The Internet of Things in a Smart Society: How Government Policy Can Help Seize Opportunities and Mitigate Threats

Ronald Pool, Jasper van Berkel, Susan van den Braak, Maaike Harbers, and Mortaza S. Bargh

Abstract The IoT is a revolutionary development for both society and governments. In this chapter opportunities and threats of the IoT are discussed. Linking technological, societal, economic, and policy-oriented aspects of the IoT, this chapter introduces a conceptual framework to map and analyze the factors or obstacles that arise in addressing IoT opportunities and threats, and possible government measures to mitigate these factors. By adopting a broad view and paying attention to the relations between different factors, this chapter shows that there is no one-size-fits-all solution for IoT-related issues, as different problems and solutions are interdependent and require a coherent government approach.

Keywords Internet of Things · Opportunities · Threats · Human and societal values · Government measures

R. Pool
ICTRecht, Amsterdam, The Netherlands
e-mail: r.pool@ictrecht.nl

J. van Berkel · S. van den Braak (✉)
Research and Documentation Centre, Ministry of Justice and Security, Den Haag, The Netherlands
e-mail: j.j.van.berkel@minvenj.nl; s.w.van.den.braak@minvenj.nl

M. Harbers
Research Centre Creating 010, Rotterdam University of Applied Science, Rotterdam, The Netherlands
e-mail: m.harbers@hr.nl

M. S. Bargh
Research and Documentation Centre, Ministry of Justice and Security, Den Haag, The Netherlands

Research Centre Creating 010, Rotterdam University of Applied Science, Rotterdam, The Netherlands
e-mail: m.shoae.bargh@minvenj.nl; m.shoae.bargh@hr.nl

© Springer Nature Switzerland AG 2020

J. R. Gil-Garcia et al. (eds.), *Beyond Smart and Connected Governments*, Public Administration and Information Technology 30,
https://doi.org/10.1007/978-3-030-37464-8_2

Abbreviations

CE	Conformité Européenne
CLTC	Center for Long-term Cybersecurity
GDPR	General Data Protection Regulation
IoT	Internet of Things
ISO	International Organization for Standardization
IT	Information technology
R&D	Research and development
SWOT	Strengths, weaknesses opportunities, threats

Introduction

The Internet of Things (IoT) will play an increasingly prominent role in everyday life. It is estimated that the IoT will contain 20–30 billion objects in 2020 (Gartner 2015; WEF 2015), where "objects" can range from toothbrushes and lamps to animals and humans (with implants), from cars and houses to energy networks and cities. It will therefore have a major impact on many aspects of society, such as employment, healthcare, transportation, and prosperity (Atzori et al. 2010; Borgia 2014; Whitmore et al. 2015; Al-fuqaha et al. 2015).

Technological developments, such as the IoT, will also influence governments and public policy (GO-Science 2014). With an increasing amount of connected devices containing sensors, more and more data will be collected and exchanged. As a result, more relevant and real-time information will be available (Whitmore et al. 2015). By combining, analyzing, and interpreting these data, processes can become more transparent and new insights can be obtained. This can help governments to make better and more informed decisions.

The use of technologies to facilitate government activities has long been discussed, using concepts such as e-government, digital government, and smart government (Layne and Lee 2001; Moon 2002; West 2004; Gil-Garcia et al. 2014; Janowski 2015). The scope of each concept differs. Some authors limit the scope to the use of technology for daily public administration (Moon 2002) or to government services delivered by digital means (West 2004). In a broader sense, it could be seen as a "creative mix of emergent technologies and innovation in the public sector" (Gil-Garcia et al. 2014: 17).

Regardless of the scope, it is clear that the IoT will influence these concepts. This chapter uses a scheme of human and societal values, as a way to address the opportunities and threats of the IoT. It should be noted that the notion of values has been used as a framework of categorization and should not be interpreted as a theoretical approach. The starting point of our categorization was the idea that technology has an impact on human values (Friedman et al. 2013). Some values are positively affected by the IoT and others are negatively affected, constituting both opportunities

and threats. The public sector plays a vital role in seizing these opportunities and mitigating the threats. In this chapter we offer a conceptual framework for understanding, framing, and approaching the factors that arise in addressing both opportunities and threats.

The outline of the chapter is as follows. Section "Related work" discusses related work on opportunities and threats of the IoT in specific domains and IoT regulation. Section "Approach" discusses our approach and methodology. Section "IoT Opportunities and Threats" provides an overview of the opportunities and threats posed by the IoT. Section "Government Measures" introduces a conceptual framework including factors and government measures for addressing the opportunities and threats. Section "Conclusion" provides a conclusion.

Related Work

This chapter aims to provide a broad overview of IoT-related issues, including its opportunities and threats, possible measures that allow society to benefit from the IoT, and the role of the public sector in particular. While doing so, the chapter brings together scientific research, professional literature, news articles, and expert opinions. This wide perspective distinguishes this work from most other contributions on this topic, which often concentrate on a specific application domain or a narrower problem related to the IoT. Related work focuses on, for example, opportunities and challenges of the IoT in healthcare (Fernandez and Pallis 2014) and industries (Da Xu et al. 2014), security concerns (Sicari et al. 2015; Xu et al. 2014), privacy concerns (Sicari et al. 2015), or issues in relation to big data (Sun et al. 2016). There are a number of papers that discuss the opportunities and threats of the IoT in general (e.g., Davies 2015; Rose et al. 2015), but these only shortly discuss the possible measures needed for overcoming the challenges and supporting the opportunities.

Besides having a broader focus, this chapter distinguishes itself from other contributions by providing an analysis of the obstacles that hinder the implementation of IoT-related measures to seize opportunities or mitigate threats. Other institutes (GO-Science 2014; CSR 2016a) published their reports proposing some measures for mitigating IoT challenges. However, they fail to explicate the relations between different measures and the relations of those measures to the fundamental obstacles in implementing them. The obstacles that are discussed in this chapter are brought up in some other papers as well. For example, Danezis et al. (2014) and Peppet (2014) mention some obstacles like lack of governance, incentives, and knowledge. However, they neither provide the relations between different obstacles nor between obstacles and solution directions.

This work is one of the few that links technological, societal, economic, and policy-oriented aspects of the IoT. By adopting a broad view and paying attention to the relations between different issues, this chapter shows that there is no one-size-fits-all solution for IoT-related issues, as different problems and solutions are

interdependent and require a coherent approach. Our work has focused on the situation in the Netherlands, but we expect that many of the findings are applicable to other (developed) countries as well.

Approach

The research presented in this chapter was performed in two phases. First, we made an overview of the opportunities and threats of the IoT. Second, we investigated which measures need to be taken to seize these opportunities and mitigate the most important threats. In this process, we used the notion of "values" as a conceptual tool for mapping, describing, and analyzing the opportunities and threats, and determining which measures to take. Again, it is important to note that these "values" are not used as a theoretical foundation for analyzing the opportunities and threats.

This approach is founded on the idea that people's values guide what they consider important in life, what judgments they make about the world, and how they act in specific situations. Likewise, in governance, all policy decisions are underpinned by values, even though they often remain implicit (Chang 1997; Kooiman and Jentoft 2009). It has been argued that making values explicit can help making policy decisions. Song and colleagues, for example, state that "governance challenges could be lessened if stakeholders' values, images, and principles are made explicit, understood, and articulated into the policy and decision-making process" (Song et al. 2013: 1). The concept of responsible innovation (adopted, among others, by the European Commission), which looks at the potential impact on society and environment of an innovation process, also takes values into account (Stilgoe et al. 2013). For these reasons, we deemed the framework of values suitable to map the opportunities and challenges of the IoT.

