sufficient control and protection of consumers and society at large. The results of the public consultation can be summarized as follows.[6]

### 2.1. *Privacy and data protection*

The public consultation has shown diverging results regarding privacy issues. The industry has been of the opinion that the current data protection framework would be sufficient, whereas a large majority of interested citizens and consumer organizations have claimed that a greater focus on privacy and data protection in the context of the IoT would be needed. However, the new instrument of the data protection impact assessment (PIA) is largely welcome.[7]

Special emphasis should be put on user consent as well as on the right of the users to delete data. Furthermore, since the possibility to build extensive personal profiles can be hardly avoided, data anonymization is important in case of data sharing.[8] In addition, the transparency about data collections and the accountability of data collectors need to be improved.

### 2.2. *Security and safety*

The majority of the responses to the public consultation expressed the opinion that guidelines and standards need to be created to ensure data confidentiality, integrity, and availability in the IoT context. However, the industry has warned that the regulator should be careful not to over-regulate the technical environment and to create unnecessary regulatory burdens, whereas civil society representatives consider safety and security of being more important than economic liberty.[9]

Cooperation is seen as a possible instrument to ensure security on an end-to-end basis; furthermore, voices are raised in favor of a continued and sound breach notification policy.[10]

In respect of the security of critical IoT supported infrastructures in particular, generally more stringent and mandatory information security measures are welcomed. However, some of those consulted also warned against rules becoming too prescriptive with the potential consequence that the emergence of a better architecture could be inhibited.[11] Again, cooperation between industrial players, public sectors and governmental institutions is considered to be a sensible tool to rightly address security issues and to improve safety of services.

### 2.3. *Ethics*

The issue of ethics has been addressed by the IoT expert group at a comparatively late stage. In the public consultation, responses supported the inclusion of ethical elements into the IoT debate, in particular elements such as personal identity, autonomy of individuals, user consent, fairness and social justice.[12] Obviously the difficulty consists in the search of finding an agreement regarding the level of ethical standards that might be different according to industrial and societal environments.

A special part of the questionnaire looked at procedural issues in ethics, opening the debate of what measures would have to be adopted in order to properly take into account the ethical aspects in the design and development of the IoT. Civil society representatives have been skeptical in assuming that an ethical charter or another form of self-regulation would be sufficient to cover the needs in ethics since respect by IoT providers could not be enforced. Therefore, many respondents have called for regulatory oversight and governance.[13]

### 2.4. *Object identifiers and interoperability*

The result of the consultation in this respect has been quite coherent: most voices see interoperability as an important policy object pointing to open IoT platforms that promote competition and service innovation. The critical questions concern the legitimacy of closed platforms in vertically integrated systems which are justified by their proponents as schemes allowing competition between different models (open/close) being an approach which would become more suitable and successful in an application area.[14]

In view of the global character of the IoT the development of global identification schemes in the form of unique identifiers is important. Nevertheless, many respondents have expressed the opinion that a single global numbering scheme would be unrealistic since already a number of organizations do have their own object identification scheme to identify objects.[15] In

[6] European Commission, Report on the Consultation on IoT Governance, Jan. 16, 2013, available at https://ec.europa.eu/digital-agenda/en/news/conclusions-internet-things-public-consultation.
[7] Report, supra note 6, p. 3.
[8] Report, supra note 6, p. 4.
[9] Report, supra note 6, p. 5.
[10] Report, supra note 6, p. 6.
[11] Report, supra note 6, pp. 6/7.
[12] Report, supra note 6, p. 8.
[13] Report, supra note 6, p. 9.
[14] Report, supra note 6, p.10.
[15] Report, supra note 6, p. 10.

this connection the privacy issues occurring in relation to IoT identification schemes are to be taken into account.

