Chapter 8

# Governance of the Internet of Things

## 8.1. Introduction

### 8.1.1. *Notion of governance*

The forthcoming advent of the Internet of Things (IoT) raises questions about "governance". For about 10 years, governance topics have been discussed and debated in relation to many market segments and different organizations/enterprises. It is therefore not surprising that the "governance wave" is also reaching scholarly discourses on the IoT.

"Governance" can be traced back to the Greek term "kybernetes", usually translated into English as "steersman", and the Latin word "gubernator" leading to the English notion of "governor". Consequently, governance addresses aspects of steering or governing behavior.

Different disciplines have addressed governance issues which, in a nutshell, can be summarized as the discussion on the appropriate allocation of duties and responsibilities. It includes the proper structuring of the "organs" concerned, thereby balancing performance-

---

Chapter written by Rolf H. WEBER.

*The Internet of Things: Connecting Objects to the Web* Edited by Hakima Chaouchi

based strategic management and financial/economic control [for a sociological point of view see LAN 04; a political science approach is given by BEN 04]. Or, in other words:

> "Governance, at whatever level of social organization it may take place, refers to conducting the public's business − to the constellation of authoritative rules, institutions and practices by means of which any collectivity manages its affairs." [RUG 04]

### 8.1.2. *Aspects of governance*

As far as organizations are concerned, light must be shed on the specific aspects of corporate governance. The main focus lies with the question of participation in corporate decision-making; insofar as "legitimacy" becomes a central theme. Among others, corporate governance is the subject of how and to what extent the interests of the various agents involved in an organization are reconciled.

To a certain extent, the corporate governance debate is the search for the status of an organization and the procedures of decision-making within such an organization. Substantively, the result can be seen as a politico-economic discussion of the owner control of organizations brought about by market conditions. Particular aspects concern:

– the rights of all stakeholders in an organization;

– the equitable treatment of the stakeholders;

– the role of the stakeholders in the decision-making processes of the organization;

– the disclosure and transparency requirements the board of directors/management must comply with; and

– the responsibilities of the board of directors/management.

Further details can be found in the Organization for Economic Co-Operation and Development, *OECD Principles of Corporate Governance*, www.oecd.org/dataoecd/32/18/31557724.pdf.

Being still in its infancy, the IoT's development, particularly regarding its future extent, is hardly predictable. Nevertheless, a preliminary assessment of the current environment of the Internet's structure, institutional issues and governance principles is desirable.

Further research may be needed to determine whether the IoT – being closely related to the Internet – should be governed separately from the Internet or as part of Internet governance. Given the difference in stakeholders between the two frameworks (global society *versus* mainly businesses) and the difference in purpose, separate governing bodies seem to be more suitable to take the specific needs of each framework into account. Nevertheless, close cooperation will be indispensable.

As a form of global governance with reference to an international framework, new attempts to introduce governance principles in the IoT must be seen in connection with the globalization of governmental relationships. For obvious reasons, such a framework should aim to provide a conceptual setting that describes the combination of rulemaking systems, political coordination and problem solving; the respective activities constitute a highly ambitious and complex undertaking.

## 8.2. Bodies subject to governing principles

### 8.2.1. *Overview*

Many organizations are directly or indirectly involved in the process structuring of the IoT. These organizations exercise different functions, thereby focusing particularly on technical, policy or administrative issues.

Different rules should apply to organizations with different tasks in the IoT. The organizational structures within the governing body at the highest level as well as its decisions, preferably including the deliberations and opposing arguments, have to be made public because of the impact of its work.

Organizations that are made up of individual members (such as EPCglobal, see section 8.2.2.1) must be transparent and accountable to their members. This requirement can be satisfied by distributing the necessary information to the listed stakeholders.

Furthermore, all organizations at a lower level have to inform the highest bodies of their activities in order to allow for coordination and cooperation at a lower level, which is indispensable if the IoT wants to present itself as a global information and exchange platform. However, these organizations – while providing the everyday user with the most important developments, do not have to publish all of their information on a globally accessible site. Only potential members need access to this information.

### 8.2.2. *Private organizations*

#### 8.2.2.1. *EPCglobal*

EPCglobal is a joint venture of GS1 US (formerly the Uniform Code Council) and GS1 (formerly EAN International) and is represented locally by GS1 members in over 100 countries across the globe. EPCglobal is a private organization leading the development of industry-driven standards for the electronic product code (EPC) to support the use of radio-frequency ID (RFID) in today's networks. The organization is subscriber-driven and includes industry leaders and organizations focused on creating global standards[1].

Action groups have been introduced to which participation is a benefit of subscription to EPCglobal. Up to now, over 40 active working groups have been established. All are available to join. The Industry and Technical Action Groups aim to develop the foundational building blocks of the EPCglobal network by creating global, cross-country standards for commercial adoption[2].

---

1 http://www.epcglobalinc.org/about, accessed February 23, 2010.

2 http://www.epcglobalinc.org/what/action_group/, accessed February 23, 2010. Other groups are the Joint Requirement Groups and the Cross Industry Adoption and Implementation Groups.

8.2.2.2. *VeriSign*

VeriSign is a private company providing Internet infrastructure services. In particular, VeriSign has been assigned the practical operation of the central object naming service root. VeriSign has operated this root directory for the EPCglobal network since 2005[3].

Furthermore, VeriSign is active in the continued development of RFID standards. In particular, the use of RFID in the public domain is observed in order to protect consumer privacy and confidentiality. It also provides security solutions to protect RFID information[4].