In the first phase of our research we assessed which human and societal values are affected most by the rise of the IoT. Generally, technological developments have both positive and negative impacts, constituting opportunities and threats, respectively. For example, a smart grid can decrease energy consumption and thus support the value of sustainability—an opportunity. Yet the smart meters needed for such a solution may violate one's privacy—a threat.

We collected information about values and the IoT through the following methods: (1) desk research, (2) interviews, and (3) roundtable discussions. Desk research was performed using a selection of fixed search terms to search for available scientific literature in Google Scholar. Based on these initial results we expanded our search by using a snowball method, which enabled us to find additional literature that seemed relevant for our study. As many of the developments are recent and new we also included media articles in our literature survey. Next to the desk research, two themed roundtables were organized to discuss Smart Cities and Smart Industry using a SWOT analysis. To supplement these findings a total of six semi-structured interviews were conducted with various experts and stakeholders from different sectors. We used the results from this research to categorize the potential positive

and negative effects of the IoT according to the "value at stake," giving priority to those effects that were mentioned multiple times. This resulted in a list with positively affected values—opportunities, and a list with negatively affected values—threats, as described in Section "IoT Opportunities and Threats". It is important to note that these lists are by no means exhaustive, but rather, form a useful taxonomy to describe the societal and economic opportunities and threats of the IoT.

In the second phase, the most important opportunities and threats identified in the first phase were taken as a starting point to identify measures for seizing and mitigating them. They were selected from all measures that came up in the desk research, interviews and roundtables. Again, we paid attention to those measures that were emphasized or mentioned multiple times. We also identified the possible relations and interdependencies between different measures and their corresponding solution directions. This phase resulted into two insightful diagrams that also illustrate the relations among the various measures (see Section "Government Measures").

IoT Opportunities and Threats

This section presents the positive and negative effects of the IoT on different human and societal values in Sections "IoT Opportunities" and "IoT Threats", respectively.

Opportunities

As is discussed in the introduction, data produced and exchanged by the IoT can improve understanding and transparency, which can contribute to better decisions by businesses and governments. As a result, the IoT can have a strong positive impact on the following values: well-being, sustainability, productivity and prosperity, which prominently arose in our desk research and interviews. The positive impact of the IoT on these values is discussed below.

Well-Being

The IoT can contribute to well-being in several ways. Firstly, it can improve quality of life by automating processes in daily life. IoT applications can make cities more accessible and more attractive to citizens by, for example, optimizing the flow of traffic, monitoring the availability of parking spaces, and improving garbage disposal routes (Miorandi et al. 2012; Pandya & Champaneria 2015; Whitmore et al. 2015; Zanella et al. 2014). Secondly, it can be used to improve the health of users. Wearables, for instance, can help people to adopt a healthy lifestyle by improving their movement, sleeping and eating patterns (Beaudin et al. 2006; Kong et al. 2012;

Silver et al. 2012; Swan 2013). The IoT can also assist people with a visual, auditory, or physical impairment (Domingo 2012), or the IoT devices can be used to monitor at-risk patients (Healey et al. 2015). Finally, it can contribute to well-being by making people's surrounding and the public domain safer. The IoT can monitor homes and detect break-ins, smoke, or flooding. The same sensors could also be used in the public domain and assist law enforcement (Farooq et al. 2015; Miorandi et al. 2012). Smart lampposts could, for example, detect noise and possible criminal behavior.

Sustainability

The IoT can help sustainability in several ways. Firstly, applications in homes provide ways for consumers to save on energy and water usage. Smart meters and thermostats provide real-time feedback on energy usage, and they can automatically adjust heating. Secondly, IoT applications in cities can provide insight into the energy use of public services, and help to optimize it (Zanella et al. 2014). IoT sensors can also monitor the air quality in cities (Farooq et al. 2015; Miorandi et al. 2012; Zanella et al. 2014) and based on that, for example, automatically redirect cars when certain limits are exceeded. Thirdly, energy networks can be turned into smart grids by embedding sensors in them, increasing their efficiency, security, and reliability (Wang et al. 2012; Yan et al. 2013; Borgia 2014). Smart grids make it possible to detect malfunctions in the network at an earlier stage, and to better balance the supply and demand of energy. Increasingly, this will also extend to homes, for example, by temporarily storing and discharging energy in electric cars, depending on the needs of the network (Yan et al. 2013). Lastly, the IoT could also contribute to the circular economy by providing insight in the use of energy and resources during the lifetime of a product (Ellen MacArthur Foundation 2016). In the wake of the Paris climate agreements, this can contribute to achieving their objectives.

Productivity

The IoT can increase productivity by making predictions, optimizing processes and taking decisions. A few examples of applications in logistics, manufacturing, and agriculture are discussed below. In the logistics sector, RFID chips are used to track products through the entire supply chain. This helps optimizing the supply chain, for example, by maintaining smaller inventories (Atzori et al. 2010; Whitmore et al. 2015). Manufacturing processes can also be optimized through real-time access to information (Atzori et al. 2010; Stratix 2015), for instance by performing preventive maintenance (Atzori et al. 2010; Al-Fuqaha et al. 2015; Borgia 2014). In agriculture, the IoT can advance precision agriculture, in which crops and animals are closely monitored and treated. It can monitor soil and crop properties, weed densities, and diseases and pests (Bos and Munnichs 2016). Livestock farmers can also use the IoT to monitor the performance of animals individually, for example with

respect to milk yields, fertility and possible diseases (Bos and Munnichs 2016). It is expected that IoT use will be vital for companies and countries to stay competitive in the future.

Prosperity

Estimations of the potential economic impact of the IoT range from $1.9 trillion to as much as $14.4 trillion annually (Bradley et al. 2013; Lund et al. 2014; Manyika et al. 2013; GO-Science 2014). Despite this discrepancy in predictions it is clear that the IoT will have a big impact on the economy. In part, this will be due to the availability of a whole range of physical IoT products (e.g., sensors) that provide opportunities for companies to innovate and develop new products. Besides that, the IoT will impact services. IoT products, data and software will be sold as a service by offering subscription-based access to products, data and software (Castermans et al. 2014; CPB and PBL 2015; Frenken 2015). Many physical IoT products will be accompanied with complementary services. For example, some smart thermostats already come with services that give users additional information on how to optimize their energy usage. Finally, the IoT will improve existing services, for example, by offering preventive maintenance (Smit et al. 2016), by giving personalized offers, or by providing information about product availability to consumers in stores (Gregory 2015). Traditional business models of one-off deals are thus transformed into a situation in which products generate revenue over their entire lifetime.

The IoT will also have a big impact on the job market. Historically, technological revolutions have been positive for the job market. Although certain types of jobs disappeared, technological developments have also created new jobs (Van Est and Kool 2015; Went and Kremer 2015). Such a shift offers opportunities for people and businesses with the right expertise. With an aging population and a shrinking workforce, the IoT offers opportunities to maintain economic growth by replacing certain jobs (as demand for labor exceeds supply), and by improving labor productivity, often seen as an important prerequisite for economic growth (Van Est and Kool 2015).

Threats

The previous section described various opportunities and possibilities that the IoT offers by collecting large amounts of (sensor) data. However, collecting such large amounts of data and increasing the use of connected devices also have a downside. This section will describe how the following values, as identified in our desk research and interviews, are threatened by the advent of the IoT. These values are security and safety, privacy, prosperity, well-being, equality, and autonomy.

Security and Safety

As the number of objects connected to the IoT increases, so too will the number of security and safety risks and their impacts. Therefore, lack of an adequate level of security and safety is one of the main concerns regarding the IoT (Goodman 2015; FTC 2015; Peppet 2014). A security risk is an intentionally caused risk, for example, the risk associated with a system attack carried out intentionally by malicious people (Aoyama et al. 2013). Security risks affect the confidentiality, integrity, and availability of devices (Mattord 2014). For example, by rendering the device unavailable with ransomware (Goodman 2015; Williams 2016) or affecting its integrity by adjusting or deleting sensor data (Koebler 2015).

