

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

Accountability in the Internet of Things

Rolf H. Weber

University of Zurich, Switzerland

ABSTRACT

Keywords:

Accountability
Legitimacy
Sanctions
Standards
Surveillance

Accountability of governing bodies in the Internet of Things (IoT) is of major importance and requires a partly different approach than applied in the (general) Internet. Improving accountability makes the implementation of new general principles necessary in order to provide for a stable and foreseeable legal framework on which businesses can rely. In particular, standards need to be introduced that hold governing bodies accountable, information should be made more readily available and beneficiaries of accountability must be able to impose some sort of sanction on the accountable in case of non-compliance. Improving accountability by creating such framework also supports the betterment of security in the Internet of Things.

© 2011 Rolf H. Weber. Published by Elsevier Ltd. All rights reserved.

1. Introduction

The Internet of Things as an emerging global Internet-based information architecture facilitating the exchange of goods and services is gradually developing. While the technology of the Internet of Things (IoT) is still being discussed and created, an adequate legal framework should be established before the IoT is fully operable, in order to allow for an effective introduction of the new information architecture and therewith protect the developing new services.

In this context the accountability of governing bodies in the IoT is of major importance.¹ As business transactions and information exchanges are carried out through that system, it is essential for the involved parties to know how the respective actions will be carried out. Furthermore, if commercial transactions fail because of faults in the system (potentially involving large amounts of money), businesses need to know whom to hold responsible.

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.² Consequently, accountability asks for a legal framework providing for regulations about the conduct of governing bodies and upon which actions can be measured.

2. Elements of the conceptual framework

2.1. Governance principles

Being developed beyond a regulatory legal framework the Internet was mainly based on self-regulation by its users since the assumption prevailed that cyberspace was an independent new “province” in the world, not governed by law in the legal sense but rather by “codes” defining the Internet as

¹ This paper is based on the presentation which the author has given at the Internet of Things 2010 Conference in Tokyo on November 29, 2010; it further develops ideas having been addressed in other publications of the author.

² For more details see R.H. Weber, *Shaping Internet Governance: Regulatory Challenges*, Zurich, 2009, 2002, pp. 132–148.

parameters resulting from technical protocols, standards and procedures.³ Indeed the Internet in the nineties of the last century evolved from a new communication platform of a comparatively small research and academic community into a global facility available to and used by the general public⁴; over time more and more actors felt a need for more regulation.⁵

According to the working definition proposed by the Working Group on Internet Governance (WGIG) in 2005 and adopted by the UN World Summit on the Information Society (WSIS), Internet Governance is generally understood as “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 programs that shape the evolution and use of the Internet”.⁶

Compliant with this multi-stakeholder approach, several players like governmental agencies, industry and civil society are concerned by the governing of the online world to date, each of them trying to enforce their respective interests. A similar development can be seen in respect of the IoT: Business “invented” new platforms, at the beginning mainly for commercial purposes, whereupon legislators are becoming active by introducing a legal framework.

Obviously, for historical reasons, the discussion of governance issues in the IoT is likely to rely on the general Internet governance principles. Notwithstanding, the differences should not be underestimated: Internet governance discussions have largely focussed on DNS-related questions such as addresses and registries. In contrast, the IoT will focus on identifiers and the origins of identifying mechanisms which are quite different.

Since IoT-related technologies can be used anywhere and are in practice quiet and unobtrusive,⁷ for the protection of all participants in the IoT the creation of a legal framework is of fundamental importance. The specialized field of IoT regulation requires a high level of competence and expertise whereby the joint involvement of all stakeholders having the necessary knowledge is desirable.⁸

³ On codes as the law in the Internet see L. Lessig, *Code and other Laws of Cyberspace*, New York, 1999; regarding its critical appraisal as well as the myth of independence of cyberspace and the role of law see R.H. Weber, *Regulatory Models for the Online World*, 2002, pp. 25/26 and 93–99; on the decentralized standard-setting process see J.P. Liu, *Legitimacy and authority in Internet coordination: A domain name case study*, *Indiana Law Journal*, vol. 74, 1999, pp. 587/588 and 595–604; D.W. Drezner, *All Politics is global: Explaining International Regulatory Regimes*, Princeton/Oxford, 2007, pp. 107ss.

⁴ Tunis Agenda for the Information Society, 2005, para 30, available at: <http://www.itu.int/wsis/docs2/tunis/off/6rev1.html> (accessed 1 Dec 2010).

