laws

MDPI

Article

Governance of the Internet of Things—From Infancy to First Attempts of Implementation?

Rolf H. Weber

Faculty of Law, University of Zürich, Rämistrasse 71, 8006 Zürich, Switzerland; rolf.weber@rwi.uzh.ch; Tel.: +41-44-634-4884

Academic Editor: Jacqueline D. Lipton
Received: 29 April 2016; Accepted: 16 June 2016; Published: 24 June 2016

Abstract: In the course of the Internet's growing importance within the last decade, the Internet of Things (IoT) has also been a subject of much debate. Being defined by the International Telecommunication Union (ITU) as the development of item identifications, sensor technologies and the ability to interact with the environment, the term Internet of Things, in more simple words, stands for a technology that is based on the connection of everyday objects to the Internet which exchange, aggregate and process information regarding their physical environment for providing value-added services to end-users. Notwithstanding the extensive research activities having been conducted in the recent past and the broad consensus as to the necessity of a basic normative framework for IoT applications, a final multilateral agreement is still missing. In this respect, an analysis of possible approaches solving the present challenges seems to be worthwhile to conduct.

Keywords: bottom-up approach; dynamic coalition on the Internet of Things; governance structures; Internet of Things (IoT); legal interoperability; multistakeholderism; soft law

1. Introduction

The Internet of Things (IoT) stands for a technology that is based on the connection of everyday objects to the Internet which exchange, aggregate and process information regarding their physical environment for providing value-added services to end-users ([1], p. 2). Being first coined by British technology pioneer Kevin Ashton in 1999 to describe a system in which objects in the physical world could be connected to the Internet through sensors, recently, many definitions of the term IoT have been developed [2]. By way of example, the International Telecommunication Union, a specialized agency of the United Nations, described the IoT in 2012 as being a global infrastructure for the whole information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies ([3], p. 2). However, a standard or universally accepted definition of the IoT does not exist so far.

During the last years, the IoT's scope has been widened and it is now encompassing a broad spectrum of device forms that are used in a number of varying settings such as, among others, in the context of energy, healthcare, transport, and environment. By way of example, prospectively, the refrigerator informs the customer about the products contained or even orders the missing products itself.

The most commonly known usage of the IoT is based on the RFID (radio frequency identification device) technology that aims at preventing the disappearance of goods. However, other forms such as tracking parts through manufacturing processes and measuring variables such as temperature and humidity in a storage facility are common IoT applications as well. In practice, the level of sophistication and the price of RFID can be quite different, starting with the cheap passive device without a power source and limited storage to an active self-powered RFID possessing advanced storage and communication capabilities.

Being "on the threshold of integration into the lives of European Citizens" ([4], p. 3), the IoT is said to have the potential to change the people's lives to a great extent by, among others, helping to simplify human beings' everyday life by controlling stocks and accomplishing orders, monitoring the state of health or protecting the safety of workers, etc. However, the already large volumes of data produced and processed will rise dramatically [5].

2. Research Activities

Within the last years a number of general and sectoral research activities have been conducted. Hereinafter, for example, a summary of the recent activities of the European Commission, the Alliance for Internet of Things Innovation, the European Research Cluster on the IoT, the Federal Trade Commission, the Dynamic Coalition on the Internet of Things, the International Conference of Data Protection and Privacy Commissioners and the Article 29 Data Protection Working Party is provided.

2.1. General Activities

2.1.1. European Commission

Already at an early stage, the European Commission (EC) has been cooperating with both Member States and third countries towards the IoT technology's development and future deployment. In so doing, the EC has been the first supranational organization trying to work out an IoT governance framework by appointing a large group of experts to examine the relevant aspects of a possible IoT governance regime. In that regard, the expert group analyzed in sub-groups several issues of importance in connection with the Internet of Things, namely architecture, identification, privacy and security, standards, and governance as well as ethics.

Subsequently, in order to identify the relevant aspects of an appropriate IoT policy approach including a suitable protection of all EU citizens, the EC conducted a detailed survey in 2012 ([1], p. 2). Having attracted wide interest—altogether more than 600 answers from citizens, civil society organizations, academics and industry players (both ICT and non-ICT) were received (all of them mainly established in the European Union) ([1], p. 2)—the EC published a *Report on the Public Consultation on IoT Governance* in 2013, providing an overview of the answers received [1]. With regard to the security of critical IoT-supported infrastructures, the survey's respondents were of the opinion that the future IoT architecture should be based on reference design principles.