Safety risks, on the other hand, occur due to, for example, human errors, design errors, or malfunctions without explicit intentions (Aoyama et al. 2013). These risks can be caused by faulty hardware, such as malfunctioning sensors, glitches in the underlying infrastructure, or emergent behavior between interconnected devices (Roca et al. 2016).

At this point in time, it is noteworthy that few mitigation measures are being taken to reduce security and safety risks. Moreover, basic security measures like avoiding default usernames and passwords are often not taken by companies, making hacking of IoT devices considerably easier. For example, the Mirai botnet consisted of thousands of IoT devices that were hacked because of this vulnerability (Krebs 2016). Because of the disruptive impact that insecure or unsafe devices will have on society, taking security and safety measures will become an increasingly important policy topic.

Privacy

As described above, IoT applications collect large amounts of data. These data can often be traced back to specific people and their use may violate these people's privacy. The anonymization of personal data collected by IoT devices proves to be problematic (Peppet 2014). Moreover, by combining and editing apparently "innocent" data, sometimes new sensitive personal data can be created (Rose et al. 2015; Hildebrandt 2008; WRR 2016). For example, combining and analyzing data on heart rate and acceleration can result in data on stress levels, happiness, or overall health of users (Peppet 2014).

Another privacy-related risk is automated decision-making based on sensor data. Several authors point out that this could lead to social exclusion and discrimination (Custers et al. 2013; Peppet 2014; Zarsky 2014, 2016). Furthermore, data collected could end up being used for different IoT applications, without people being aware of it (WRR 2016). The IoT also offers opportunities for government agencies to collect data (Ackerman and Thielman 2016). IoT applications enable continuous monitoring of individuals and therefore are particularly suited for police surveillance and spying purposes. For example, through microphones in CCTV cameras, an act of aggression can be identified using special software (Flight 2016). It is also possible for a retailer

to count the number of people by measuring Wi-Fi and Bluetooth signals (WRR 2016). The above applications may violate the right to privacy in a variety of ways and could have a "chilling effect," as people tend to adjust their behavior according to a new (or alleged) measure (Kaminski and Witnov 2015).

Current legislation in Europe, such as the General Data Protection Regulation (GDPR) requires the purpose of data processing to always be clear in advance. However, for IoT applications this has proven not to be the case. This could lead to a "function creep," where data is used for a different purpose than it was originally collected for (WRR 2016). Furthermore, many applications will use big data analyses, in which generally all available data are analyzed and the outcome of the analysis is often not clear in advance (Zwenne 2015). Lastly, informed consent will be challenged as devices without a screen make it difficult for users to view the privacy settings (Peppet 2014) and to allow unequivocal permission for data processing (Zwenne 2015). Above examples show that the IoT will introduce many potential privacy issues that will need to be addressed in the future.

Prosperity

Over the past twenty years, technological developments have contributed significantly to prosperity and economic growth (Van Est and Kool 2015). While opinions on the relationship between employment and the robotization of society differ (Van Est and Kool 2015; Arntz et al. 2016), it is clear that technological advancements are likely to affect both job market and business competitiveness. The IoT creates new markets and opportunities, but if companies fail to respond in time, they may no longer be able to compete with international companies. Some companies have difficulty responding to the new "online reality," which, with the advent of the IoT, is about to increase even more. These digital platforms are new technology-driven business models, often with a winner-takes-all mentality (Van Est and Kool 2015; Bijlsma et al. 2016). Emerging IoT-enabled services may diminish the market share of those players that do or cannot timely embrace the opportunities. Some authors (Van Est and Kool 2015; Bijlsma et al. 2016) warn that these digital platforms may lead to the so-called platform capitalism, in which one or two parties are dominant in a certain sector. Related to this, a lack of standards for IoT services and systems affects the interoperability and durability of IoT devices and services. There is a risk that IoT devices that are purchased now will become unusable because the existing specifications are no longer supported. This problem plays on an international level and therefore requires collaboration between governments on a global scale. In this global context, it is noteworthy to mention the development of standards for smart cities with the ISO 37120:2014.[1] This is the first ISO standardization of city data, defining 100 city performance indicators. Measuring the performance of a city can be seen as a fundamental aspect of a smart city.

[1] https://www.iso.org/standard/62436.html.

Well-Being

Technological advancements of the IoT can threaten the general well-being of our society in a number of ways. Firstly, as the IoT collects large amounts of data, people have access to and also share a lot of information. To make sure all this information does not overwhelm its users, IoT applications also help to process and interpret it. To that end, Weiser and Seeley-Brown (1995) suggest that "the way to become attuned to more information is to attend to it less". When IoT applications fall short in this regard, it could lead to an information overload, concentration issues and stress (Wurman 1989), as people have difficulties handling large amounts of information (Bawden and Robinson 2009).

Secondly, autonomous devices may limit our freedom of choice. Advanced algorithms can, for instance, determine when to turn on your lights or central heating systems, and how to drive your car to a specific destination. Consequently, it becomes more difficult for users to influence the system's decisions (Amichai-Hamburger 2002) and to completely evade IoT applications and not share personal information (Peppet 2014).

Lastly, the rapid growth of the IoT comes with some new developments of which the effects are not yet fully known. One of these developments is the fact that technology can have a negative impact on social interactions. In literature it is argued that with increased use of technology, morality is divided between humans and technology (Van den Berg and Keymolen 2013). This could lead to a reduction of critical reflection on our actions and a reduced moral awareness of people (Keymolen 2014). Technology philosophers also point out that people are becoming increasingly fused with technology, which fades the boundary between human and technology (Floridi 2015; Verbeek 2011).

Government involvement may contribute to emphasizing the importance of this human value in societal development.

Equality

Technological progressions have led to a gap between those who can benefit from digital technologies and those who cannot (Norris 2001), which can result in impending equality. The arrival of the IoT threatens to increase the digital divide. Those individuals who cannot benefit from new technologies are subjected to the increasing threat of being excluded from (public) services because they are unable to use digital resources (effectively). For example, it is plausible that insurance premiums would go down for people with a smart home or smart car in the near future. Furthermore, some warn that certain areas or neighborhoods not connected to the IoT will run the risk of being excluded from certain public services (CLTC 2016). Lastly, economical changes could also lessen equality in the workforce when it comes to salary, working conditions, and job opportunities (Roose 2014; Van Est and Kool 2015).

Autonomy

The more dependent society is on technology, the greater are the consequences of technological failures. This increasing reliance on technology, which is enhanced by the rise of the IoT, poses a threat to our autonomy in several ways. Firstly, it creates a risk of failure of IoT devices due to Internet and power outage, or due to an overload of communication networks. Infrastructure failures will affect an increasing number of devices and technologies. Secondly, with an increased reliance on technology, knowledge, and skills could be lost as they are no longer needed. This, in turn, increases the impact of possible technological failures (Pereira et al. 2013; Lu 2016).

In addition to the risk of technical malfunctions, a growing IoT also creates new dependencies on manufacturers. This can cause safety hazards, for example, because software and hardware vulnerabilities/leaks are no longer patched. The dependency on manufacturers may also harm national interests. The CLTC (2016) outlines a future in which countries nationalize IoT production to counter potential spying or tampering efforts from other countries. The CLTC predicts that a number of large networks will emerge from countries such as China and the United States. Small countries in particular will have to choose which area of influence they want to belong to. This raises all kinds of questions about, for example, the impact these countries will have on the produced (privacy-sensitive) data, and the role governments should play in this process.