8.2.2.3. *ICANN*

The Internet Corporation for Assigned Names and Numbers (ICANN) [for further details see WEB 09c, p. 603-619] was created through a Memorandum of Understanding between the US Department of Commerce and ICANN in 1998[5]. It is a non-profit, public benefit organization with the legal status of a corporation, organized under the California non-profit public benefit corporation law for charitable and public purposes.

The organization is governed by Californian/US law and domiciled in Marina del Rey, State of California, where its principal office is situated. A further office in Brussels, presences in Africa, Latin America, Europe, and the Middle East, as well as the Pacific Rim, provide for its international outreach[6].

ICANN is responsible for vital tasks in the functioning of the Internet. In particular, it has to coordinate:

---

3 http://www.verisign.com/information-services/naming-services/emerging-name spaces/page_DEV044094.html, accessed March 23, 2010.

4 http://www.verisign.com/information-services/naming-services/emerging-name spaces/ page_DEV044094.html, accessed March 23, 2010.

5 The Memorandum of Understanding between the Department of Commerce and the Internet Corporation for Assigned Names and Numbers (ICANN) is available at: http://www.ntia.doc.gov/ntiahome/domainname/icann.htm, accessed February 23, 2010.

6 ICANN Fact Sheet, available at: http://www.icann.org/en/factsheets/, accessed February 23, 2010.

– the unique technical identifiers' allocation and assignment;

– the operation and evolution of the domain name system (DNS) root name server system; as well as

– the policy developments related to these technical functions[7].

Through its activities, ICANN aims to preserve the operational stability of the Internet. In particular, it aims to produce a bottom-up, consensus-based process for developing policies that include all relevant stakeholders[8].

Under the angle of (corporate) governance, the special relations between ICANN and the US have been subject to intensive discourses and discussions since its incorporation in 1998. The Memorandum of Understanding was followed by a Joint Project Agreement in 2006, which in turn was replaced by the joint "Affirmation of Commitments" (AoC), dated September 30, 2009[9]. ICANN and the US Department of Commerce signed the AoC in order to:

– ensure the outcomes of ICANN's decision-making were accountable, transparent, and in global Internet users' interests;

– preserve DNS's security and stability;

– promote competition, consumer trust and consumer choice in the DNS market place; and

– advance DNS's international participation.

The AoC highlights the importance of ICANN's decisions being in the public interest and not just in the interests of a particular set of stakeholders. In consequence of the AoC, ICANN will no longer be subject to unilateral oversight by the US, but will be reviewed constantly by independent panels. These panels consist of volunteer community members, the Chair of ICANN's Governmental Advisory

7 Article I, Section 1, ICANN bylaws.

8 ICANN Fact Sheet, available at: http://www.icann.org/en/factsheets/, accessed February 23, 2010.

9 http://www.icann.org/en/announcements/announcement-30sep09-en.htm, accessed February 23, 2010.

Committee, the Chair of the Board of ICANN, and representatives of the relevant ICANN Advisory Committees. Subsequently, the review's output will be published for public comment. With this new arrangement it is to be hoped that the involvement of more stakeholders in the applicable governance processes can be achieved.

As the Internet is an important element of the IoT, ICANN will also play an inevitable part in its governance. Lessons can be drawn from similar discourses on governance that took place with regard to the Internet. In particular, ICANN has gained sufficient power to issue publicly-reliable information, to define the recipient as an essential component for the perception of both information and transparency and to ensure this information is available as well as constantly visible [WEB 09a]. Furthermore, acknowledging the importance of accountability, ICANN has introduced an independent review of its accountability and transparency principles and the execution of management operating principles for the consultation of civil society, enabling its members to participate in responsive procedures [WEB 09a]. Similar mechanisms need to be introduced for bodies governing the IoT.

### 8.2.3. *International regulator and supervisor*

#### 8.2.3.1. *Conceptual background theories*

The IoT as a global framework needs to be governed by an organization operating across borders, including all relevant stakeholders from all geographic regions. Existing gaps between the governments of different states need to be closed through cooperation and coordination, "creating a new sort of power, authority, and legitimacy" [AND 05].

Such networks can be very powerful and permit international cooperation without states having to go through the formal processes of referring authority from national institutions to a supranational entity [MAY 03]. Furthermore, mechanisms should be established that allow for the speedy setting up of networks, whereas the negotiation of international treaties usually takes years [MAY 03]. The networks'

establishing regulation also has to foresee provisions for democratic elections, representation of all interested parties and mechanisms ensuring accountability [see AND 05, p.1301-1310; JAC 94, p. 14-15].

A variation of this approach would be to establish public-private partnerships, through which public policymakers delegate certain tasks to private participants and institutions providing specific knowledge and that are therefore in a better position to establish and implement the envisaged goals. This concept has been criticized for a lack of transparency as well as accountability [REI 97].

8.2.3.2. *Newly established organization*

A newly established organization specializing in IoT issues would permit coordination on a global level and create a new authority responsible and accountable for IoT governance. The IoT being an emerging framework itself, the introduction of a new governing body seems sensible. This organization would also be in the position to take due account of already existing international organizations, corporations, non-governmental organizations and other interested parties [SLA 04].