Business organizations and individuals answering the survey agreed to a great extent (66%) on the public sector role being crucial in driving the definition of future IoT architecture's security ([1], p. 20). Besides that, they emphasize the importance of policymakers providing guidance on security-by-design and applicable security technologies ([1], p. 21). Given that IoT services are not yet implemented as part of critical infrastructures, a few answers called for a later statement ([1], p. 7). Concerning the IoT's regulation, about two-thirds of the answerers were of the opinion that the strategies addressed under an IoT governance framework need to be implemented with the development of global standards; these standards' architecture should be influenced by IoT governance ([1], p. 26). In comparison, given that IoT is still in its early stages, less than half of the respondents agreed with the statement that further IoT standardization should be guided by the already existing standardization frameworks ([1], p. 26; [6], pp. 342–43). Following the report's completion, the EC temporarily withdrew from exercising active efforts related to the regulatory framework of the IoT and moved its main attention to issues of security and trust in the Internet ([6], p. 343); for security implications of the IoT see also [5].

Only two years later, in 2015, the EC published a study dealing with IoT and cloud computing [7]. Having investigated the conditions for the European industry to actively participate in the emerging IoT ecosystem's development, this study provides a number of recommendations for the EC, the national governments and large enterprises to meet Europe's IoT-related research and innovation challenges ([7], p. 8). For enabling the emergence of IoT ecosystems supported by open technologies

and platforms [8], the EU announced a Horizon 2020 call for proposals on Internet of Things Large Scale Pilots ending in April 2016. Besides that, the EU organized a series of information events to explain its details [8]. For strengthening the research activities, a further call is foreseen in 2017 [9].

Additionally, for developing and supporting the dialogue and interaction among the various IoT actors, the EC and various IoT players both from the private and public sector initiated the Alliance for Internet of Things Innovation (AIOTI) in March 2015 [10]. The AIOTI's goal is to create a dynamic European IoT ecosystem that unleashes the IoT's potential.

The European Commission's adoption of the "Digital Single Market Strategy for Europe" [11] (DSM) in May 2015 (for more details on the DSM see [12], pp. 1–2), being made up of three policy areas [13] and, among others, consolidating initiatives on security and data protection which are of importance for the IoT technology's adoption, leads Europe a step further in accelerating developments on IoT [14].

2.1.2. Alliance for Internet of Things Innovation

Being open to any entity that accepts the Alliance's terms of reference [15], the AIOTI works towards the creation of a dynamic European IoT ecosystem [10] and aims at setting up a European IoT roadmap until 2020 [16]. The Alliance has been built to assist the European Commission in the development of future IoT standardization policies and is going to build on the work of the later-described IoT Research Cluster (IERC).

In October 2015, the AIOTI published 12 reports [17] having been elaborated by 11 working groups encompassing industry high-level experts, end-users and representatives of societal challenges; these reports include information on a wide range of IoT-related subjects such as applications (AIOTI Working Group 1), standards (AIOTI Working Group 3), policy issues (AIOTI Working Group 4) and smart cities (AIOTI Working Group 8). Following this, in December 2015 the AIOTI announced its long-term strategy to promptly maintain AIOTI as a leading IoT global actor [18].

2.1.3. European Research Cluster on the Internet of Things

Having been founded in 2007 in the course of Europe's effort to develop a future IoT for its businesses and citizens, the European Research Cluster on the Internet of Things (IERC), among others, aims at establishing a cooperation platform, developing a research vision for IoT activities in Europe and becoming a global contact point for IoT research [19]. As to that, the IERC brings together EU-funded IoT projects, coordinates cooperation activities, organizes workshops, etc. Additionally, the IERC has created a number of activity chains to foster the cooperation between the different IoT projects. Addressing the challenges of the different IoT-related topics, various activity chains published position papers in 2015 dealing with the IoT technologies' standardization, IoT governance, privacy issues, and interoperability, among others [20].

2.1.4. Federal Trade Commission

In January 2015, the Federal Trade Commission (FTC) released a Staff Report on the Internet of Things [21] summarizing a workshop that was held in November 2013 to explore privacy and security issues posed by the increasing connectivity of devices both in the consumers' homes and when they are on the move [22]. Despite the technology's tremendous potential to improve the consumers' life in aspects of healthcare, transport, environment and energy, there was broad agreement among the workshop's participants that an increasing connectivity between devices and the Internet is also creating a big number of security and privacy risks ([21], pp. 10–18). Nevertheless, prescriptive regulations are not likely to come from the Federal Trade Commission in a timely manner. Rating the right balance between protecting consumers and optimizing innovation as being the IoT's biggest challenge, the FTC argues in support of companies having strong, voluntary self-regulation and best practices, rather than having the FTC to impose strict standards [23].

2.1.5. International Telecommunication Union

In June 2015, members of the International Telecommunication Union (ITU) established a new expert group being responsible for studies relating to the IoT and its applications, thereby focusing on Smart Cities and Communities (Study Group 20). Later in the year, the ITU and the Georgia Institute of Technology agreed upon the mutual monitoring of global IoT activities and the collaboration on developing standards. Study Group 20 is preparing an extensive report on IoT issues to be published soon.