Summary and Analysis

The previous sections have shown that the IoT will have a big impact on our society, with both positive and negative consequences for different human values. The extent to which these consequences will affect society depends on the ways in which the IoT will be used, developed, and regulated. As these human values are closely aligned with public policy goals, IoT developments should be taken into account when creating (new) policy.

Considering all values that are positively affected by the IoT, we see IoT-driven economic growth as the biggest opportunity of the IoT because it will have the biggest impact on society. It affects many of the values discussed in Section "Opportunities", which, in turn, also contribute to economic growth. For example, sustainability benefits not only the environment but also the economic growth, by offering new sustainable products and services. The IoT can also help to lower costs because, for example, the elderly can live at home longer or because healthcare costs decrease.

Regarding threats, we consider risks related to cybercrime (security), dysfunctional IoT devices (safety), and the invasion of privacy as the biggest threats. To a certain extent, this also relates to the other values discussed in Section "Threats". Government policy can play a more significant role in the values of prosperity and

the loss of autonomy; where the negative consequences of something going wrong will grow as we get more dependent on technology.

Lastly, it is important to note that not addressing the opportunities or threats can lead to physical, social, or economic damage. However, when both the opportunities and threats are addressed, it can positively affect economic growth and other values. Thus, there is a positive interaction between stimulating economic growth and taking security measures. This means that only focusing on one aspect will limit the potential benefits the IoT can have.

Government Measures

Although businesses are mainly in a leading position to take initiatives for seizing IoT opportunities and mitigating its threats, governments can encourage companies to take actions through policies. In fact, in this section we will show that the government plays a crucial role in ensuring a profitable and safe IoT. An overview of possible government measures to stimulate economic growth, as the main positive consequence of the IoT, and mitigate security, safety, and privacy risks, as the main negative consequences of the IoT, is provided below.

Economic Growth

Figure 1 shows a summary of the factors and the associated (government) measures that can positively affect economic growth. These *factors* (dark grey blocks) can be divided into (1) boosters of economic growth and (2) conditions for economic growth, as indicated in Fig. 1. This classification is based on a conceptual model of Statistics Netherlands (CBS 2013). In this section we use this model to discuss *measures* (light grey blocks) that can contribute to economic growth due to the IoT. The figure shows that preventing security and privacy-related risks is an important requirement for promoting economic growth. Measures to mitigate these risks are discussed in Section "Security, Safety and Privacy".

Human Capital and Workforce

Human capital and workforce are associated with knowledge and skills of the workforce (CBS 2013). The IoT as well as the further digitization of the economy requires a workforce with sufficient IT skills. This also applies to businesses and governments, which need sufficient knowledge to develop new products, services, and policies. Previous research shows that there is currently a shortage of IT knowledge in the country's workforce as well as in organizations (Van Lakerveld et al. 2014; SER 2016).

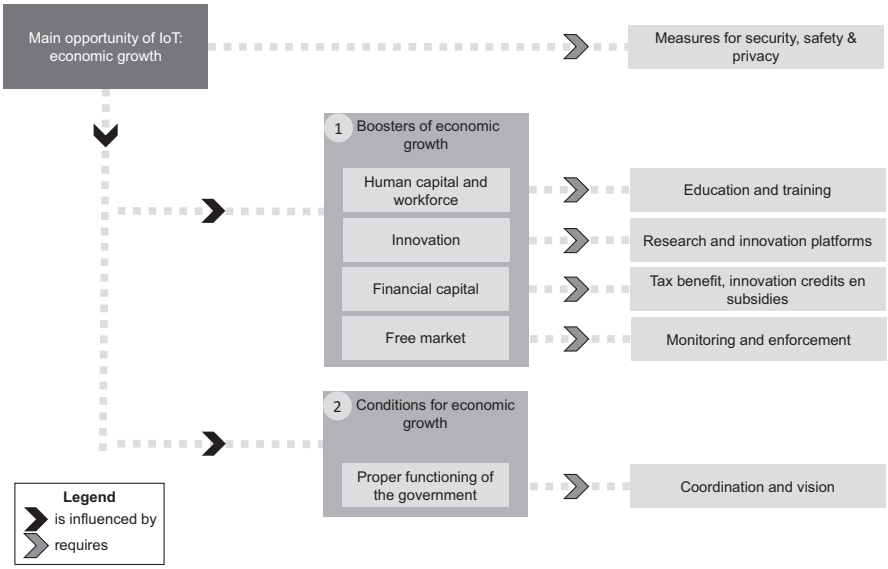

Fig. 1 Factors and measures that foster economic growth through the IoT

Government measures can ensure that the education system better nurtures the IT knowledge and skills needed. Possible solutions are to introduce specific courses that teach skills such as programming, or to incorporate IT skills in existing courses (GO-Science 2014). In addition, governments and organizations should also offer sufficient resources to (re)train the existing workforce.

Innovation

Innovation plays an important role in increasing the productivity of businesses and prosperity in countries. As discussed above, this is partly related to the availability of sufficient knowledge but also depends on the ability of businesses to apply this knowledge to product development and innovations. Businesses and countries that succeed in this challenge are able to stay competitive (CBS 2013).

Governments can support research into new IoT technologies and applications in order to promote economic growth. Universities, research institutes as well as companies with R&D departments can carry out such research. This support includes stimulating spin-offs based on research done at universities and co-development of new technologies by universities and businesses. It is also important that businesses get enough room to experiment and innovate. One possible solution is to implement a "regulatory sandbox," in which authorities work together with stakeholders to create safe spaces for exploring new applications (Vermeulen et al. 2016). Experiments done with self-driving cars in different countries are examples of this regulatory sandbox approach.

Capital

Capital involves both physical capital (buildings or machines) and financial capital. Availability of capital in a country determines, to a certain extent, whether businesses choose to invest in that country (CBS 2013). Governments can support businesses through different measures such as tax benefits, innovation credits, and subsidies.

Because of the importance of the IoT, governments should use financial incentives to stimulate IoT applications in those sectors that are important in their respective countries. In addition, startups should be given ample space to develop new ideas, for example through small grants that allow startups to develop a new IoT product. Governments could also stimulate the development of new IoT products by acting as an intermediary that connects startups with parties in traditional sectors.

Free Market

A free market mechanism is an important prerequisite for the development of the IoT and economic growth. It encourages companies to operate efficiently, create economic value, and share this value with customers (CBS 2013). Various policy instruments can be used to influence market forces, such as laws and regulations that determine the rules of a free market. These include, for example, labor laws and regulation that ensure a level playing field for domestic and foreign companies. Competition authorities are vital to safeguard a free market and to prevent unfair competition.

To ensure a free market in the wake of the IoT and its digital platforms, it is vital that competition authorities, both national and international, have sufficient resources to monitor and enforce applicable laws.

Proper Functioning of the Government

Government functioning influences the country's business climate (CBS 2013). Firstly, the government imposes rights and obligations on companies by implementing laws and regulations. Secondly, as a service provider, the government supports these rights and obligations by granting permits and subsidies, and levying taxes. Lastly, the government can also be a customer of certain products or services. For an optimal business climate, a certain predictability of a government's actions is favorable (CBS 2013). This reduces the risks for the businesses that want to invest. Research indicates that a smart government should take simultaneous actions to innovate technology, management, and policy, as governments need the normative basis in order to innovate (Eger and Maggipinto 2009; Gil-Garcia et al. 2016).

Developing a government vision for the IoT can help businesses to assess whether there is room to innovate and invest. This is especially important if these innovations challenge existing business models. Such developments could evoke

resistance within affected sectors and could call for stricter legislation. A clear government vision can help businesses to anticipate possible changes, and adjust investments accordingly. In this context, it is imperative for the government to take on a leading role as well as be a strategic customer of IoT innovations (GO-Science 2014).