The creation of such a body presents challenging issues. In particular, an election mechanism needs to be developed that ensures equal participation of all regions, as well as of the different categories of participants. Representatives of governments and of the business sector as well as scholars with specific knowledge on particular subjects of the IoT have to be included in the governing body. Accordingly, mechanisms need to be established to elect these representatives based on democratic processes. Such a mechanism is of the utmost importance for legitimacy and accountability of the governing body.

Of a more practical nature is the objection that the election of such a body will take quite some time. The IoT is not yet fully functional and the establishment of a governing body may therefore not seem too urgent. Nevertheless, it is highly probable that such a body will not be functional in time, particularly taking into account that this body

should be operating before legal problems related to the IoT occur. For this reason, regulations would have to be established by the governing body ahead of extensive IoT use [WEB 10]. The consequence of this appreciation would be to include a body concerned with the IoT in an existing international organization[10].

8.2.3.3. *New committee of the World Trade Organization*

Following the General Agreement on Tariffs and Trade regime according to the Havana Charter of 1948, which has not introduced a distinct organizational structure, the World Trade Organization (WTO) was established in 1994 in order to deal with the rules of trade between nations at a global or near-global level[11]. The WTO provides extensive knowledge on international commerce and may therefore be appropriate to consider matters of the IoT, which is also subject of the exchange of goods and services at a global level. Furthermore, the WTO with 153 members includes a large part of the world's states, which is a requirement for the IoT as a global framework.

Several committees on various aspects are included in the WTO[12]. These committees have specific obligations and are accountable to the general council. Following this approach, a new committee on the IoT would have to be introduced. This committee should be supplied with the necessary resources to effectively create a legal framework for the IoT. By appointing specialists as members of such a body, knowledge and experience in IoT matters would be made available at a high regulatory level.

Nevertheless, it has to be kept in mind that this approach does not allow for private organizations or enterprises to contribute to the establishment of a legal framework. Within the WTO, only representatives of member states are in the position to vote for a

10 Such an approach is considered in the next two sections.

11 http://www.wto.org/english/thewto_e/whatis_e/tif_e/fact1_e.htm, accessed 23 February, 2010

12 Such as a Committee on Trade and Environment, a Committee on Trade and Development, a Committee on Regional Trade Agreements, etc. (see http://www.wto.org/english/ thewto_e/whatis_e/tif_e/org2_e.htm, accessed February 23, 2010).

particular decision. The inclusion of the private sector could only be achieved if member states establish consultation processes for private parties before they meet for discussions in the WTO [WEB 10]. However, the present political climate is not ideal for introducing this kind of committee in all member states within a reasonable time period.

8.2.3.4. *New committee of OECD*

The OECD) may also be an appropriate organization to act as international legislator for the IoT. The OECD is the successor of the Organization for European Economic Co-operation (OEEC), created in 1947. The OECD took over from the OEEC in 1961, its goals being sustainable economic growth and employment as well as a rise of the standard of living in member countries while maintaining financial stability. These goals are along the same lines as those of the IoT, which also include the growth of international trade and thereby an improvement in the standard living in all countries.

The OECD disposes of various committees that include representatives of member states and discuss specific areas. A special committee responsible for rule-setting and supervision in the IoT could be established, being made up of representatives of OECD member states, thereby assuring an international approach. The committee would be in the position, after deliberations, to issue formal agreements, standards and models, recommendations or guidelines on various issues of the IoT. It has to be kept in mind, however, that only 30 countries[13] are members of the OECD. While these 30 countries include the wealthiest states, the power of decisions nevertheless lies with only a small proportion of the world. Furthermore, while the OECD has extensive contacts with non-member economies, civil society, parliamentarians and other international organizations and bodies, the committee would only include governmental representatives of member states. This would be the case, even though it would be important in the IoT to include private parties (in

13 Australia, Austria, Belgium, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, Slovak Republic, Spain, Sweden, Switzerland, Turkey, United Kingdom and United States.

particular businesses) in discussions about how the framework is governed.

Nevertheless, the peer review process of the OECD, through which the performance of countries is monitored by other countries at the committee-level, deserves attention. Such a mechanism increases the simultaneous, more or less identical implementation as well as application of the IoT and should be introduced in any organization chosen to govern the IoT.

## 8.3. Substantive principles for IoT governance

### 8.3.1. *Legitimacy and inclusion of stakeholders*

The inclusion of the whole of society challenges the traditional legal and political understanding of legitimacy and makes it necessary to tackle the general question of who could be a legitimate stakeholder. Consequently, architectural principles need to be developed and compiled in an international legal framework; representation only has a legitimizing effect if the outcome reflects the values of the stakeholders represented. In particular, such a comprehension calls for procedures that establish equal bargaining powers and fair proceedings, as well as enhanced transparency and review mechanisms that enable the allocation of accountability [WEB 09a].

An IoT being within a specific public or private authority's power would hence increase the lack of legitimacy and democratic participation. In contrast, the system should be designed in a way that the rules are fair, are firmly rooted in a framework of formal requirements about how rules are made and are correspondingly interpreted and applied. Including all stakeholders concerned with the IoT in one way or the other generally ensures a form of reasonable representation. This is an important aspect when considering the legitimacy of institutions [WEB 09a]. The stakeholders' co-action, enhanced communication, coordination and cooperation in a kind of forum, frame a central institutional point for the regulation of IoT

issues, allowing for participation and dialog [for participation of civil society in the Internet, see [WEB 09b].