2.1.6. Dynamic Coalition on the Internet of Things

Set up at the Internet Governance Forum (IGF) in Hyderabad in 2008 to explore the usefulness of IoT devices, the Dynamic Coalition on the Internet of Things (DC-IoT) aims at bringing together all stakeholders for discussing and developing a framework for the Internet of Things [24]. In the course of the IGF in Joao Pessoa in 2015, the DC-IoT published a Draft Statement for Internet of Things Good Practice Policies. Offering a multi-stakeholder approach, the Good Practice Policies highlight the importance of considering ethical aspects when developing IoT devices, services and ecosystems (Internet of Things Good Practice Principle) [25].

Hence, for establishing a free, secure, and enabling rights-based environment, good practices in IoT products require a meaningful transparency to users including an overview on what is tracked and the possibility to turn off individual tracking or alternatively allowing users to control access to their own tracking data. Besides that, the security of individual IoT devices and the compliance with privacy and data protection norms and international law throughout the whole Internet value chain are of importance. For supporting mutual trust among all elements of the IoT ecosystem and therewith promoting the implementation and enforcement of the Good Practice Policies, the recognition of personal needs and a strengthening of both transparency and accountability are needed ([25], chap. 4). The final statement for Internet of Things Good Practice Policies is expected by mid-2016.

2.2. Sectoral Activities

2.2.1. Article 29 Data Protection Working Party

On 16 September 2014, the Article 29 Data Protection Working Party (WP29) (for more information see [26]), consisting of representatives of the national data protection authorities, the European Data Protection Supervisor and the European Commission, published its Opinion on the Internet of Things' recent developments [4]. Taking into account the unpredictability of the IoT's development, the WP29's report focuses on three (already used) categories of IoT devices and combinations therefrom, in particular (i) *wearable computing* referring to sensors, microphones and cameras incorporated in everyday objects such as watches or glasses to extend their functionalities; (ii) *quantified self* dealing with devices used by individuals to record potentially sensitive data about their own physical condition or sporting activities; and (iii) so-called *domotics*, placed on homes or offices, that can be controlled remotely over the Internet (thermostats, washing machines, light bulbs, etc.) ([4], pp. 5–6).

The WP29's Opinion aims at alerting both businesses and customers to the challenges and risks arising from the use of IoT technologies. Already known problems are a lack of control and information asymmetry to the detriment of the users, inadequate user consent, interferences derived from data and repurposing of original processing, intrusive bringing out of behavior patterns and profiling, limitations to remain anonymous online and information security risks ([4], pp. 6–9). To ensure a safe handling with the IoT-technologies, the WP29 provides a number of recommendations for both all stakeholders and device manufacturers ([4], pp. 22–23), application developers ([4], p. 23) and standardization bodies ([4], p. 24), in particular covering, among others, the performance of privacy impact assessments, the deletion of raw data, the comprehensive information of all users and therewith their empowerment for being able to exercise their rights and the application of the principles of Privacy by Design and Privacy by Default ([4], pp. 21–24).

2.2.2. International Conference of Data Protection and Privacy Commissioners

Being the output of the 36th International Conference of Data Protection and Privacy Commissioners [27], the Mauritius Declaration on the Internet of Things of 14 October 2014 [28] emphasizes the IoT's benefits related to healthcare, transportation and energy by also referring to the device's potential to simultaneously disclose large amounts of intimate details without the data subject's content. Therefore, in order to ensure effective data protection measures, the Internet of things' sensor data should be regarded and treated as personal data ([28], p. 1).

The Mauritius Declaration ranks data protection as being a joint responsibility of all actors in society and considers transparency as being of utmost importance; privacy policies of companies offering IoT devices should provide information in a clear and understandable manner ([28], p. 1). Given that data processing starts with the collection of data, the Declaration encourages the development of technologies facilitating new ways to incorporate data protection from the outset and therewith enhancing consumer protection ([28], p. 2). To strike a balance acceptable to all parties, developers, data protection authorities and individuals should engage in active and constructive debates about the IoT's implications ([28], p. 2).

2.3. Interim Conclusion

As set out above, recently the Internet of Things and related aspects have been addressed by various actors and entities having extensively elaborated the IoT technology's benefits and potential risks. Nevertheless, a final multilateral agreement is still missing. Even though the Dynamic Coalition on the Internet of Things Good Practice Policies' publication is imminent, these policies will produce its effects only after the adoption by the entire business economy.