To facilitate this vision new policies might be needed. Thierer (2015) states in this context that new technology should in principle be unrestricted, unless there are convincing arguments not to do so. Others have stated that if there is a lot of technological uncertainty, a technological neutral policy is preferred (Bijlsma et al. 2016). This means that if the adoption costs of new legislation are low for businesses, governments should facilitate experiments and wait with devising or imposing further legislations. Yet if the adoption costs are high, delaying new legislation is expensive (Bijlsma et al. 2016).

Previous studies suggest that there should be one body that is responsible for creating an IoT or technology vision and coordinating its implementation (GO-Science 2014; Kool et al. 2017). Experts that partook in this study, however, expressed worries that introducing a new body could be counterproductive and inefficient, as it creates yet another layer of government. Either way, our findings show that, given the wide range of measures discussed, there should be one party that coordinates and controls them to ensure their effectiveness.

Security, Safety, and Privacy

Figure 2 gives an overview of the *factors* (dark grey blocks) that can hinder the development and use of secure, safe, and privacy-sensitive IoT applications. These obstacles are (1) complexity of the IoT, (2) lack of knowledge and awareness, (3) lack of incentives, and (4) lack of monitoring and enforcement. For all these obstacles, the figure shows some *measures or solution directions* (light grey blocks) to reduce their impact. They are discussed below.

While in some cases it is difficult to take action, government policy could undoubtedly play a fundamental role in mitigating the risks. One could think of principles such as security and privacy by design, which requires that products and software be developed from the ground up to be secure. As a result, safety of both products and software is increased. The government should work closely with the industry to implement this approach on an international level, in order to safeguard the consumer from security threats.

Complexity

Complexity is one of the impeding factors in making IoT applications more secure, safe, and privacy-friendly. In this context, complexity stems from (1) the wide variety of IoT devices, (2) the processing of (big) data, and (3) the playing field. Firstly, the heterogeneity of IoT technology makes it challenging to intro-

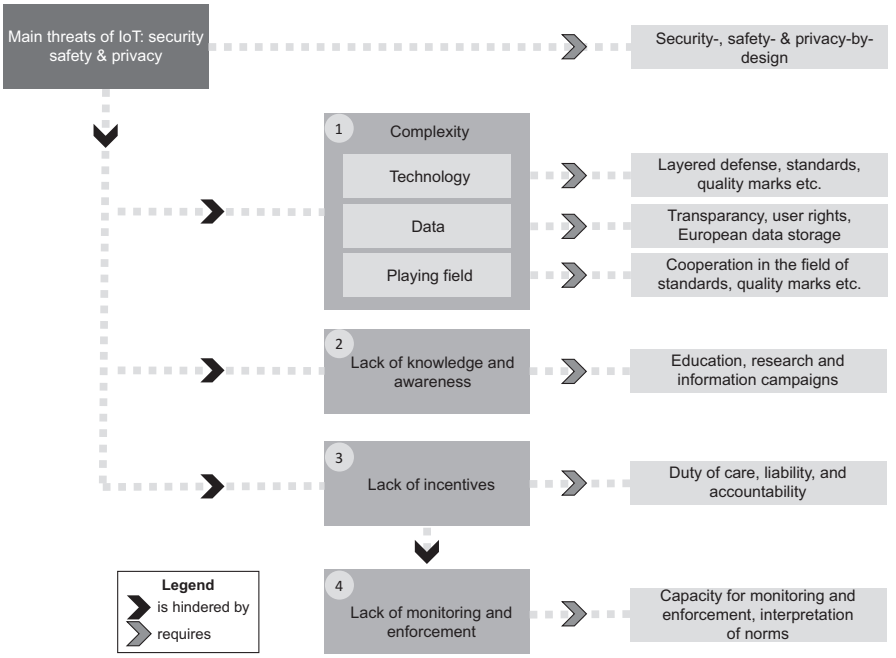

Fig. 2 Obstacles to developing secure, safe, and privacy-friendly applications, and solution directions to overcome them

duce general security measures. Secondly, the important role of data in IoT applications contributes to complexity because of the size and heterogeneity of the data, ambiguity about where they are stored, who has access to and makes use of them, and the legal interpretation of fundamental rights on data. Thirdly, due to the large amount of players on the IoT market, the (international) playing field is rather complex and lacks overview on who is responsible for what. This problem is worsened because governments involved have different rules and standards, as well as different interests.

The following governmental measures may contribute to coping with the complexity of the IoT. First of all, international conformity marks (i.e., CE marking) and standards can contribute to safety by harmonizing IoT technology. They help in determining which security and privacy requirements manufacturers of IoT products have to meet and make it easier to conform to them.

Secondly, transparency in data use can be increased by compelling companies to draft clear and understandable privacy policies. Agreements have been made in the EU's General Data Protection Regulation (GDPR)—article 12, obliging companies to present their policies in a concise, transparent, and understandable language to users. One way to provide users the right of removal of personal data is to integrate an on/off switch in devices, specifically for data transfer to third parties. Finally, localizing data storage can help confining data processing and usage. It should be noted that many of the measures discussed could be more effective when they are designed and implemented in an international context.

Lack of Knowledge and Awareness

Taking measures to mitigate security, safety, and privacy threats is also hampered by a lack of awareness and knowledge about (the risks around) the IoT and IT in general. This applies to the government, citizens, as well as businesses.

Education remains one of the most important duties of any government. Investing in education is, therefore, an important tool for increasing a safe Internet use and developing digital skills (CSR 2016b; Munnichs et al. 2017). In addition, knowledge institutions—such as universities—should emphasize security, safety, and privacy in their education related to developing and using IoT applications. Information campaigns on cybersecurity can also increase awareness and hence the digital resilience of citizens. Through research, knowledge about the current state of technology, cybersecurity and privacy can be acquired, maintained, and enhanced. Public–private partnerships can increase knowledge by monitoring and sharing information about current threats. This collaboration is already taking place; however, this should further be intensified to fully exploit the potential (CSR 2016b).

Lack of Incentives

Taking security, safety, and privacy measures is also impeded by a lack of incentives for users and businesses. Users are often unaware of security and privacy risks, and often, they do not even notice that their IoT devices are hacked (Kolias et al. 2017). For companies, there is an economic incentive to be first-to-market with a product, with or without adequate security features (Wolters and Verbruggen 2016). Moreover, once a device has been sold, their motivation to provide security updates is limited. Maintenance of a product requires time and money, and in most cases it does not yield benefits that outweigh its costs (Munnichs et al. 2017).

Though the lack of incentives applies to both users and manufacturers, in principle, users may assume that manufacturers sell sound products. Governments should therefore take measures that generate incentives for manufacturers to build secure, safe, and privacy-friendly products. One of these measures is to expand the duty of care legislation. Duty of care is an obligation "to take into account and possibly act in the interests of someone else" (Tjong Tjin Tai 2006: 376). The duty of care may also cover the security of IoT products. Liability on the basis of the damage caused by IoT products may also be an important incentive for companies and could serve as a basis for the duty of care.

In addition, the government can influence companies' incentives through their own purchasing policies. Hereby, the government can fulfill an example role as a launching customer. A new purchasing policy may also include the condition that only products and services that comply with certain cybersecurity standards are chosen, which may also serve as an encouragement to abide with certain standards and conformity marks.