The future IoT, consequently, needs a multipolar and decentralized policy institutional setting considering the requirements of all stakeholders involved. It needs to be managed by several entities (for more details, see [FAB 08, p. 48-61]; from a political point of view, see [BEN 07]).

### 8.3.2. *Transparency*

Transparency is a key issue in the governance of any system or framework. Transparent mechanisms are central with regard to the introduction of regulations and internal structuring of an organization. The compliance with the following five elements is of importance [WEB 09a]:

– availability of an organization or an institution with sufficient power to influence the management of resources in the society, i.e. with a role in governance;

– existence of publicly reliable information, i.e. substantive quality standards related to information, supported by an adequate legal framework that influences people's choices, since a rational person would arguably organize his or her conduct in accordance with the law;

– definition of the recipient as an essential component for the perception of both information and transparency;

– availability of information, for example by establishing disclosure procedures, reporting requirements, granting the recipient investigative powers or a general right of access to information;

– observance of the time element, i.e. transparency implies constant visibility of information.

In this chapter, the focus will lie on transparency of governing bodies of the IoT, which are responsible for establishing regulations as well as ensuring the functioning of the IoT.

Transparency must be established for procedures, decision-making and elaboration of regulation. Stakeholders have to be in a position to follow all important actions in the governance of the IoT. Besides transparency in governing bodies, hierarchical transparency needs to be established – superior/principal bodies should have insight into the actions of their subordinates and vice versa.

Discussions on governance of the Internet have frequently raised the issue of transparency. Lessons for transparency in the IoT can be drawn from these discourses; proposed suggestions may help to establish transparent mechanisms before the IoT becomes fully functional (for transparency in other markets, see [WEB 09a, p. 124-127]).

After consistent criticism of ICANN's election-processes and decision-making procedures, ICANN has started to take steps to improve transparency in their governance of the Internet [WEB 09a, p. 127-129]. In particular, the aim has been a consensus-driven and bottom-up approach. Such an approach leads to broader transparency and additionally makes private entities accountable to the public, also giving non-state parties a voice in the rulemaking process [WEB 09a]. The inclusion of private entities is furthermore extremely important in the IoT, where users are mainly private parties and where it is therefore very possible that private entities will be responsible for its governance. These private entities will then have to be held accountable to the public.

The medium of the Internet, on which the IoT is based, offers valuable opportunities for transparent communication. In fact, in order to achieve transparency in the regulatory process, the Internet could be used to achieve open access to negotiations, to collect proposals and statements from the various stakeholders concerned and to present the decisions and results. It could thereby enhance and facilitate communication and dialog between IoT institutions and interested parties.

In the IoT, it is also of particular importance that mechanisms ensuring transparency are adaptable to technological change. As the IoT is still evolving, various (technological) changes in the system are

likely to be implemented. Notwithstanding these developments, transparency mechanisms should stay usable in the evolving system in order to ensure that information channels as well as participation mechanisms remain accessible for businesses, which will increasingly rely on an operable framework for their operations.

A certain consistency of the respective methods is also desirable with regards to convenience for individual users. They should not be forced to switch from one point of access or participatory mechanism, respectively, to another any time the technology evolves. This approach would render effective participation very difficult, in particular because users may not have the necessary capacities to follow up on technological developments in the IoT, except for major changes with considerable impact.

### 8.3.3. *Accountability*

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 the various segments of society, has to follow up on a multi-stakeholder approach to accountability. In particular, governance would improve if standards were harmonized in a way that makes governing bodies accountable, at least at the organizational level (for more details see 9WEB 09a, p. 132-148]). Consequently, accountability asks for a legal framework providing for regulations about the conduct of governing bodies and upon which actions can be measured.

Accountability can be framed along the following three elements (see [BUC 06, WEB 09a]):

– standards need to be introduced that hold governing bodies accountable, at least on the organizational level; such standards help to improve accountability;

– 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. In order to make information flow active rather than passive (seen from a

recipient's point of view) consultation procedures are to be established;

– accountability holders must 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.

These requirements have to be considered when establishing a legal framework introducing accountability measures for governing bodies. They serve as a basic guideline as to what key elements must be included. The legal framework should consequently address these issues in more detail.

The establishment of a code including the fundamental values that lay the foundation of accountability could provide for a viable way forward. Such a code may be similar to a Magna Carta or a constitutional approach; the standards in it could help implement a legitimizing structure and a guideline for governance of the IoT in general. Furthermore, the standards would be suitable to contain significant self-constraints for the policy-making institutions, and hence, move towards substantiating the realistic implementation of accountability (see also [WEB 07]). Nevertheless, the strengthening of the legal framework by a treaty-related model of governance, encompassing some kind of international supervision, would have supplemental merits. This is because pressure on privately introduced structures has the tendency to improve compliance by "market players".

Consequently, private initiatives need to be complemented by functional surveillance, for example under the organization that acts as international legislator, which will benefit from an extensive knowledge of the IoT itself as well as of its regulations. However, the exact embodiment of the respective surveillance should be decided upon by governments, scholars and businesses together. In particular, businesses as the main group of users should be asked for a feedback to proposed mechanisms and be able to comment on policy proposals.

Such inputs may increase the practicability and efficiency of the body to be established.

The legislative approach must also include sanctions that can be imposed on accountability-holders in the case of non-compliance with accountability criteria. Standards could help implement legitimizing structures and a guideline for governance principles [WEB 09a]. Furthermore, compliance with standards is generally increased by the threat of sanctions in the case of violations.