3. IoT Governance Framework

Despite the non-existence of a multilateral agreement, there is broad consensus as to the necessity of a basic normative framework for IoT applications and services. Given that legal fragmentation jeopardizes the successful outlet of the IoT, coherence between different initiatives is advisable. For providing the business community with a stable and predictable environment, legal interoperability as an object must be envisaged and implemented.

3.1. Legal Interoperability as Objective

3.1.1. Avoidance of Business-Detrimental Fragmentation

Recently developed, the term "legal interoperability" addresses the process of making legal rules cooperate across jurisdictions. This objective can be realized in a matter of degrees, as many options exist between a full harmonization of normative rules and a complete fragmentation of legal systems. Given that these two extremes are not reflected in either the law in the books nor in the law in action, the ideal is usually between the two poles, depending on the given circumstances. As is so often the case, striking the correct balance is of importance: while an excessively high level of interoperability would cause difficulties in the management of the harmonized rules and disregard social and cultural differences, a too-low level could present challenges for smooth (social or economic) interaction.

Based on the common understanding of interoperability being a tool to interconnect networks, legal interoperability can facilitate global communication, reduce costs in cross-border business and drive innovation, thereby creating a level playing field for the next generation of technologies and cultural exchange. From a structural perspective, legal interoperability can be implemented by applying a top-down or a bottom-up approach.

3.1.2. Problems of the Top-Down Approach

A top-down approach necessarily requires the establishment of a global agency, for example the United Nations (UN) or any of the UN special organizations, and usually generates the implementation of large bureaucracies ([29], pp. 184–85). With regard to the thematically connected Internet governance, the ITU appears to be the most prominent top-down actor.

However, experience over the last 20 years has shown that the ITU was not able to play an influential role in the governing of the Internet. In addition, as the outcome of the World Conference on International Telecommunications in Dubai showed in December 2012 the attempt to agree by consensus on new rules, not even explicitly related to Internet governance, failed. Furthermore, common visions of global norm-setting did not evolve ([30], pp. 102–3). Accordingly, with regard to the Internet of Things the successful implementation of a top-down approach appears to be unlikely.

3.1.3. Merits of the Bottom-Up Approach

In contrast, a bottom-up process to achieve legal interoperability is based on a step-by-step model encompassing the major entities and persons concerned of the substantive topic in question ([29], p. 185). Exemplary for a successful bottom-up process, the NETmundial, held in Sao Paulo in April 2014, and the IGF of 2015 hosting the Dynamic Coalition on the IoT need to be mentioned, being considered to be the most important events of the recent past. While in the context of the NETmundial conference the various stakeholders had been granted "equal" rights in the negotiation processes of the final non-binding declaration [31], the IGF's activities are gaining influence in the regulatory environment (see above Section 2.1.5).

Generally speaking, a bottom-up process requires a large amount of coordination, but no harmonization or management by central bodies. Hence, coordination processes can be time-consuming and extremely cumbersome. In the past, the bottom-up approach gained increased acceptance and experiences in different forms lead to improved deliberation and decision-making processes. Nevertheless, the normative environment of this approach still needs further elaboration.

3.2. Theoretical Foundations for Normative Models

During the last decade more attention has been paid to the development of theoretical foundations for bottom-up activities. In that regard two main approaches are particularly noteworthy, namely the networks model and mesh regulation.

3.2.1. Networks Model

For overcoming the weakness of the traditional top-down concepts based on sovereign lawmaking, some 10 years ago a legal doctrine started developing conceptual thoughts about the establishment of network structures. In that regard, Raustiala assessed the viability of trans-governmental networks ([32], p. 17). By addressing the fields of securities regulation, competition policy, and environmental regulation, Raustiala exemplified trans-governmental cooperation. Additionally, he emphasized the informal information exchanges among the competent authorities for sector-specific legal rules through the development of a set of direct interactions among sub-units of different governments that are not controlled by the decision-making bodies of the respective States. Although Raustiala's examples do not concern the rule-making needs in the online world, the results drawn by him, namely the acknowledgement of a disaggregation of States in favor of the established networks, also apply to the Internet of Things, i.e., the actual cooperation and solution achievement are based on a framework of "disaggregated sovereignty" ([32], pp. 10, 23–24, 55–56). The networks model's approach could encompass the activities of the Alliance for Internet of Things Innovation, the European Research Cluster on the Internet of Things and the Dynamic Coalition on the Internet of Things (see above Sections 2.1.2, 2.1.3 and 2.1.5).