⁵ For a basic overview of the regulatory problems see R.H. Weber, *Regulatory Models for the Online World*, supra note 3, pp. 101ss.

⁶ Report of the Working Group on Internet Governance, 2005, para 10, available at: <http://www.wgig.org/docs/WGIGREPORT.pdf> (accessed 1 Dec 2010).

⁷ European Parliament resolution of 15 June 2010 on the Internet of Things (2009/2224(INI)), para 15, available at: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2010-0207+0+DOC+XML+V0//EN> (accessed 1 Dec 2010).

⁸ H.J. Kleinstaubler, *The Internet between Regulation and Governance*, in: *OSCE Representative on Freedom of the Media, The Media Freedom Internet Cookbook*, C. Möller/A. Amouroux (eds), Vienna, 2004, pp. 72/73.

2.2. Notion of accountability

Accountability, based on the Latin word *computare* (to calculate), is a pervasive concept, encompassing political, legal, philosophical, and other aspects; each context casts a different shade on the meaning of accountability. Nevertheless, a general definition incorporating the main elements of accountability is directed to the obligation of a person (the accountable) to another person (the accountee), according to which the former must give account of, explain and justify his actions or decisions in an appropriate way.⁹

Together with checks and balances, accountability is a prerequisite for legitimacy and a key element of any governance discussion. While checks and balances take place by providing mechanisms to prevent the abuse of power, accountability steps do so by providing for or accessing actions with mechanisms such as non-judicial remedies, or judicial review.¹⁰ In particular, accountability implies that the stakeholders who form part of the governance mechanisms should be obliged to being called out to answer to anyone.

As a fundamental principle, accountability concerns itself with power and power cannot be divorced from responsibility.¹¹ Therefore, responsibility should be commensurate with the extent of the power possessed.¹² Furthermore, accountability depends on reliable information which needs to be available, accessible (both logistically and intellectually) and based on known sources. Without such mechanisms, civil society will not be informed or able to participate, and decision-making will not be democratic.

2.3. Elements of accountability

Accountability can be framed along the following three elements:¹³

- 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 the concerned recipients, 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 passive¹⁴ consultation procedures are to be established;

⁹ See R.H. Weber/R. Weber, *Internet of Things: Legal Challenges*, Zurich, 2010, p. 80; R.M. Lastra/H. Shams, *Public Accountability in the Financial Sector*, in: *Regulating Financial Services and Markets in the 21st Century*, E. Ferran/Ch.A.E. Goodhart (eds), Oxford, 2001, pp. 165–188, 167; J. Malcolm, *Multistakeholder Governance and the Internet Governance Forum*, Perth, 2008, p. 262.

¹⁰ Ch. Kaufmann/R.H. Weber, *The Role of Transparency in Financial Regulation*, *Journal of International Economic Law*, Vol. 13, 2010, p. 779, pp. 791–796.

¹¹ S.B. Young, *Reconceptualizing accountability in the early nineteenth century: how the tort of negligence appeared*, *Connecticut Law Review*, vol. 21, 1989, p. 201.

¹² R.M. Lastra/H. Shams, supra note 9, p. 167.

¹³ R.H. Weber/R. Weber, supra note 9, p. 81; A. Buchanan/R.O. Keohane, *The legitimacy of global governance institutions*, *Ethics and International Affairs*, vol. 20.4, November 2006, pp. 405–437.

¹⁴ Seen from a recipient's point of view.

- Beneficiaries of accountability 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.

3. Concretization of an accountability concept

3.1. Code of standards as foundation

The establishment of a code of principles 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 Charta or a constitutional approach; the standards could help implement a legitimizing structure and a guideline for the governance of the IoT in general in order to ensure that the accountable parties behave in a way that benefits all participants in the IoT, rather than solely themselves.

The importance of standards in the information and communication environment has become obvious for more than a decade. Standards help to reduce the diversity of (technical) forms and allow exchanges between market participants in a not too complicated way. Insofar, standardization should be based on compatibility and technology-neutrality. Often a distinction is made between two sorts of standards, namely coordinating and regulating standards: A coordinating standard is a rule that facilitates an activity which otherwise might not exist; a regulatory standard restricts a certain behavior according to a policy rule set by the regulator.¹⁵

Furthermore, a code of standards is suitable to contain significant self-constraints for the policy-making of the governing institution and hence, more towards substantiating the realistic implementation of accountability.¹⁶ 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”.