Businesses are subject to regular (independent) reviews in most countries. Respective provisions are usually included in codes on private law. Lessons could be drawn from the respective experiences. An example of an independent external monitoring mechanism is the auditing agencies in Swiss banking law. According to Swiss law, review bodies of banks have to be independent from the company management (in fact they must also differ in appearance) and report directly to the administrative board or an external auditing agency[14]. Furthermore, the review bodies have an unlimited right to access information if they request it[15].

The idea behind such an approach is that external monitors are considered more independent than internal monitors and therefore more likely to criticize the governing body or mechanisms within the framework. As they do not have their own individual interests in play, the appropriate functioning of the company is the only criterion for reviewers. Such a mechanism of supervision requires the involvement a private organization (to be established). A private institution seems to be more appropriate than the involvement of an intergovernmental supervision, because stakeholders are mainly private businesses. Therefore, a private organization may be in a better position to judge the needs and desires of these private users.

---

14 Art. 20 para. 3 Bundesgesetz vom 8. November 1934 über die Banken und Sparkassen (BankG).

15 Art. 19 para. 2 BankG.

## 8.4. IoT infrastructure governance

### 8.4.1. *Robustness*

A "robust" system is capable of dealing with changes in its operation without suffering from major damage or loss of functionality and can absorb attacks without failing. The IoT, as a system with a multitude of technological devices attached, is very exposed to failure. Therefore, robustness as a requirement of the framework has to be considered carefully.

In particular, in the IoT with sensors at its base, devices should have some knowledge about their own functionality and be able to "call for help" in case of failure [KEN 09]. Ideally, the IoT itself should include self-managing, self-monitoring, self-diagnosing and self-repairing structures in order to ensure the permanent functioning of the system [CAS 09]. On one hand, detecting singular points of failure at an early stage allows particular components to be detached and thereby helps to ensure the functioning of the rest of the system. On the other hand, potential problems could be solved before they increase to a size that would render the IoT inoperable.

The provision of a robust system for the IoT is primarily a task for technicians and engineers. They carry the responsibility of developing a system that can absorb attacks. In particular, it is important not to overload the functionality in objects. Rather than loading each device with copies of the same functionality, the possibility to seek additional information from a dedicated device or sensor should be adopted [KEN 09]. An ideal approach – as we are still in the development stages of IoT – would be to generate various models, which are then to be tested for their robustness through the inducement of failures.

The business sector as the user could assist this process by participating in the test. Such participation would allow for technicians to determine exactly how businesses will be using the IoT and what effect this use can have on the system. Thereby, problems can be recognized and analyzed before the system becomes fully functional. Furthermore, the mechanism enables the business sector to

comment on various technologies and give their preferences at a very early stage, which may avoid complaints about the IoT at a later stage.

### 8.4.2. *Availability*

Availability of a system is the proportion of time that it is able to be used and the time it takes the system to recover from a failure [BIR 07, STA 03]. Availability is important for any technology. However, for the IoT it is particularly significant because businesses are involved. Risks from a lack of availability include a cutback in functionality, a production stop or sabotage for producers. Under the aspect of logistics, the limitation of availability may result in problems related to ordering and supplying, hindrance of status updates, a cutback in functionality, sabotage or reduced transparency. For the end-user, a lack of availability gives rise to product data not being available, limited functionality of services for "smart offices" or "smart homes" or limited functionality of personal consulting services [DEU 09].

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". If the one existing root is attacked and suffers a breakdown – e.g. through a denial-of-service attack – the whole IoT is incapacitated. Therefore, the IoT has to be decentralized in order to allow for singular roots or other points in the system to be detached. Such detachment should, however, not affect the function of the IoT. Other roots or services would need to take over the tasks of the incapacitated fragment. The ideal scenario would allow for roots to intercept queries directed to the attacked root and answer them instead. Technology may not yet be in the position to configure such a mechanism, however. Furthermore, it would require that every root has all the data available, which is neither realistic nor very practical.

The requirement of availability includes the system's capability to accommodate a large number of subscribers. Users need to be able to retrieve information from the IoT without delays. If immediate access is not possible, businesses may lose part or all of their benefits as prices may be fluctuating. Therefore, the IoT can only serve as a

global platform if availability is ensured. Otherwise, businesses may not make use of the system. Consequently, availability has to be guaranteed even if a large number of businesses are simultaneously making enquiries for information, i.e. the service should not be slowed down.

Furthermore, before the tagging of objects is started, the number of possible unique identification numbers has to be determined. It must be made sure that this number is sufficient to identify all possible objects for at least the mid-term future. The IoT should not get into the situation that the number of identifications possible is used up while still in its infancy.[16]

Notwithstanding this fact, an expansion of the IoT may at some time become necessary. Therefore, the system has to be construed in a way that ensures the capability of future expansion, i.e. the long-term sustainability of the IoT must be guaranteed. The IoT should continuously be accessible while the system is transformed or extended, without suffering from a temporary shutdown. This is particularly important as an increasing number of businesses will transfer a large part of their delivery and/or ordering through the IoT and are therefore dependent on the system functioning in order to carry out their daily business.

### 8.4.3. *Reliability*

The reliability of a system is 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. In more technical terms, "[r]eliability is the probability of a product performing without failure, a specified function under given conditions for a specified period of time" [STA 03; see also BIR 07].