The most prominent theoretical concept in the networks' discussion has been developed by Slaughter, offering a solution for the "governance dilemma" by referring to "governmental networks" [33] which are set out as "relatively loose, cooperative arrangements across borders between and among like agencies that seek to respond to global issues" ([34], p. 1257). According to Slaughter, governmental networks manage to close gaps through coordination among governments from different States, thereby creating a new sort of power, authority, and legitimacy ([33], p. 14). Stating that national governments cannot effectively address every problem in a networked world and should therefore delegate their responsibilities and "actual sovereign power to a limited number of supranational government officials" ([33], p. 263), Slaughter suggests that the mandated officials would have to engage in intensive interactions and in the elaboration and adoption of codes of best practice and agreements of coordinated solutions to common problems ([33], p. 263).

Looking at the theoretical foundation, networks can be seen as an institutional answer allowing the rationalization of potential conflicts that result from the differentiation and autonomization of systems ([35], p. 159). Law enables the medium "power" to materialize, for example by allocating power to individuals or different governmental authorities, and therewith law has the tendency to support the aforementioned autonomization ([35], p. 413).

The proper functioning of a transnational regulatory network requires the fulfillment of a number of conditions; next to a proper definition of common rules and communication channels and a widely shared regulatory philosophy, a high level of professionalism and a sufficient amount of mutual trust are needed. However, while the networks model has unique benefits, there are also certain drawbacks. The main weaknesses of this approach consist in the lack of political control and the potential democratic deficit. Besides that, there are normative concerns that exist regarding the failure to come to a (formal) legal framework.

A (rudimentary) implementation of the networks model approach can be found at the European Commission's activities (see above Section 2.1.1) and in the context of the Mauritius Declaration on the Internet of Things (see above Section 2.2.2).

3.2.2. Mesh Regulation

Mesh regulation questions the traditional system of law that structures the rule-making authority in the form of a pyramid with the national legislator on top representing the sovereign State. Ost/van de Kerchove justify this shift with the generally acknowledged fact that State sovereignty is not an intangible status anymore. They also point out that the will of the State legislator ceases to be received as dogma, and that powers (State, private enterprises, civil society) need to interact ([36], p. 14). Being of the opinion that a paradigm shift has occurred due to the profound transformation of the State and of modern law in the sense that the pyramidal model with the government at the top is replaced by the network (réseau) model even if some remnants of the old models still exist, Ost/van de Kerchove base their arguments on the insight that in the era of globalization and internationalization, a State's internal legal order cannot survive as a stand-alone solution anymore ([30], p. 93).

The move towards mesh regulation [37] is considered the result of two major transformations in the legal and political landscape, namely (i) the move from the use of the statute as the primary instrument of control to different other forms of regulation and (ii) the increased use of the notion of governance instead of government ([36], pp. 26–32). While the first transformation leads from a centralized sovereign authority to a flexible, decentralized, adaptive and often negotiated regulation ([38], p. 69), the second transformation causes a process that co-ordinates the efforts of actors and social groups not attached to the State or State-owned entities to attain their objectives in fragmented and uncertain environments ([36], p. 29). Thereby, the concept of mesh regulation comes close to Reed's approach of consensus-building by way of communities' understanding ([39], p. 11) or Murray's approach of "network communitarism" being a process of discourse and dialogue between the individual and society ([40], p. 68).

The model of the mesh regulation allows the development of a regulatory environment that encompasses the efforts and activities of all relevant stakeholders concerned. In that regard, reference can be made to last year's general and sectoral activities of the different mentioned bodies (see above Sections 2.1 and 2.2).

3.3. Soft Law Approach as Viable Solution

Due to the fact that traditional legal instruments such as national governmental regulations and international agreements can hardly cope with today's regulatory needs, such as cyberspace, in the recent past the search for alternative rules emerged. As a result, nowadays traditional (hard) law is complemented and partly replaced by so-called "soft law".

The most well-known form of "soft law" is self-regulation. To date, self-regulation exists in many fields, particularly in the media environment and the banking markets.

3.3.1. Characteristics and Merits of Self-Regulation

Being commonly based on the principle of subsidiarity according to which governmental intervention should only take place if participants of a specific community are not able to find suitable solutions themselves, self-regulation emerges in two different characteristics ([41], p. 80), namely as a concept of and initiated by private groups to limit their participants' behavior and as a concept occurring within a framework set by the government (co-regulation, etc.) (See [30], pp. 23–24 for more details). Substantially, each self-regulatory approach requires a specific design depending on the respective problem's nature and the number of participants and can contain either procedural rules or material rules dealing with substantive topics or both kinds of rules ([41], p. 81).