Lack of Monitoring and Enforcement

The effectiveness of incentives is impeded by a lack of monitoring and enforcement. Without these, measures such as duty of care and liability have little effect. The same goes for conformity marks and standards, which are only effective with supervision and enforcement. An example of this can be found in the CE marking, which signifies that a product complies with current European requirements regarding safety, health and the environment. Nevertheless, various CE-marked products are withdrawn annually from the market as they pose a risk to users' health or safety (The Netherlands Court of Audit 2017). The Netherlands Court of Audit (2017: 7) indicates, among other things, that presently the resources and capacity are inadequate for effective supervision of the CE marking. This example shows that a label alone is not enough to ensure that a product meets certain requirements.

Further research and discussion on the duty of care for manufacturers of hardware and software are needed. Currently it is unclear, for instance, how duty of care and liability relate to the durability of products. Many products are only supported for a few years while they last many years. Therefore, it should also be considered whether companies should have obligations to provide support also after the expected product lifetimes.

Limitations

Although the research has reached its aims, we are aware of a number of limitations. Firstly, there is no clear definition of the Internet of Things concept. We have chosen to combine definitions, and in that way provide the reader with a comprehensive definition. Secondly, this research project encompasses various technologies and affects many application domains and stakeholders. Because of the large scope of this research, combined with a limited time within which the research had to be completed, it was decided to give a broad overview of the entire playing field. The relevant developments, players, and applications have been mapped out as much as possible. Such a broad focus causes the depth of the research to be limited. Lastly, this research did not aim to quantify the effect of different measures. The present research does describe the expected consequences of various actions, but does not discuss how strong the effects of different measures are. In a follow-up study, attempts could be made to measure the influence of the IoT on the named values (for example, to what extent does the IoT increase prosperity?). Subsequently, an attempt can be made to measure the extent to which certain proposed measures affect this. The interaction effects between different measures could also be taken into account.

Conclusion

In this chapter, we have shown that the IoT can contribute to a wide range of human values that correspond with public policy goals, such as well-being, sustainability, productivity, and prosperity. As such, the IoT can be used as a tool to achieve certain policy goals. At the same time, it also negatively affects certain values, such as security, safety, privacy, prosperity, well-being, equality, and autonomy. Therefore, the IoT may have a disruptive impact on society and cause physical, social, or economic damage. Because of this, both the positive and negative consequences should be taken into consideration when creating new public policy.

What is most worrying is that numerous examples and incidents show that IoT applications are currently poorly protected. This poses a serious threat to our security, safety, and privacy, but also hinders the ability to seize opportunities presented by the IoT. It is important that these risks are addressed in order to reduce and prevent damages as much as possible. To take advantage of the opportunities, it is also important to create a safe environment for new developments and innovation.

As manufacturers of IoT applications and infrastructures, companies are responsible for the creation of not only new and innovative but also secure and privacy-protective IoT applications. Currently this happens insufficiently due to the complexity of the IoT, a lack of knowledge, a lack of incentives, and a lack of monitoring and enforcement. We have shown that all these obstacles can and need to be addressed by government measures. Unfortunately, there is no one-size-fits-all solution for this problem. Instead, several interrelated measures are required, which are only effective if they are implemented as a whole. This requires a supported government vision, where one body is designated to control and coordinate a (new) IoT policy. Because the IoT is related to other technological developments and cybersecurity in a broader context, governments should adopt a coherent approach in which all these topics are covered.

References

Ackerman, S., & Thielman, S. (2016). *US intelligence chief: We might use the internet of things to spy on you*. Retrieved July 24, 2017, from https://www.theguardian.com/technology/2016/feb/09/internet-of-things-smart-home-devices-government-surveillance-james-clapper.

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials, 17*(4), 2347–2376.

Amichai-Hamburger, Y. (2002). Internet and personality. *Computers in Human Behavior, 18*(1), 1–10.

Aoyama, T., Koike, M., Koshijima, I., & Hashimoto, Y. (2013). A unified framework for safety and security. *Safety and Security Engineering V, 134*, 67–77.

Arntz, M., Gregory, T., & Zierahn, U. (2016). *The risk of automation for jobs in OECD countries: A comparative analysis*. Paris: OECD Publishing. *OECD Social, Employment and Migration Working Papers,* 189.

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer Networks, 54*(15), 2787–2805.

Bawden, D., & Robinson, L. (2009). The dark side of information: Overload, anxiety and other paradoxes and pathologies. *Journal of Information Science, 35*(2), 180–191.

Beaudin, J. S., Intille, S. S., & Morris, M. E. (2006). To track or not to track: User reactions to concepts in longitudinal health monitoring. *Journal of Medical Internet Research, 8*(4), 1–22.

Bijlsma, M., Overvest, B., & Straathof, B. (2016). *Marktordening bij nieuwe ICT-toepassingen*. Den Haag: Centraal Planbureau.

Borgia, E. (2014). The Internet of Things vision: Key features, applications and open issues. *Computer Communications, 54*, 1–31.

Bos, J., & Munnichs, G. (2016). *Digitalisering van dieren*. Den Haag: Rathenau Instituut.

Bradley, J., Barbier, J., & Handler, D. (2013). *Embracing the Internet of everything to capture your share of $14.4 trillion*. San Jose: Cisco.

Castermans, J., Feijth, H., Verheij, M., Beekhuizen, J., & Wong-A-Tjong, S. (2014). *Internet of Things: Slimme en internet-verbonden producten en diensten*. Utrecht: Kamer van Koophandel.

CBS (Centraal Bureau voor de Statistiek). (2013). *Het Nederlandse ondernemings klimaat in cijfers 2013*. Den Haag: CBS.

Chang, R. (1997). *Incommensurability, incomparability, and practical reason*. Cambridge: Harvard University Press.

CLTC (Center for Long-term Cybersecurity). (2016). *Cybersecurity futures 2020*. Berkeley: University of California.

CPB & PBL. (2015). *Toekomstverkenning welvaart en leefomgeving: Achtergronddocument binnenlandse personenmobiliteit*. Den Haag: CPB/PBL.

CSR (Cybersecurity Raad). (2016a). *The opportunities and risks of the Internet of Things: Perspectives for action*. Den Haag: CSR.

CSR (Cybersecurity Raad). (2016b). *De economische en maatschappelijke noodzaak van meer Cybersecurity: Nederland digitaal droge voeten*. Den Haag: CSR.

Custers, B. H. M., Calders, T., Schermer, B., & Zarsky, T. Z. (2013). *Discrimination and privacy in the information society: Data mining and profiling in large databases studies in applied philosophy*. Heidelberg: Springer.

Da Xu, L., He, W., & Li, S. (2014). Internet of things in industries: A survey. *IEEE Transactions on Industrial Informatics, 10*(4), 2233–2243.

Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J.H., Le Métayer, D., Tirtea, R., et al. (2014). Privacy and data protection by design—From policy to engineering. Technical report. https://doi.org/10.2824/38623.

Davies, R. (2015). The Internet of Things opportunities and challenges. Retrieved July 24, 2017, from https://www.europarl.europa.eu/RegData/etudes/BRIE/ 2015/557012/ EPRS_BRI(2015)557012_EN.pdf

Domingo, M. C. (2012). An overview of the Internet of Things for people with disabilities. *Journal of Network and Computer Applications, 35*(2), 584–596.

Ellen MacArthur Foundation. (2016). Intelligent assets: Unlocking the circular economy potential. Retrieved July 24, 2017, from https://www.ellenmacarthurfoundation.org/publications/ intelligent-assets

Eger, J. M., & Maggipinto, A. (2009). Technology as a tool of transformation: e-Cities and the rule of law. In A. D'Atri & D. Saccà (Eds.), *Information systems: People, organizations, institutions, and technologies*. Heidelberg: Physica-Verlag.

Farooq, M. U., Waseem, M., Mazhar, S., Khairi, A., & Kamal, T. (2015). A review on Internet of Things (IoT). *International Journal of Computer Applications, 113*(1), 1–7.