Reliability should be maximized through specific measures before the IoT becomes operable. Furthermore, tests need to be carried out

16 For example, in the Internet, a transition of IP (from IPv4 to IPv6) has become necessary because the current IP addressing system is at risk of not being able to satisfy all IP address requests made by Internet hosts [WEB 09a].

once the IoT is used in order to determine points of weakness and improve confidence in the IoT. As a large part of businesses' activities will rely on the IoT, confidence in the system is indispensable.

In practice, reliability can be improved by anticipating the sources of failure or reduced performance of the system, i.e. the disconnection of the network or degraded performance. Furthermore, consequences of such scenarios must also be considered. In particular, mechanisms have to be foreseen for such cases, as well as their practical implementations. In the constructing of such mechanisms, the source of failure plays an important part. Three different types of reliability issues may arise: intentional damage, failures caused by extrinsic factors or random failures. Each of these categories requires different responses and different mechanisms to avoid failures in the first place. In addition, for each foreseeable point of failure, information about services depending on this point has to be available in the hope that the failure can be addressed at an early stage and will not affect all of the services depending on it [STA 03; see also BIR 07].

Reliability can only be measured for each service individually (see also [BIR 07, STA 03]). Therefore, the reliability of the IoT cannot be evaluated as such, but different components of the IoT have to be considered and, thereupon, a comprehensive assessment be carried out. Individual services of the IoT include, for example, the posting of information or the accessibility of information for interested parties. Another aspect may be the provision of services through the IoT.

Besides considering potential failures that may arise during the future operation of the IoT, constant monitoring of the system while it is in operation is also necessary to ensure reliability. Failures have to be located and addressed as soon as possible. Thereupon, their sources and reasons should be followed up in order to avoid the same problems recurring.

### 8.4.4. *Interoperability*

The IoT requires various forms of connectivity and interoperability. 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. While connectivity assures that various devices are linked to one another, interoperability refers to the compatibility of the respective parts (for interoperability for telecommunications see [SCH 05]).

Interoperability of different parts of the IoT requires a certain extent of standardization. However, private parties do not usually voluntarily agree to conform to standards. Therefore, incentives need to be introduced. These incentives for standardization can be economic. But incentives are low when the transaction costs of the standard development swamp the benefits or when standardization eliminates competitive advantage [PER 00]. In order to make sure that incentives are high enough, the economic effects of standardizing mechanisms have to be considered in their establishment and be installed in a way that ensures that private parties are likely to agree to the standardization.

Furthermore, backward compatibility is indispensable in a technology such as IoT. As technologies are constantly evolving and improving, individual parts of the system have to be adaptable to new technologies without being replaced. The IoT – at this moment – is still in its infancy and technologies have only recently been developed. Therefore, compatibility with older parts is not an issue. However, bearing in mind that the IoT also makes use of the Internet, certain aspects of the IoT have to be construed in a way that makes them compatible with older versions of the Internet.

A further approach to the interoperability of the IoT is to separate its functionality from its technical implementation, i.e. integrate a diverse set of technologies into the structure of the IoT. This allows for the application of various solutions to different applications. Such an infrastructure including various technologies will also satisfy the requirement for compatibility over time as an infrastructure built with heterogeneity in mind will easily be able to implement newly-developed devices and networks [HAL 09].

### 8.4.5. *Access*

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 widespread availability of access points [WEB 03].

Since access and interconnection are of major importance, particularly for smaller market players and businesses in developing countries, not only the principles but also the details of the framework are significant. The degree of openness in respect to access and interconnection substantially influences the effectiveness of market forces [GRE 99]. Increasing entrepreneurial mobility in the information technology value chain will only occur if the use of the IoT is available to all interested persons and enterprises. Interconnection means the physical linking of separate networks (establishment of any-to-any communications); access is a broader concept comprising all requests by market participants to obtain access to a network operator's assets or its users [GRE 99].

An important topic in this context is the affordability of access and its communication possibilities. Relevant aspects include international connectivity prices and costs. Reasonable pricing is crucial for the successful implementation of the IoT and for maintaining its end-to-end functionality. In other words, the costs associated with building the networks and accessing aspects as well as associated revenues are to be distributed among the different players in a fair way [WEB 09a].

Affordability of access to the IoT is particularly relevant in less developed countries that could take advantage of the IoT in their comparative handling of cross-border trade. With regard to the inclusion of participants from developing countries, lessons can be drawn from discourses on digital divide in the Internet. At least in the beginning, financial as well as technological assistance must be provided to businesses in developing countries. However, users from developed countries will in turn also benefit from the presence of businesses from less developed countries.

The right to access can also be seen to be based on the *essential facilities doctrine*. The concept emerged in US law and expanded into European law. A number of decisions of the European Commission have lead to the general acceptance of this doctrine, concerning the grant of access to some kind of facility or resource controlled by a dominant undertaking. A refusal to grant access to an essential facility may be construed as a breach of competition rules[17].

The European Court of Justice has defined dominance as:

> "a position of economic strength enjoyed by an undertaking which enables it to hinder the maintenance of effective competition on the relevant market by allowing it to behave to an appreciable extent independently of its competitors and users and ultimately of users"[18].

Depending on the number of governing bodies and servers providing access, a dominant undertaking may develop for the IoT, which calls the essential facilities doctrine into being.