### 2.5. *IoT governance*

The European Commission has put much emphasis on governance issues in the IoT from the beginning. In fact, the wish to establish a new regime not fully dependent upon ICANN has been a main driver of the EU efforts.[16] This approach has been questioned by US and Pacific scholars for many years. The differing views are now also reflected in the report about the results of the public consultation.[17] Partly it is argued that special IoT governance is not needed since the existing Internet governance schemes could be used; IoT technologies should be integrated and made compliant with the existing applicable rules avoiding the development of separate legislation or the replication of already existing rules. Furthermore, some voices argued that there would be no need for an authority deciding or approving the different applications or the infrastructure of devices.[18]

In part, a framework for IoT governance was supported, particularly from civil society and consumer organizations. A new body realizing a multi-stakeholder approach should address important issues such as privacy, interoperability and ethical issues. However, the views were divided on the level of prescriptiveness of IoT governance, in particular no common understanding respectively as to the controversy of the hard law vs. the soft law approach.[19]

### 2.6. *Standards for meeting policy objectives*

The questionnaire of the European Commission also looked at the need to develop standards that would support IoT policy objectives and the best way to develop them. The result of the public consultation does not show a clear direction: Different areas for standardization were put forward, encompassing the issues of privacy, security, interoperability (addressing, protocols, formats) and openness of platforms. In particular, industry representatives seem to be reluctant to identify a need for new standards to achieve specific policy objectives, whereas consumer organizations rather tend to support alternative ways for public authorities to steer the standardization processes by empowering authorities to act as facilitator and moderator in the field of IoT.[20]

## 3. Possible issues for IoT governance

After the above described survey was completed, the European Commission has basically withdrawn from exercising active efforts related to the regulatory framework of the IoT. The main attention has been moved to issues of security and trust in the Internet. Notwithstanding this change in the political agenda, the question must be asked whether in fact the need for regulatory action regarding IoT markets is (any longer) required. Thereby it must be kept in mind that the IoT does not only concern objects, but also the relations between the everyday objects surrounding humans and humans themselves.[21] Consequently, the IoT encompasses many factors of the society. Tools for governance must embrace the requirements in respect of cooperation, policy, coordination, standards and laws including rules extending to grass-roots national and city governance, as well as relating to structural matters.[22] Based on this assumption, possible issues for IoT governance as well as the legal environment of IoT governance must be discussed.

### 3.1. *Particularities of the IoT compared to the Internet*

The Internet is designed according to the well-known domain name system (DNS) of ICANN.[23] The IoT is based on the object naming service (ONS) being a service containing the network addresses of services; each service available on the ONS embraces data about the electronic product code (EPC).[24] Instead of saving all the information on a radio-frequency identification (RFID) tag, a supply of the information by distributed service on the Internet is achievable through linking and cross-linking with the help of the ONS.[25]

The first ONS was introduced by the (private) company VeriSign, the first European ONS was established by France in 2009. The ONS is authoritative (linking meta-data 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.[26]

The following differences can be identified between the ONS and the DNS[27]:

- *Standardization 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 standardization process developed and 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.[28]
- *Use models*: The DNS is based in an extensible and multi-purpose Internet-based public infrastructure; the ONS uses a private infrastructure that is specific to RFID-related business activities/partners.

[16] For further details see below subchapter 3.1.
[17] Report, supra note 6, p. 11.
[18] Report, supra note 6, p. 12.
[19] Report, supra note 6, p. 13.
[20] Report, supra note 6, pp. 13–14.
[21] G. Santucci, The Internet of Things: The way ahead.
[22] See A. Furness, Foundations for IoT Governance, in I. G. Smith/O. Vermesan/P. Friess/A. Furness (eds.), The Internet of Things. 2012. New Horizons, Halifax 2012, p. 239.
[23] For further details see Weber, supra note 5, pp. 28, 51–54.
[24] Weber/Weber, supra note 2, pp. 5–6.
[25] B. Fabian, Secure Name Services for the Internet of Things, Thesis, Berlin 2008, p. 33.
[26] Weber/Weber, supra note 2, p. 6.
[27] Weber/Weber, supra note 2, p. 8.
[28] Fabian, supra note 25, p. 37.

As a consequence, it can be said that Internet governance is focusing on addresses and registries, whereas IoT governance rather looks at identifiers. The origins of the identifying mechanisms are different from the Internet in general as some identifiers have resolving mechanisms, others not. Some rely on the actual Internet to operate, others not. Some have a covered geographic scope and/or a covered application sector, some are standardized at the international level, others not, and the assignment/management varies substantially.

### 3.2. *IoT-specific issues requiring a regulatory framework*

In view of the mentioned relevance of the IoT technical structure, a good number of issues need to be addressed in order to implement an appropriate regulatory framework for the IoT markets. As mentioned, the key issues have been subject of the survey done by the European Commission in 2012.[29] Summarizing the debates and without differentiating between structural and operational approaches[30] the following topics merit special attention.