Fernandez, F., & Pallis, G. C. (2014). Opportunities and challenges of the Internet of Things for healthcare: Systems engineering perspective. In *2014 EAI 4th International Conference on Wireless Mobile Communication and Healthcare (Mobihealth)* (pp. 263–266). New York: IEEE.

Flight, S. (2016). Politie en beeldtechnologie: Gebruik, opbrengsten en uitdagingen. *Justitiële Verkenningen, 42*(3), 68–93.

Floridi, L. (2015). *The onlife manifesto: Being human in a hyperconnected era*. Cham: Springer International Publishing.

Frenken, K. (2015). *Reflecties op de deeleconomie*. Retrieved July 24, 2017, from https://dspace.library.uu.nl/handle/1874/320399.

Friedman, B., Kahn, P. H., Jr., & Borning, A. (2013). Value sensitive design and information systems. In K. E. Himma & H. T. Tavani (Eds.), *Early engagement and new technologies: Opening up the laboratory* (pp. 55–95). Hoboken: John Wiley & Sons, Inc..

FTC. (2015). *Privacy & security in a connected world*. Washington: FTC.

Gartner. (2015). *What's new in Gartner's hype cycle for emerging technologies, 2015*. Retrieved July 24, 2017, from https://www.gartner.com/smarterwithgartner/whats-new-in-gartners-hype-cycle-for-emerging-technologies-2015

Gil-Garcia, J. R., Helbig, N., & Ojo, A. (2014). Being smart: Emerging technologies and innovation in the public sector. *Government Information Quarterly, 31*, I1–I8.

Gil-Garcia, J. R., Zhang, J., & Puron-Cid, G. (2016). Conceptualizing smartness in government: An integrative and multi-dimensional view. *Government Information Quarterly, 33*, 524–534.

Goodman, M. (2015). *Future crimes: Everything is connected, everyone is vulner-able and what we can do about it*. London: Transworld.

GO-Science (The Government Office for Science). (2014). *The Internet of Things: Making the most of the Second Digital Revolution*. London: GO-Science.

Gregory, J. (2015). *The Internet of Things: Revolutionizing the retail industry*. Retrieved July 24, 2017, from https://www.accenture.com/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_14/Accenture-The-Internet-Of-Things.pdf

Healey, J., Pollard, N., & Woods, B. (2015). *The healthcare internet of things: Rewards and risks*. Washington: Atlantic Council.

Hildebrandt, M. (2008). Defining profiling: A new type of knowledge? In M. Hildebrandt & S. Gutwirth (Eds.), *Profiling the European citizen* (pp. 17–45). Dordrecht: Springer.

Janowski, T. (2015). Digital government evolution: From transformation to contextualization. *Government Information Quarterly, 32*(2015), 221–236.

Kaminski, M. E., & Witnov, S. (2015). The conforming effect: First amendment implications of surveillance, beyond chilling speech. *University of Richmond Law Review, 49*, 465–518.

Keymolen, E. (2014). A moral bubble: The influence of online personalization on moral repositioning. In J. de Mul (Ed.), *Plessner's philosophical anthropology: Perspectives and prospects* (pp. 387–406). Amsterdam: Amsterdam University Press.

Koebler, J. (2015). *Hackers killed a simulated human by turning off its pacemaker*. Retrieved July 24, 2017, from https://motherboard.vice.com/en_us/article/hackers-killed-a-simulated-human-by-turning-off-its-pacemaker

Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. *Computer, 50*(7), 80–84.

Kong, A., Beresford, S. A., & Alfano, C. M. (2012). Self-monitoring and eating-related behaviors are associated with 12-month weight loss in postmenopausal overweight-to-obese women. *Journal of the Academy of Nutrition and Dietetics, 112*(9), 1428–1435.

Kooiman, J., & Jentoft, S. (2009). Meta-governance: Values, norms and principles, and the making of hard choices. *Public Administration, 87*(4), 818–836.

Kool, L., Timmer, J., Royakkers, L., & Van Est, R. (2017). *Opwaarderen:- Borgen van publieke waarden in de digitale samenleving*. Den Haag: Rathenau Instituut.

Krebs, B. (2016). *Who makes the IoT things under attack?* Retrieved July 24, 2017, from https://krebsonsecurity.com/2016/10/who-makes-the-iot-things-under-attack

Layne, K., & Lee, J. (2001). Developing fully functional E-government: A four stage model. *Government Information Quarterly, 18*(2), 122–136.

Lu, J. (2016). Will medical technology deskill doctors? *International Education Studies, 9*(7), 130–134.

Lund, D., MacGillivray, C., Turner, V., & Morales, M. (2014). *Worldwide and regional internet of things (IoT) 2014–2020 forecast: A virtuous circle of proven value and demand*. Framingham: International Data Corporation (IDC).

Manyika, J., Chui, M., Bughin, J., Dobbs, R., Bisson, P., & Marrs, A. (2013). *Disruptive technologies: Advances that will transform life, business, and the global economy*. San Francisco: McKinsey Global Institute.

Mattord, W. (2014). *Principles of information security*. Delhi: Cengage India.

Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad Hoc Networks, 10*(7), 1497–1516.

Moon, M. J. (2002). The evolution of e-government among municipalities: Rhetoric or reality? *Public Administration Review, 62*(4), 424–433.

Munnichs, G., Kouw, M., & Kool, L. (2017). *Een nooit gelopen race: Over cyberdreigingen en versterking van weerbaarheid*. Den Haag: Rathenau Instituut.

Norris, P. (2001). *Digital divide: Civic engagement, information poverty, and the Internet worldwide*. Cambridge: Cambridge University Press.

Pandya, H. B., & Champaneria, T. A. (2015, January). Internet of things: Survey and case studies. In *2015 International Conference on Electrical, Electronics, Signals, Communication and Optimization (EESCO)* (pp. 1–6). New York: IEEE.

Peppet, S. R. (2014). Regulating the internet of things: First steps toward managing discrimination, privacy, security and consent. *Texas Law Review, 93*, 85–176.

Pereira, Â. G., Benessia, A., & Curvelo, P. (2013). *Agency in the Internet of Things*. Luxemburg: Publications Office of the European Union.

Roca, D., Nemirovsky, D., Nemirovsky, M., Milito, R., & Valero, M. (2016). Emergent behaviors in the Internet of Things: The ultimate ultra-large-scale System. *IEEE Micro, 36*(6), 36–44.

Roose, K. (2014). *The sharing economy isn't about trust, it's about desperation*. Retrieved July 24, 2017, from http://nymag.com/daily/intelligencer/2014/04/sharing-economy-is-about-desperation.htm

Rose, K., Eldridge, S., & Chapin, L. (2015). *The Internet of Things: An overview: Understanding the issues and challenges of a more connected world*. Genève: Internet Society.

SER (Sociaal-Economische Raad). (2016). *Verkenning en werkagenda digitalisering: Mens en technologie: samen aan het werk*. Den Haag: SER.

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks, 76*, 146–164.

Silver, E., Wallenstein, S., & Levy, A. (2012). Inward and outward: The role of patient self-monitoring and patient communities in IBD. *Inflammatory Bowel Diseases, 18*, 45–46.

Smit, W., Peters, S., Kemps, D., Vos, R., & Sterk, W. (2016). *Industrial Internet of Things: Noodzaak voor industrie, kans voor IT-sector*. Retrieved July 24, 2017, from https://insights.abnamro.nl/2016/02/industrial-internet-of-things

Song, A. M., Chuenpagdee, R., & Jentoft, S. (2013). Values, images, and principles: What they represent and how they may improve fisheries governance. *Marine Policy, 40*, 167–175.

Stilgoe, J., Owen, R., & Macnaghten, P. (2013). Developing a framework for responsible innovation. *Research Policy, 42*(9), 1568–1580.