Essential facilities were defined as "a facility or infrastructure without access to which competitors cannot provide services to their users"[19]. Access to facilities by competitors has to be truly "essential" to justify obliging dominant players undertaking to grant access; a desire to access is not sufficient [GRI 03, JON 08]. In the future, access to the IoT may become indispensable in order for businesses to access any information on products. If the IoT develops into the main system of trade, not being able to access it may lead to the demise of a

17 European Court of Justice, Case C-418/01, IMS Health GmbH & Co. OHG *versus* NDC Health GmbH & Co. KG, judgment of April 29, 2004; European Court of Justice, Case C-241/91 P and C-242/91 P, Radio Telefis Eireann (RTE) and Independent Television Publications Ltd. (ITP) *versus* Commission of the European Communities, judgment of April 6, 1995; PER 00, section 2.20; JON 08, 537-542, SCH 01, 65-78.

18 European Court of Justice, Case 322/81, Michelin *versus* Commission, 1983, E.C.R. 3461, at 3503; see also GRI 03, 435-438, SCH 01, 80 - 81.

19 Sealink/B&I Holyhead: Interim Measures, 1992, 5 CMLR 255.

company. Therefore, the IoT may be considered an essential facility in the future.

## 8.5. Further governance issues

Various difficulties can still stand in the way of a successful introduction of IoT at the global level. Some of these difficulties are of a more practical nature, while others concern legal challenges. However, they need to be addressed before the IoT's launch in order to avoid a partial failure of the system.

### 8.5.1. *Practical implications*

Users of the IoT have diverse linguistic backgrounds. Therefore, for information made available through the IoT, translations of the relevant documents are necessary. Information should be provided primarily in English in order to make it understandable for as many people as possible.[20] However, efforts need to be undertaken to translate important documents so that information may be disseminated in at least the six United Nations languages (English, French, Spanish, Arabic, Chinese and Russian). Lessons on this subject can be drawn from discussions on multi-lingualism that have taken place in Internet governance[21].

Businesses are the primary beneficiaries of the IoT, so it may be justified that they are given the task of translating their own information. As long as translation is only required into one main language, the benefits from increasing turnover are still likely to outweigh the additional costs of a translation service. Furthermore, these translators will also be needed once contact with interested users has been established and the process of negotiations has started (for more details, see WEB 10).

---

20 English is the most common programming language; it can therefore be assumed that English is the language that reaches the most people.

21 See, for example WSIS, Geneva Declaration of Principles, Article 48.

### 8.5.2. *Legal implications*

Various legal problems may also emerge with the introduction of the IoT. In particular, two areas of concern come to mind. First, the RFID as an aspect of the IoT relies on radio frequencies, which is controlled by national regulations. Therefore, allocated bands or the conditions of such use may vary between states [CAS 09, p. 54]. Second, opposition to the attribution of all objects with RFID tags outputting electromagnetic energy could also come from states which are concerned with matters of health[22] and safety.

With regard to the regulation of radio frequency, it is important for the IoT that all RFID tags attached to objects operate at the same frequency in order to allow users to effectively use the system. If different frequencies are installed in different states, the IoT as a platform for the exchange of information becomes impractical. Accordingly, bands have to be harmonized and regulated. Such harmonization is necessary to obtain interoperability. It may be best suited for governments to establish a universal frequency for RFID tags that are subsequently used in the IoT. As frequency allocation falls within the autonomy of states, these should also be responsible for handling IoT frequencies. Furthermore, states will have to make sure that the frequencies allocated to RFID tags do not interfere with other services, such as radio or television.

As far as health impacts of RFID-tagged objects are concerned, studies need to be carried out identifying the potential risks before the IoT becomes reality, or is rejected based on insufficient studies that do not exhaustively address health risks. In particular, electromagnetic fields resulting from the tagging of all things have to be measured. Furthermore, solutions to potential risks have to be introduced, such as for example barriers that intercept radiation. Such barriers can only practically be installed in specific locations for very specific purposes, for example in hospitals. They are not suitable to protect the individual from negative effects of radiation. The results of these

22 The IoT does also have various positive effects on health. For example, it provides the possibility of transmitting information about patients as well as alerting emergency health services to dangerous situations, such as heart attacks.

studies and assessments could consequently be transformed into guidelines or – if possible – binding law. In particular, provisions could be introduced in existing energy law. Thereby, states would be bound to take measures to protect the general public from the electromagnetic fields emitted by tagged objects. Possibilities to establish such regulation at international level have to be explored, as radiation through tagged things has a global impact[23].

## 8.6. Outlook

Governance issues have not yet been addressed in detail regarding the structuring of the IoT. The respective lack of discussions is regrettable in light of the importance of governance issues. Debates are required about:

– organizational issues (such as the establishment of self-regulatory organizations and an international legislative body);

– substantive topics (legitimacy, transparency, accountability); and

– infrastructure requirements (robustness, availability, reliability, interoperability and access).

Further, scholarly research and programming for practical implementation of the IoT should be undertaken in order to broaden the chances the IoT will be successful.

## 8.7. Bibliography

[AND 05] ANDERSON K., "Book Review: Squaring the Circle? Reconciling Sovereignty and Global Governance through Global Government Networks", *Harvard Law Review*, vol. 118, p. 1255-1312, 2005.

[BEN 04] BENZ A., "Einleitung: Governance – Modebegriff oder nützliches sozialwissenschaftliches Konzept?", in: Arthur Benz (ed.), *Governance – Regieren in komplexen Regelsystemen*, Wiesbaden 2004, p. 11-28.