#### 3.2.1. *Privacy and security*

IoT privacy, data protection, and data security have been identified as key issues of a regulatory framework; IoT business has to comply with human integrity, human identity, and privacy allocating control of personal data generated or processed within the IoT to the concerned individuals.[31] Therefore, adequate organizational data security risk management as well as privacy by design and privacy by default rules should tackle the risks in a context-aware and situational manner, avoiding unlawful processing, traceability and profiling of persons and leading to a design of data protection friendly technologies.[32] In this context, identification issues are at stake, embracing object identifiers, network addresses as well as resolution and discovery functions.

#### 3.2.2. *Standardization and IoT architecture*

The execution of efficient IoT business requires the availability of harmonized standards, at least on a regional level, preferably on a global level. Many organizations, particularly in Europe, are in the process of joining forces in order to realize the required harmonization of the standards.[33] Since the IoT is encompassing a wide range of technologies, a single reference architecture is not suitable as a blueprint for all possible concrete implementations. Therefore, several reference architectures might co-exist in the IoT, which makes it necessary to specify the physical components and the functional organization in the configuration of networks, their operational principles and procedures, as well as data formats used in the operation.[34] In this context, spectrum management and interoperability as well as identification need to be addressed.[35]

#### 3.2.3. *Ethical features*

During the last few years, ethics in the context of the IoT have become an important discussion topic. The expert group of the European Commission has identified six key ethical issues, namely social justice, trust (exceeding the traditional notions of reliance and confidence), the blurring of contexts (private vs. public), the non-neutrality of IoT metaphors, agency (social contract concept), and autonomy (informed consent vs. obfuscation of functionality).[36] Social justice includes problems of digital divide caused by the lack of access to the technological infrastructure.[37] Furthermore, corporate social responsibility in IoT enterprises has become an important element of an ethical framework.[38]

## 4. Relevant pillars of IoT governance

### 4.1. *Establishment of an international regulator?*

Generally it is acknowledged that a basic legal framework for IoT applications and services would be desirable. However, the most recent research activities and industry studies seem to point to the conclusion that it would be too premature to define a concrete policy development process which would establish a strict legal framework of principles. Possible organizational structures have been presented in legal doctrine, such as (i) the establishment of a completely new organization or (ii) the creation of a new committee of the World Trade Organization (WTO) or (iii) of a new committee of the OECD.[39]

However, specific proposals to establish a particular IoT governance mechanism on the global or on the regional level by creating an intergovernmental IoT Treaty Organization under the auspices of the United Nations[40] do not seem to be realizable in the near future. Nevertheless, from this assessment it is not possible either to draw the conclusion that the existing Internet governance eco-system is currently sufficient for the IoT needs. Emphasis must be put on the question of identifying the particular requirements of the IoT governance environment.

[29] For details see above chapter 2.
[30] See Furness, supra note 22, p. 242.
[31] Weber/Weber, supra note 2, p. 41; see also European Commission, Internet of Things, Factsheet Privacy and Security, available at https://ec.europa.eu/digital-agenda/en/news/conclusions-internet-things-public-consultation.
[32] For a general overview on Privacy Enhancing Technologies (PET) see Weber/Weber, supra note 2, p. 47–51.
[33] K. Mainwaring/ L. Srivastava, The Internet of Things – Setting the Standards, in: H. Chaouchi (ed.), The Internet of Things, Connecting objects to the Web, London/ Hoboken 2010, pp. 191 et seq.
[34] European Commission, Internet of Things, Factsheet Architecture, p. 1, available at https://ec.europa.eu/digital-agenda/en/news/conclusions-internet-things-public-consultation.
[35] Factsheet Architecture, supra note 34, p. 11, 15.
[36] European Commission, Internet of Things, Factsheet Ethics, available at https://ec.europa.eu/digital-agenda/en/news/conclusions-internet-things-public-consultation, pp. 6, 18.
[37] R. H. Weber/V. Menoud, The Information Society and the Digital Divide, Legal Strategies to Finance Global Access, Zurich 2008.
[38] See R. H. Weber, Corporate social responsibility as new challenge for the IT industry, [2012] 28 Computer Law & Security Review, pp. 634–640.
[39] For further details see R. H. Weber, Governance of the Internet of Things, in: H. Chaouchi (ed.), The Internet of Things, Connecting Objects to the Web, London/ Hoboken 2010, pp. 223, 230–233.
[40] Furness, supra note 22, pp. 227 and 238 seem to go into this direction.