3.2. Accountability challenges

Challenges in holding participants in IoT markets accountable are manifold. Three areas of particular relevance with regard to accountability can be identified:¹⁷

¹⁵ L. Lessig, The limits in open code: regulatory standards and the future of the net, *BTLJ*, vol. 14, 1999, p. 759; R.H. Weber, *supra* note 3, p. 119.

¹⁶ R.H. Weber/M. Grosz, Internet Governance- From Vague Ideas to Realistic Implementation, *Medialex*, vol. 3, 2007, p. 128.

¹⁷ Ch. Kaufmann/R.H. Weber, *supra* note 10, pp. 792–795.

- The institutional challenge relates to the accountability of the participants in the IoT markets towards society; in this regard, the nature of some of the key actors as “independent” institutions and expert networks is relevant.
- The second challenge is the contractual challenge: Two of the basic accountability mechanisms with regard to the relation between the customers and the suppliers in the IoT markets are a legal remedy to claim compensation for losses and the possibility to sanction violations.
- The third challenge is embedding accountability in an international context since IoT markets are undisputedly global markets and yet there is no specific legally binding global regulatory framework.

In light of the direct involvement of businesses in the IoT the elements of market accountability also play a major role. A business’ ability to attract and maintain customers is a central indicator of its accountability to the public in the market place; insofar, choices of the concerned market players are the key constituents for the organization.¹⁸ Consequently, the accountability mechanism is reflected in the responsiveness to the needs of all participants in the IoT.

Accountability should encompass two main objectives which need to be kept in mind:

- Promotion of public understanding of the business system and consequently maintenance of confidence in the system;
- Assurance of an appropriate degree of consumer protection.

Public understanding and confidence can be achieved if the accountable person provides for an adequate account of his/her decisions or actions and explains/justifies the decisions or causes of actions; in other words, accountability implies a duty to give account and explain.¹⁹ Partly, legal doctrine distinguishes between “explanatory accountability” where the obligation is to answer questions, i.e. to give account of actions, and “amendatory accountability” where there is an obligation to make amends and grant redress.²⁰

A further distinction concerns the timing: Accountability can be exercised *ex ante* or *ex post*, namely before/during the process of taking the decisions/actions, or after decisions/actions have been taken.²¹ The definition of the appropriate degree of consumer protection cannot easily be answered since it leads to a variety of aspects depending upon the given circumstances. Nevertheless, in general it can be said that, unless external criteria are presented, accountability has to be given in a form which makes the recipients capable of measuring and assessing the given information (Goodhart, 2001).

¹⁸ De Vey Mestdagh and Rijgersberg, *International Review of Law, Computers and Technology*, March 2007, pp. 27, 32.

¹⁹ R.M. Lastra/H. Shams, *supra* note 9, p. 168.

²⁰ C. Turpin, Ministerial Responsibility, in: *The Changing Constitution*, J. Jowell/D. Oliver (eds), 2nd edn., Oxford, 1994, p. 109.

²¹ R.M. Lastra/H. Shams, *supra* note 9, p. 169.

3.3. Participants' respective roles regarding IoT accountability

Businesses are the main drivers of the IoT. However, an appropriate framework is composed of governmental agencies, the private sector and civil society. Their respective roles need to be discussed.

3.3.1. Role of private sector

The "organization" of the IoT mainly stems from the private sector, but private initiatives need to be complemented by functioning "supervision" mechanisms, for example under an organization that acts as international legislator,²² which will benefit from an extensive knowledge of the IoT itself as well as of its regulations. However, the exact embodiment of the respective mechanisms 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 input may increase the practicality and efficiency of the body to be established.

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. The auditing agencies in Swiss banking law are an example of an independent external monitoring mechanism. According to Swiss law, review bodies of banks have to be independent from the company management and report directly to the administrative board or an external auditing agency. Furthermore, the review bodies have an unlimited right to access information if they request it.²³

The idea behind such an approach, based on the concept of market accountability, is that external persons 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 of a private organization (to be established). A private institution seems to be more appropriate than the involvement of an inter-governmental supervisor, 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.

3.3.2. Role of civil society

In view of the fact that the Internet has evolved into a global facility and that IoT-technologies will have an impact in various areas, the IoT's international management and, consequently, the development of an accountability framework should be done with the full support of all; next to the governments and the private sector civil society has to participate actively in the rulemaking processes.