Self-regulation is often used to improve marketing possibilities for enhancing the image of a market segment. Usually, rules created by specific communities' participants respond to real needs. This increases the probability that the rules contain incentives for compliance, mirror the respective technology, provide the opportunity to adapt the regulatory framework to changing technology in a more flexible way and can be implemented at reduced costs ([30], p. 27 with further references and [41], pp. 83–84). However, certain weaknesses of self-regulation mechanisms cannot be overlooked. Next to the uncertainties of the "legislative" procedural quality, among others, resulting from the velocity in which most self-regulation is introduced, the limited transparency within the origination process and the missing involvement of all relevant groups need to be mentioned. The legitimacy of soft law is based on the fact that private incentives lead to a need-driven rule-setting process. However, the large number of "outsiders" or "dark sheep" not acknowledging the validity of the (non-binding) self-regulation lowers the respective rules' legitimacy ([30], p. 28 with further references and [41], pp. 84–85). Therefore, soft-law is justified if it is more efficient than hard law and if compliance with the rules of traditional norm-setters is less likely than compliance with self-regulatory rules ([42], p. 10). Given that multilateral agreements are an illusion, a functioning IoT regulation should be based on soft-law.

3.3.2. Implementation of Multi-Stakeholder Approach

Self-regulation plays an important role in the online world. Today, numerous codes of conduct are available mainly addressed to Internet service providers and search engine businesses (for more details see [43], pp. 112–28). Given that these rules of conduct are generally accepted in the online community, the self-regulatory approach has gained widespread application in the cyberspace environment ([44], p. 511). On that regard, multistakeholderism has become a "buzzword" in many international discussions about regulatory structures without gaining a coherent institutional form ([45], p. 575).

Very originally applied by the International Labor Organization (ILO) in 1919 and later taken up during the sustainability/climate changes debates mainly at the Earth Summit (Rio de Janeiro) in 1992 and in corresponding conferences, the term was particularly coined in the Internet Governance

context. The acknowledgement of the need to have more actors involved in rule-making processes has led to the working definition of Internet Governance referring 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 programs that shape the evolution and use of the Internet" ([46], p. 4). Thereby, the interests of the actors involved should not be defined by any specific group but through participatory mechanisms reflecting the whole society's views ([47], p. 8).

It is recognized today that the involvement of civil society in rule-making procedures can have a legitimizing side effect and allow for better credibility of actions taken by the governing bodies. The participation of the general public in the decision-building efforts, based on adequate transparency mechanisms, strengthens confidence in and accountability of the competent institutions ([48], p. 6). Additionally, the conclusion of new issues, interests, and concerns communicated by civil society can also encourage the governing bodies to look at a specific substantive question from different angles ([48], p. 7). Given the fact that the private sector understands the IoT's problems and difficulties best, its inclusion within the rule-making procedure helps to develop functioning policies for the Internet of Things (critically [5]).

4. Outlook

Without being completely new, the Internet of Things having the potential to change people's lives by simplifying their everyday life is still in its infancy. Even though a number of both general and sectoral research activities have been conducted within the last five years, the implementation of undisputedly necessary appropriate regulatory mechanisms still remains a not yet settled task.

Given that a fragmentation of the normative order jeopardizes the successful outlet of the IoT, a future normative framework should be based on the following legal pillars:

(1) *Legal interoperability*: By facilitating global communication, reducing costs in cross-border business and driving innovation, legal interoperability is adapted for building a stable and predictable IoT environment. Although, from a structural perspective, legal interoperability can be implemented by applying a top-down or a bottom-up approach, with regard to the Internet of Things only the bottom-up approach meets the given requirements. A successful implementation of a top-down approach appears to be very unlikely. The normative environment of the bottom-up approach still needs further elaboration. Additionally, the recently developed networks model and the mesh regulation concept are worth being considered.

(2) *Networks model*: Being understood as an institutional answer to overcome the traditional law-making weaknesses the networks model enables the medium "power" to materialize by allocating power to individuals or to different governmental authorities. The networks model can be found at the European Commission's activities and in the context of the Mauritius Declaration on the Internet of Things.

(3) *Mesh regulation*: The concept of mesh regulation, allowing the development of a regulatory environment encompassing the efforts and activities of all stakeholders concerned, can be found within all of the different bodies' last years' general and sectoral activities. Since the involvement of all stakeholders concerned in rule-making procedures, among others, allows for better credibility of actions taken by the governing bodies, the inclusion of the private sector helps to tackle the IoT's problems and difficulties best.

Acknowledgments: The author would like to thank Ulrike I. Heinrich (attorney-at-law) for her valuable support in the preparation of this article.