### 4.2. *IoT governance and regulatory approaches*

Governance plays an important role in the implementation of international network structures. Experiences from the regulation of the Internet suggest that the concept of "multi-stakeholder governance" should be perceived as the new way forward in favor of the inclusion of the whole society. Being still in its infancy, the development of the IoT, particularly regarding its future reach, is hardly predictable. Nevertheless, debates regarding the structure, the root system, the institutional issues and the governance principles are desirable.[41] Rule-making processes can be based on different legal mechanisms, such as international legal instruments, binding national laws, soft law recommendations of international organizations, co-regulation (being a mechanism which is based on objectives laid down in an legislative act but implemented by private parties) or self-regulation (being based on rules adopted by industry organizations).[42] Due to the complexity of the governance mechanisms in the IoT, it seems to be obvious that a combination of several mechanisms as described, need to be taken into account in a multilevel approach.

Looking from a broader perspective, two main approaches are possible: (i) A top–down/centralized approach would mean that a single body is established and is coordinating all the actors; (ii) a bottom–up approach does not start from a coordinated single point but does try to implement horizontal exchanges between actors. Both approaches, however, do not seem to be suitable since an extreme mechanism is not likely to work out. Moreover, a variable-geometry approach may be preferred, combining various top–down and bottom–up actions, depending on the technical environment and the given societal situation.

Such kind of variable-geometry approach could be based on enhanced cooperation, allowing market participants and consumers to apply different speeds and/or move toward different calls in certain areas on the bases of a general understanding of the market structures.[43] Another possibility consists in an open mechanism of coordination, based on an appropriate identification of the objectives to be achieved and an adequate implementation of measuring instruments (for example benchmarking of the performances of the market actors). A further approach could call for a multi-stakeholder regime as applied in the Internet.

### 4.3. *Substantive principles of IoT governance*

A couple of substantive principles are to be realized in an adequate IoT governance framework; the most important pillars are given below.[44]

#### 4.3.1. *Legitimacy and representation*

The IoT business is sensitive to the whole society. An appropriate political understanding of legitimacy makes it necessary to establish procedures that implement equal bargaining, powers and fair proceedings allowing for representation of all stakeholders. An IoT being within a specific public or private authority's power would lack legitimacy and not comply with the principle of democratic participation having a legitimizing effect, since the outcome should reflect the values of the stakeholders represented.

Therefore, the system should be designed in a way that the rules are fair and firmly rooted in a framework of formal requirements about how rules are made and are correspondingly interpreted and applied.[45] The stakeholders' enhanced communication, coordination and cooperation in a kind of forum, frame a central institutional point for the regulation of IoT issues. The concept should also enhance transparency and review mechanisms that enable the allocation of accountability. Therefore, the future IoT needs to have a multipolar and decentralized policy institutional setting, considering the requirements of all stakeholders involved.[46]

#### 4.3.2. *Transparency*

It is not only the Internet in general, but IoT transparency too that is a key governance issue. Transparent mechanisms are central for external and internal structures of markets and organizations. Usually, compliance with the following five elements is of importance[47]: (i) availability of an organization or an institution with sufficient power to influence the management of the resources in the society; (ii) existence of publicly reliable information, i.e. substantive quality standards related to information, allowing influence effects based on people's choices; (iii) definition of the recipient as an essential component for the perception of both information and transparency; (iv) availability of sufficient information including establishment of reporting requirements, rights of access to information and disclosure procedures; (v) observance of the time element (visibility of information).