Stratix. (2015). *Internet of Things in the Netherlands: Applications, trends and potential impact on radio spectrum*. Stratix: Hilversum.

Sun, Y., Song, H., Jara, A. J., & Bie, R. (2016). Internet of things and big data analytics for smart and connected communities. *IEEE Access, 4*, 766–773.

Swan, M. (2013). The quantified self: Fundamental disruption in big data science and biological discovery. *Big Data, 1*(2), 85–99.

The Netherlands Court of Audit. (2017). *Producten op de Europese markt: CE-markering ontrafeld*. The Hague: The Netherlands Court of Audit.

Thierer, A. (2015). The internet of things and wearable technology: Addressing privacy and security concerns without derailing innovation. *Richmond Journal of Law & Technology, 21*(2).

Tjong Tjin Tai, T. F. E. (2006). *Zorgplichten en zorgethiek*. Deventer: Wolters Kluwer.

Van den Berg, B., & Keymolen, E. (2013). Techniekfilosofie: Het medium is de maat. *Wijsgerig Perspectief, 53*(1), 8–17.

Van Est, R., & Kool, L. (2015). *Working on the robot society: Visions and insights from science concerning the relationship between technology and employment*. Den Haag: Rathenau Instituut.

Van Lakerveld, J. A., Broek, S. D., Buiskool, B. J., Grijpstra, D. H., Gussen, I., Tonis, I. C. M., & Zonneveld, C. A. J. M. (2014). *Arbeidsmarkt voor cybersecurity professionals*. Leiden: PLATO.

Verbeek, P. P. (2011). *De grens van de mens: Over techniek, ethiek en de menselijke natuur*. Rotterdam: Lemniscaat.

Vermeulen, E., Fenwick, M. Kaal, W. A. (2016). Regulation tomorrow: What happens when technology is faster than the law? *TILEC Discussion Paper No. 2016-024*.

Wang, Y. F., Lin, W. M., Zhang, T., & Ma, Y. Y. (2012). Research on application and security protection of internet of things in smart grid. In *IET International Conference on Information Science and Control Engineering 2012 (ICISCE 2012)*, 1–5.

Went, R., & Kremer, M. (2015). Hoe we robotisering de baas kunnen blijven: Inzetten op complementariteit. In *Wetenschappelijke Raad voor het Regeringsbeleid (WRR), De Robot de baas: De toekomst van werk in het tweede machinetijdperk* (pp. 23–46). Amsterdam: University Press.

Williams, C. (2016). *Thermostat ransomware*. Retrieved July 24, 2017, from https://www.theregister.co.uk/2016/08/08/smart_thermostat_ransomware.

Whitmore, A., Agarwal, A., & Xu, L. D. (2015). The Internet of Things: A survey of topics and trends. *Information Systems Frontiers, 17*(2), 261–274.

WEF (World Economic Forum). (2015). *Deep shift: Technology tipping points and societal impact*. Genève: WEF.

Weiser, M., & Brown, J. S. (1995). Designing calm technology. *PowerGrid Journal, 1*(1), 75–85. Retrieved May 17, 2018, from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.135.9788&rep=rep1&type=pdf.

West, D. M. (2004). E-government and the transformation of service delivery and citizen attitudes. *Public Administration Review, 64*(1), 15–27.

Wolters, P. T. J., & Verbruggen, P. W. J. (2016). De verplichting tot het bijwerken van onveilige software. *Weekblad voor Privaatrecht, Notariaat en Registratie, 7123*, 832–839.

WRR (Wetenschappelijke Raad voor het Regeringsbeleid). (2016). *Big Data in een vrije en veilige samenleving*. Retrieved July 24, 2017, from https://www.wrr.nl/publicaties/rapporten/2016/04/28/big-data-in-een-vrije-en-veilige-samenleving

Wurman, R. S. (1989). *Information anxiety*. New York: DoubleDay.

Xu, T., Wendt, J. B., Potkonjak, M. (2014). Security of IoT systems: Design challenges and opportunities. In *Proceedings of the 2014 IEEE/ACM International Conference on Computer-Aided Design* (pp. 417–423). New York: IEEE Press.

Yan, Y., Qian, Y., Sharif, H., & Tipper, D. (2013). A survey on smart grid communication infrastructures: Motivations, requirements and challenges. *IEEE Communications Surveys & Tutorials, 15*(1), 5–20.

Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of things for smart cities. *IEEE Internet of Things Journal, 1*(1), 22–32.

Zarsky, T. Z. (2014). Understanding discrimination in the scored society. *Washington Law Review, 89*, 1375–1412.

Zarsky, T. Z. (2016). The trouble with algorithmic decisions. An analytic road map to examine efficiency and fairness in automated and opaque decision making. *Science, Technology & Human Values, 41*(1), 118–132.

Zwenne, G. J. (2015). De onbestaanbare olifant: gedachten over Big Data en de Privacywet. *Tijdschrift voor Internetrecht, 4*, 142–147.

Ronald Pool is a senior legal advisor at ICTRecht and works as an in-house lawyer. Previously he worked as a researcher at the WODC, Dutch Ministry of Justice and Security. His research focused on cybercrime and issues concerning new technologies and law. He obtained his LLM in Law & ICT from the University of Groningen in 2014.

Jasper van Berkel received his BA in public administration and his LLM in law and technology from Tilburg University in 2011 and 2014. He is currently working as a researcher in the Crime, Law Enforcement and Sanctions Division at the Research and Documentation Centre (WODC). His research interests include cybercrime, cybersecurity, and the use of new technologies in the field of law enforcement. Previously he worked as a researcher in the Centre for Health Protection at the Dutch National Institute for Public Health and the Environment (RIVM). His research topics included e-medication, medical devices, and online patient empowerment.

Susan van den Braak is a senior researcher at the Statistical Data and Policy Analysis Division of the Research and Documentation Centre (WODC) of the Ministry of Security and Justice in the Netherlands. She holds a PhD in computer science from Utrecht University and an MSc in Artificial Intelligence from Radboud University Nijmegen. Her doctoral dissertation focused on argument mapping software for crime analysis. For the Ministry of Security and Justice she focusses on research in the field of AI and law, and e-government. She is currently working on data-centric information systems for policymakers which combine various large (judicial) databases. Her research interests include data science, big and open data, privacy, and cybersecurity.

Maaike Harbers is a professor of applied sciences in Artificial Intelligence & Society at Research Center Creating 010, and a senior lecturer at the Creative Media and Game Technologies program, both at Rotterdam University of Applied Sciences. Her work focuses on the intersection of artificial intelligence, ethics, and design. She studies how designers can create interactive, intelligent technology in a responsible way by accounting for the ethical and societal implications of their concepts during design time. She received a PhD in Artificial Intelligence from Utrecht University in 2011 and an MSc in artificial intelligence and an MA in Philosophy from the University of Groningen in 2006.

Mortaza S. Bargh obtained his PhD in Information Theory from Eindhoven University of Technology in 1999. Between 1999 and 2011 he carried out applied research and project management in the area of secure pervasive computing and ambient intelligence (topics such as system architecture, system security/privacy, and machine learning algorithms). Between 2012 and 2015 he was a part-time visiting Research Professor (i.e., Lector in Dutch) on cyber security and privacy at Rotterdam University of Applied Sciences (RUAS), and since 2013 he has been a scientific researcher at the research center WODC, Ministry of Justice and Security. Since December 2017 Mortaza has been appointed as Lector on Privacy and Cybersecurity Engineering at RAUS. His current research interests include privacy/security by deist engineering, privacy preserving data mining, machine learning, data publishing (e.g., in Open and Big Data settings), access and usage control, collaborative security, usable security, and risk management.