Similarly as in the Internet, a specific line of accountability in the IoT must also run to the consumers as part of civil

society. This obvious appreciation, however, is confronted with the practical problem that consumers are usually not readily organized; therefore, initiatives have to be taken which include consumer panels to represent the interests of consumers (Page, 2001). If civil society does have a voice in the IoT, market players on the offering side are in a position to become aware of the evaluation of their accountability.

4. Surveillance and monitoring as accountability instruments

In democratic States accountability can (also) be secured through institutionalized "control" mechanisms. Surveillance means a repeated surveying of certain activities, monitoring a more or less permanent and regular observation and recording of activities.

4.1. Surveillance

The implementation of standards by businesses and their application related to the private sector and civil society is often not sufficient to realize the appropriate accountability. Consequently, a supervisory body would have to be established which could intervene in case of non-compliance by certain market participants with accepted standards of accountability. If the level of the "state of the art" is not reached, a formal intervention must take place.

For the time being, a supervisory body for the IoT does not exist. Considering the global access to the IoT, the most fundamental guidelines should be established on a legally binding basis, preferably by an international legislator. This international legislator could either be newly established or be introduced as a Committee of an already existing international Organization. In principle, the incorporation of a new regulator is possible, however, reluctance to such a scheme is usually quite outspoken.²⁴ An alternative could consist in having the WTO or OECD establishing a new body which should devote its supervisory functions to the surveillance of the market participants in the IoT.²⁵ Being a Committee within an existing organization, the leeway in its creation is rather limited, however, the globality of the approach is questionable, as only representatives of member States (of the WTO or the OECD) would be electable into the Committee.

4.2. Monitoring

The design of consultation processes involving the (potential) customers in IoT markets depends on the matters concerned and on the availability of active community members. However, the participants in the IoT should not only be consulted in the preparatory phase of projects, but also in any relevant implementation phase. Feedback mechanisms to civil society concerning reviewing processes need to be consistently utilized – an aspect which would also allow the

²² See Ch. Kaufmann/R.H. Weber, supra note 10, pp. 791/92.

²³ See R.H. Weber/R. Weber, supra note 9, pp. 84/85 with further references.

²⁴ For further details see R.H. Weber/R. Weber, supra note 9, pp. 27–30.

²⁵ For further details see R.H. Weber/R. Weber, supra note 9, pp. 30–33.

participants in the process to understand how their insights and expertise have influenced the policy outcomes.²⁶

In business matters such as the IoT, many operations are necessarily cloaked with commercial confidentiality. To a certain extent, confidentiality is justified and cannot be replaced by an unrestrictedly free flow of information. A possible solution to this problem could be seen in the establishment of an overseeing board on the operations of the market participants on the offering side.²⁷ Within such an overseeing board the tensions between accountability and confidentiality could be bridged.

Accountability must equally extend to the monitoring stages of a framework's realization and empower the development of effectiveness through the participation of all parties involved. Different kinds of capacities need to be made available in order to meaningfully improve participation during a decision-making process, namely (i) the ability to understand and criticize technical issues, (ii) sufficient knowledge on the given structures and potentials, and (iii) the skills necessary to negotiate with more powerful actors.²⁸

5. Sanctions as consequence of non-compliance with accountability rules

Accountees must be able to impose some sort of disciplinary and enforcement powers, thus, attaching costs to the failure to meet the standards. Such "sanctioning" is only possible if adequate participation schemes allow the concerned persons to get hold of the relevant information constituting the basis for getting redress.

Sanctions can be of a civil or criminal nature. Civil law accountability mechanisms encompass legal remedies to claim compensation for losses; as a rule, such remedies will be provided for by the applicable national civil law framework. From a governance and policy perspective, providing effective grievance mechanisms for those who believe that they have been harmed contributes to restoring trust in the business system.²⁹ Yet, traditional remedies are not easily available to everybody, and additionally, they may be cost and time intensive. A minimum framework which could be established by the legislator would have to include legitimacy of decision-making courts, fair and equitable procedures, accessibility to courts and predictability of judicial outcome.

The legislative approach must also include sanctions that can be imposed on those accountable in the case of non-compliance with accountability criteria. Widely accepted criminal standards could help implement legitimizing structures and a guideline for governance principles.³⁰ Experience shows that compliance with standards is generally increased by the threat of criminal sanctions in the case of violations.

²⁶ R.H. Weber/R. Weber, *supra* note 9, p. 85.