Stakeholders have to be in a position to follow all important actions in the IoT governance. Insofar, transparency can also be seen as element of ethics[48]; therefore, transparency must be established for the elaboration of rules, for the decision-making processes as well as for procedures. In the IoT, mechanisms ensuring transparency that allow adaptation to technological change are of particular importance. Transparency mechanisms should stay usable in the evolving system in order to ensure that information channels as well as participation regimes remain accessible for IoT businesses, which will increasingly rely on an operable framework for their operations. Furthermore, a certain consistency of the respective methods is also desirable with regards to convenience for individual users.[49]

#### 4.3.3. *Accountability*

As discussed,[50] the possibility of holding governing bodies accountable for their mistakes generally improves their regimes due to the threat of sanctions. The IoT, which needs to cope with the particularities in various segments of society,

[41] Weber/Weber, supra note 2, p. 69.
[42] Weber/Weber, supra note 2, pp. 23–26.
[43] See also Furness, supra note 22, p. 240.
[44] This sub-chapter closely follows Weber, supra note 39, pp. 233–244.
[45] For further details see Weber, supra note 5, pp. 105–120.
[46] See also B. Benhamou, A European Governance Perspective on the Object Naming Service, 2007, ftp://ftp.cordis.europa.eu/pub/fpt/ict/docs/chI-Lisbon-20071215_en.pdf.
[47] Weber, supra note 39, p. 234.
[48] See above subchapter 2.3.
[49] See Weber, supra note 39, p. 236.
[50] R. H. Weber. Accountability of the Internet of Things, [2011] 27 Computer Law & Security Review, pp. 133–138.

has to follow up on a multi-stakeholder approach to accountability being framed alongside the following three elements[51]: (i) standards need to be introduced that hold governing bodies accountable, at least on the organizational level; (ii) information should be made more readily available to accountability holders, enabling them to apply the standards in question to the performance of those who are held to account; (iii) accountability holders must also be able to impose some sort of sanction, thus, attaching costs to the failure to meet the standards. Such "sanctioning" is only possible if adequate participation schemes are devised through direct voting channels and indirect representation schemes.

The establishment of a code including the fundamental values that lay the foundation of accountability could provide for a viable way forward. However, such kind of private initiatives need to be complemented by functional surveillance. Businesses are often subject to regular (independent) reviews, for example in the financial market sectors; lessons could be drawn from the respective experiences.[52] The idea behind such an approach is that external monitors are considered more independent than internal monitors and are therefore more likely able to criticize the governing body or mechanisms within the framework.[53]

#### 4.3.4. *IoT infrastructure governance*

*Robustness* of the system is an important element for IoT business; the system must be capable of dealing with changes in its operation without suffering from major damage or loss of functionality and should be capable of absorbing attacks without failing. The IoT, as a system with a multitude of technological devices attached, is exposed to failure; therefore, robustness as a requirement of the framework has to be considered carefully.[54] In particular, in the IoT with sensors in place, devices should have some knowledge about their own functionality and be able to "call for help" in case of failure. The provision of a robust system for the IoT is primarily a task for technicians and engineers. Thereby, it is important not to overload the functionality in objects. An ideal approach would be to generate various models, which are then to be tested for their robustness through the inducement of failures.

*Availability* is another important factor of the IoT infrastructure governance system; availability refers to the proportion of time that it is able to be used and the time it takes the system to recover from a failure. Availability is particularly significant for the IoT since businesses are involved; risks from a lack of availability include a cutback in functionality, a production stop or sabotage for producers.[55] In general, availability of the IoT is increased if it is decentralized; if the framework is based on only one root, the system can suffer from a "single point of failure". The requirement of availability includes the system's capability to accommodate a large number of subscribers; users need to be able to receive information from the IoT without delays. Therefore, the IoT system has to be construed in a way that ensures the capability of future expansion.

A third infrastructural issue is the *reliability* of the IoT system, being the ability of users thereof to gain confidence in it, i.e. to trust that the system continuously performs and functions in normal as well as in hostile or unexpected circumstances. Technically, reliability is the probability of a product performing without failure, a specified function under given conditions for a specified period of time.[56] Reliability should be maximized through specific measures before the IoT becomes operable. Reliability can be improved by anticipating the sources of failure or reused performance of the system, i.e. the disconnection of the network or degraded performance.