23 For more details on barriers to the IoT, see [WEB 10].

[BEN 07] BENHAMOU B., *A European Governance Perspective on the Object Naming Service*, Governance of Resources, 2007 (available at ftp://ftp.cordis.europa.eu/pub/fp7/ict/docs/ch1-lisbon-20071215_en.pdf, accessed February 23, 2010).

[BIR 07] BIROLINI A., *Reliability Engineering*, 5th edition, Berlin, Springer, 2007.

[BUC 06] BUCHANAN A., KEOHANE R.O., "The legitimacy of global governance institutions", *Ethics and International Affairs*, vol. 20, p. 405-437, 2006.

[CAS 09] CASAGRAS, *Final Report, RFID and the Inclusive Model for the Internet of Things*, EU Project Number 216803, RFID Global Forum, London, 2009.

[DEU 09] 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] 2009 (available at: http://www.vdivde-it.de/publikationen/dokumente/ doku-581-internet-der-dinge.pdf, accessed February 23, 2010.)

[FAB 08] FABIAN B., Secure name services for the Internet of Things, PhD thesis, Berlin, 2008.

[GRE 99] GREWLICH K.W., *Governance in "Cyberspace": Access and Public Interest in Global Communications*, The Hague, Kluwer Law International, 1999.

[GRI 03] GRINGRAS C., *The Laws of the Internet*, 2nd edition, London, Butterworth, 2003.

[HAL 09] HALLER S., KARNOUSKOS S., SCHROTH CH., "The Internet of Things in an Enterprise Context", in: Domingue J., Fensel D., Traverso P. (eds), *Future Internet – FIS 2008*, Berlin, p. 14-28, 2009.

[JAC 94] JACOBS S., "Why governments must work together", *The OECD Observer*, vol. 186, p. 13-16, 1994.

[JON 08] JONES A., SUFRIN B., *EC Competition Law*, 3rd edition, Oxford, Oxford University Press, 2008.

[KEN 09] KENNEDY D., "Five basic rules for the Internet of Things", *EURESCOM mess@ge*, vol. 2, 2009. (available at: http://www.eurescom.eu/~pub/about-eurescom/message_2009_02/Eurescom_message_02_2009.pdf, accessed February 23, 2010.)

[LAN 04] LANGE S., SCHIMANK U., "Governance und gesellschaftliche Integration", in: Lange, S., Schimank, U. (eds), *Governance und gesellschaftliche Integration*, Wiesbaden, VS Verlag für Sozialwissenschaften, p. 9-44, 2004.

[MAY 03] MAYER-SCHÖNBERGER V., "The shape of governance: analyzing the world of Internet regulation", *Virginia Journal of International Law*, vol. 43, p. 605-673, 2003.

[PER 00] PERRITT H., "The Internet is changing the public international legal system", *Kentucky Law Journal*, vol. 88, p. 885-955, 1999-2000.

[REI 97] REINICKE W.H., "Global public policy", *Foreign Affairs*, vol. 76, p. 127-138, 1997.

[RUG 04] RUGGIE J.G., "Reconstituting the global public domain – issues, actors and practices", *European Journal of International Relations*, vol. 10, no. 4, p. 499-531, 2004.

[SCH 05] SCHERER J., *Telecommunication Laws in Europe*, 5th edition, Haywards Heath, Tottel Publishing, 2005.

[SCH 01] SCHULZ R., *Der Zugang zum "blanken Draht" im Telekommunikationsrecht: Wettbewerb im Netz oder Wettbewerb zwischen Netzen?*, Munich, Beck, 2001.

[SLA 04] SLAUGHTER A., *A New World Order*, Princeton, Princeton University Press, 2004.

[STA 03] STAVROULAKIS P. (ed.), *Reliability, Survivability and Quality of Large Scale Telecommunication Systems*, Chichester, Wiley, 2003.

[TWO 07] TWOMEY P., "Effect of Multilingualism on the Internet", *NSF/OECD Workshop*, January 31, 2007, (available at: http://www.oecd.org/dataoecd/12/18/38014552.pdf, accessed February 23, 2010.)

[VAN 05] VAN DER TOGT R., VAN LIESHOUT E.J., HENSBROEK R., BEINAT E., BINNEKADE J.M., BAKKER P.J.M., "Electromagnetic interference from radio frequency identification inducing potentially hazardous incidents in critical care medical equipment", *JAMA*, vol. 24, no. 299, p. 2884-2890, 2005.

[WEB 03] WEBER R.H., *Towards a Legal Framework for the Information Society*, Zurich, Schulthess, 2003.

[WEB 07] WEBER R.H., GROSZ M., "Internet governance – from vague ideas to realistic implementation", *Medialex*, no. 3, p. 119-135, 2007.

[WEB 09a] WEBER R.H., *Shaping Internet Governance: Regulatory Challenges*, Zurich, Schulthess, 2009.

[WEB 09b] WEBER R.H., WEBER R., "Inclusion of the civil society in the governance of the internet. Can lessons be drawn from the environmental legal framework?", *Computer Law Review International*, vol. 1, p. 9-15, 2009.

[WEB 09c] WEBER R.H., "Internet Corporation for Assigned Names and Numbers (ICANN)", in: Tietje/Brouder (eds), *Handbook of Transnational Economic Governance Regimes*, Leiden, Martinus Nijhoff, p. 603-619, 2009.

[WEB 10] WEBER R.H., WEBER R., *Internet of Things*, Zurich, Schulthess, 2010.