²⁷ See Ch.A.E. Goodhart, *Regulating the regulator - An Economist's perspective on accountability and control*, in: E. Ferran/Ch. A.E. Goodhart, 2001, cited, *supra* note 9, p. 163.

²⁸ R.H. Weber/R. Weber, *supra* note 9, p. 86.

²⁹ Ch. Kaufmann/R.H. Weber, *supra* note 10, III.D.2 (2).

³⁰ R.H. Weber/R. Weber, *supra* note 9, p. 84. 7.

6. Conclusions

Improving accountability requires the implementation of some general principles which can, based on the above considerations, be summarized as follows:

- Use of developments in technology to enhance participation processes;
- Provision of information on relevant issues for the community and civil society in good time;
- Establishment of fora as the basic mechanism for conducting an exchange of opinions;
- Provision of sufficient context and background material to enable the concerned market participants to understand the issues being the topics of accountability;
- Introduction of sanctions for the case of non-compliance with accountability requirements.

Accountability of governing bodies is even more important in the IoT than it is in the Internet, because it is essential for businesses to be able to rely on a stable and foreseeable legal framework. Accordingly, improving accountability by creating such kind of framework plays a crucial role in the improvement of the security in the Internet of Things.

Rolf H. Weber (rolf.weber@rwi.uzh.ch) *Law Faculty of the University of Zurich, Switzerland*, and *Law Faculty of the University of Hong Kong, Hong Kong*.

REFERENCES

- Buchanan A, Keohane RO. The legitimacy of global governance institutions. *Ethics and International Affairs* November 2006; 20(4):405–37.
- De Vey Mestdagh K, Rijgersberg RW. Rethinking accountability in cyberspace: a new perspective on ICANN. *International Review of Law, Computers and Technology*; March 2007; 27–38.
- Drezner DW. *All politics is global, explaining international regulatory regimes*. Princeton/Oxford; 2007.
- Goodhart Ch AE. *Regulating the regulator – An Economist's perspective on accountability and control*. In: Ferran E, Goodhart Ch AE, editors. *Regulating financial services and markets in the 21st century*. Oxford; 2001. p. 151–64.
- Kaufmann Ch, Weber RH. The role of transparency in financial regulation. *Journal of International Economic Law* 13: 2010. pp. 779–797.
- Kleinsteuber HJ. The Internet between regulation and governance. In: Möller C, Amouroux A, editors. *OSCE representative on Freedom of the Media. The Media Freedom Internet Cookbook*. Vienna; 2004. p. 61–75.
- Lastra RM, Shams H. Public accountability in the financial sector. In: Ferran E, Goodhart Ch AE, editors. *Regulating financial services and markets in the 21st century*. Oxford; 2001. p. 165–88.
- Lessig L. *Code and other laws of cyberspace*. New York; 1999a.
- Lessig L. The limits in open code: regulatory standards and the future of the net. *BTLJ* 1999b;14:759–69.
- Liu JP. Legitimacy and authority in Internet coordination: a domain name case study. *Indiana Law Journal* 1999;74:587–626.
- Malcolm J. *Multi-stakeholder governance and the Internet Governance Forum*. Perth; 2008.

- Page A. Regulating the regulator – A lawyer's perspective on accountability and control. In: Ferran E, Goodhart Ch AE, editors. *Regulating financial services and markets in the 21st century*. Oxford; 2001. p. 127–50.
- Tunis Agenda for the Information Society, 2005. <http://www.itu.int/wsis/docs2/tunis/off/6rev1.html>. (accessed 01.12.10).
- Turpin C. Ministerial responsibility. In: Jowell J, Oliver D, editors. *The changing constitution*. 2nd ed. Oxford; 1994. p. 109–51.
- United Nations, Report of the Working Group on Internet Governance, <http://www.wgig.org/docs/WGIGREPORT.pdf>. (accessed 01.12.10).
- Weber RH. *Regulatory models for the online world*. Zürich; 2002.
- Weber RH, Grosz M. Internet governance – From Vague ideas to realistic implementaion. *Medialex* 2007;3:119–35.
- Weber RH. *Shaping Internet governance: regulatory challenges*. Zürich; 2009.
- Weber RH, Weber R. *Internet of Things. Legal Challenges*. Zürich; 2010.
- Young SB. Reconceptualizing accountability in the early nineteenth century: how the tort of negligence appeared. *Connecticut Law Review* 1989;21:197–292.