As already mentioned[57], the IoT requires various forms of *interoperability* and connectivity. In particular, connectivity has to be established between computers and networks, between users of different computers and networks, between people and things and among things. Apart from the need to have standardization to a certain extent, backward compatibility is also indispensable in a technology such as the IoT. As technologies are constantly evolving and improving, individual parts of the system have to be adaptable to new technologies without being replaced.[58]

Finally, a *right of access* to the IoT infrastructure must be granted. An equitable and non-discriminatory use of the IoT by all interested businesses should be achieved. Access to infrastructure encompasses open access to the system, open standards, open-source software and wide-spread availability of access points. An important topic in this context is the affordability of access and its communication possibilities, being an element of ethics and of avoidance of digital divide in the IoT environment.[59]

### 4.4. *IoT governance through competition law*

Another legal issue gaining importance in IoT markets is competition law. Looking at the economic development, IoT markets tend to cause market dominance situations. Having a monopoly does not infringe antitrust law in itself, but an enterprise in a dominant position has a "special responsibility not to allow its conduct to impair undistorted competition".[60] Therefore, it is illegal to seek or maintain a market dominant position through anticompetitive methods.

A potential risk for IoT markets consists in an exclusionary conduct of any of the few IoT market participants having a market dominant position. The main problem concerns the

[51] See Weber, supra note 39, p. 236; A. Buchanan/R.O. Keohane, The legitimacy of global governance institutions, Ethics and International Affairs 20 (2006), pp. 405–437.

[52] See also Weber, supra note 39, p. 238.

[53] If properly designed, a private institution would also be suitable to assume such kind of surveillance and sanctioning function.

[54] Weber, supra note 39, p. 239; D. Kennedy, Five basic rules for the Internet of Things, EURESCOM mess@ge 2 (2009), http://archive.eurescom.eu/message/messageSep2009/Five-basic-rules-for-the-Internet-of-Things.asp.

[55] Weber, supra note 39, p. 240; see also Deutsches Bundesministerium für Wirtschaft und Technologie, Dokumentation No. 581, Internet der Dinge [German Federal Ministry of Economics and Technology, Document No. 581, Internet of Things], May 2009, http://www.bmwi.de/DE/Mediathek/publikationen,did=306778.html.

[56] See Weber, supra note 39, pp. 241/42.

[57] See above subchapter 3.2.

[58] Weber, supra note 39, p. 243; see also S. Haller/S. Karnouskos/Ch. Schroth, The Internet of Things in an Enterprise Context, in: J. Domingue/D. Fensel/P. Traverso (eds.), Future Internet – FIS 2008, Berlin 2009, pp. 14–28.

[59] Weber, supra note 39, p. 244.

[60] R. Wish/D. Bailey, Competition Law, 7th ed., Oxford University Press 2012, p. 3.

access to the infrastructure or to specific services due to the gatekeeper (bottleneck) function. Competition law knows the notion of the essential facility requiring a monopolist to grant access at reasonable conditions.[61] Another type of conduct raising problems in IoT markets is the tying of different products or services causing anticompetitive foreclosure effects on competitors.[62] Consequently, competition law merits particular attention in the coming years.

## 5. Outlook

The European Commission has intended to be frontrunner in the efforts of implementing an adequate governance framework for the new IoT technology. Probably, the differences between the IoT and the Internet have been overestimated at the beginning. Many problems of the IoT, such as data privacy, data security, standardization, architecture, etc. are slightly different from the corresponding problems in the Internet, but not different to an extent that a completely new governance regime would have to be immediately implemented. This assessment, however, should not lead to a hands-off approach[63] since many IoT governance issues such as legitimacy, representation, transparency, accountability and the building of an adequate IoT infrastructure merit substantive attention. Furthermore, the IoT has also become subject to power politics and its governance in a broader policy cyber realm context. In addition, special emphasis should be directed to potential anticompetitive distortions caused by dominant market players. Accordingly, continuing scholarly work is essential to identify the particular requirements of the Internet of Things and establish an appropriate IoT governance mechanism in the medium term.

**Prof. Dr. Rolf H. Weber** (*rolf.weber@rwi.uzh.ch*) *Professor of Civil, European and Commercial Law at the Law Faculty of the University of Zurich, Switzerland and Visiting Professor at the University of Hong Kong.*

[61] WISH/BAILEY, supra note 60, p. 703.

[62] A. FATUR, EU-Competition Law and the Information and Communication Technology Network Industries, Oxford/Portland 2012, p. 164.

[63] The impact assessment study launched by Rand Europe and presented at the end of April 2013 mainly covers economic, innovation and research policy guidance for the EU Commission, but does not treat IoT governance in particular.