Conflicts of Interest: The author declares no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

AIOTI	Alliance for Internet of Things Initiative
DC-IoT	Dynamic Coalition on the Internet of Things
DMS	Digital Single Market Strategy for Europe
EC	European Commission
EU	European Union
FTC	Federal Trade Commission
ICT	information communication technology
IERC	European Research Cluster on the Internet of Things
IGF	Internet Governance Forum
ITU	International Telecommunication Union
IoT	Internet of Things
RFID	radio frequency identification device
WP29	Article 29 Data Protection Working Party

References and Notes

1. European Commission. "Report on the Public Consultation on IoT Governance." 16 January 2013. Available online: https://ec.europa.eu/digital-single-market/en/news/conclusions-internet-things-public-consultation (accessed on 22 June 2016).
2. Kevin Ashton. "That 'Internet of Things' Thing." 22 June 2009. Available online: http://www.rfidjournal.com/articles/view?4986 (accessed on 22 June 2016).
3. ITU. "Overview of the Internet of things: Next Generation Networks—Frameworks and functional architecture model." June 2012. Available online: https://www.itu.int/rec/T-REC-Y.2060-201206-I (accessed on 22 June 2016).
4. Article 29 Data Protection Working Party. "Opinion 8/2014 on the Recent Developmepnts on the Internet of Things." 16 September 2014. Available online: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf (accessed on 22 June 2016).
5. With regard to therewith connected cybersecurity in the IoT see Rolf H. Weber, and Evelyne Studer. "Cybersecurity in the Internet of Things: Legal Aspects." *Computer Law & Security Review*, 2016, forthcoming.
6. Rolf H. Weber. "Internet of Things—Governance quo vadis?" *Computer Law & Security Review* 29 (2013): 341–47. [CrossRef]
7. European Commission. "Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination." 13 May 2015. Available online: https://ec.europa.eu/digital-single-market/en/news/definition-research-and-innovation-policy-leveraging-cloud-computing-and-iot-combination (accessed on 22 June 2016).
8. European Commission. "Horizon 2020 Work Programme 2016–2017: Internet of Things Large Scale Pilots." Available online: https://ec.europa.eu/digital-single-market/en/news/horizon-2020-work-programme-2016-2017-internet-things-large-scale-pilots (accessed on 29 April 2016).
9. European Commission. "Topic: R&I on IoT integration and platforms." Available online: http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/2221-iot-03-2017.html (accessed on 29 April 2016).
10. European Commission. "The Alliance for Internet of Things Innovation (AIOTI)." Available online: https://ec.europa.eu/digital-single-market/en/alliance-internet-things-innovation-aioti (accessed on 29 April 2016).
11. European Commission. "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, a Digital Single Market Strategy for Europe." 6 May 2015. Available online: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=DE (accessed on 22 June 2016).
12. Rolf H. Weber. "Legal Interoperability as a Tool for Combatting Fragmentation." Paper Series: No. 4, Global Commission on Internet Governance, Waterloo, ON, Canada, December 2014. Available online: https://www.cigionline.org/sites/default/files/gcig_paper_no4.pdf (accessed on 22 June 2016).
13. European Commission. "Digital Single Market." Available online: https://ec.europa.eu/priorities/digital-single-market_en (accessed on 29 April 2016).

14. European Commission. "The Internet of Things." Available online: https://ec.europa.eu/digital-single-market/en/internet-things (accessed on 29 April 2016).
15. European Commission. "Alliance for Internet of Things Innovation Terms of Reference." 25 March 2015. Available online: https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/alliance_for_internet_of_things_innovation_terms_of_reference.pdf (accessed on 29 April 2016).
16. European Commission. "'AIOTI is a successful European IoT stakeholder forum. Now it is the time to move forward': 2nd AIOTI General Assembly Meeting's main conclusion." Available online: https://ec.europa.eu/digital-single-market/en/news/aioti-successful-european-iot-stakeholder-forum-now-it-time-move-forward-2nd-aioti-general (accessed on 29 April 2016).
17. European Commission. "AIOTI Recommendations for future collaborative work in the context of the Internet of Things Focus Area in Horizon 2020." Available online: https://ec.europa.eu/digital-single-market/news/aioti-recommendations-future-collaborative-work-context-internet-things-focus-area-horizon-2020 (accessed on 29 April 2016).
18. European Commission. "Alliance for Internet of Things Innovation (AIOTI) defines its long term strategy." Available online: https://ec.europa.eu/digital-single-market/en/news/alliance-internet-things-innovation-aioti-defines-its-long-term-strategy (accessed on 29 April 2016).
19. European Research Cluster on the Internet of Things (IERC). Available online: http://www.internet-of-things-research.eu/about_ierc.htm (accessed on 29 April 2016).
20. IERC. "Documents and Publications." Available online: http://www.internet-of-things-research.eu/documents.htm (accessed on 29 April 2016).
21. Federal Trade Commission. "Internet of Things—Privacy and Security in a Connected World—FTC Staff Report." Available online: https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf (accessed on 29 April 2016).
22. FTC. "Internet of Things—Privacy and Security in a Connected World." Available online: https://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-security-connected-world (accessed on 29 April 2016).
23. Chase Gunter. "FTC in no rush to regulate Internet of Things." *FCW*, 9 February 2016. Available online: https://fcw.com/articles/2016/02/09/gunter-ftc-iot-regs.aspx (accessed on 22 June 2016).
24. Dynamic Coalition on the Internet of Things (DC-IoT). "What is DC IoT." Available online: http://www.iot-dynamic-coalition.org/about-us/ (accessed on 29 April 2016).
25. Dynamic Coalition on the Internet of Things (DC-IoT). "Internet of Things Good Practices." Available online: http://review.intgovforum.org/igf-2015/dynamic-coalitions/dynamic-coalition-on-the-internet-of-things-dc-iot-4/ (accessed on 29 April 2016).
26. European Commission. "Article 29 Working Party." Available online: http://ec.europa.eu/justice/data-protection/article-29/index_en.htm (accessed on 29 April 2016).
27. In that regard, the author gave a presentation on the IoT's basic principles. His remarks dealing with challenges posed by the IoT and the growing need for appropriate regulatory as well as technical action for bridging the gap between the automated surveillance by IoT services and the rights of the individual consumers who are often unaware of the potential risk to which they are exposed has later been published in Rolf H. Weber. "Internet of things: Privacy issues revisited." *CLSR* 31 (2015): 234–42. [CrossRef]
28. Jacob Kohnstamm, and Drudeisha Madhub. "Mauritius Declaration on the Internet of Things." Available online: http://www.privacyconference2014.org/media/16596/Mauritius-Declaration.pdf (accessed on 29 April 2016).
29. John Palfrey, and Urs Gasser. *Interop: The Promise and Perils of Highly Interconnected Systems*. New York: Basic Books, 2012.
30. Rolf H. Weber. *Realizing a New Global Cyberspace Framework—Normative Foundations and Guiding Principles*. Zurich: Schulthess and Springer, 2014.
31. Global Multistakeholder Meeting on the Future of Internet Governance (NETmundial). "NETmundial. Multistakholder Statement." Available online: http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf (accessed on 29 April 2016).
32. Kal R. Raustiala. "The Architecture of International Cooperation: Transgovernmental Networks and the Future of International Law." *Virgina Journal of International Law* 43 (2002): 192. [CrossRef]

33. Anne-Marie Slaughter. *A New World Order*. Princeton: University Press Group, 2004.
34. Kenneth Andersen. "Book Review: Squaring the Circle? Reconciling Sovereignty and Global Governance through Global Government Network." *Harvard Law Review* 118 (2005): 1255–312. [CrossRef]
35. Gunther Teubner. *Constitutional Fragments: Societal Constitutionalism and Globalisation*. Oxford: Oxford University Press, 2012.
36. François Ost, and Michel van de Kerchove. *De la pyramide au réseau? Pour une théorie dialectique du droit*. Bruxelles: Publication des Facultés universitaires Saint-Louis, 2002.
37. The term mesh is also used in the networks theory describing the creation of a local networking that perches small routers throughout the area to produce a mesh.
38. Emily M. Weitzenboeck. "Hybrid net: The regulartory framework of ICANN and the DNS." *International Journal of Law and Information Technology* 22 (2014): 49–73. [CrossRef]
39. Chris Reed. *Making Laws for Cyberspace*. Oxford: Oxford University Press, 2012.
40. Andrew Murray. *Information Technology Law: The Law and Society*. Oxford: Oxford University Press, 2012.
41. Rolf H. Weber. *Regulatory Models for the Online World*. Zurich: Schulthess, 2002.
42. Rolf H. Weber. "Overcoming the Hard Law/Soft Law Dichotomy in Times of (Financial) Crises." *Journal of Governance and Regulation* 1 (2012): 8–14.
43. Damian Tambini, Danilo Leonard, and Chris Marsden. *Codifying Cyberspace: Communications Self-Regulation in the Age of Internet Convergence*. London: Routledge, 2008.
44. Llewellyn J. Gibbons. "No Regulation, Government Regulation, or Self-Regulation: Social Enforcement or Social Contracting for Governance in Cyberspace." *Cornell Journal of Law and Public Policy* 6 (1997): 475–551.
45. Mark Raymond, and Laura DeNardis. "Multistakeholderism: Anatomy of an inchoate global institution." *International Theory* 7 (2015): 572–616. [CrossRef]
46. Working Group on Internet Governance. "Report of the Working Group on Internet Governance." June 2005. Available online: http://www.wgig.org/docs/WGIGREPORT.pdf (accessed on 22 June 2016).
47. Rolf H. Weber. "Future Design of Cyberspace Law." *Journal of Politics* 5 (2012): 1–14.
48. Rolf H. Weber. "Shift of legislative powers and multi-stakeholder governance." *International Journal of Public Law and Policy* 1 (2011): 4–22. [CrossRef]