Beyond control

Exploratory study on the discourse in Silicon Valley about consumer privacy in the Internet of Things

Sarah Eskens, Jelte Timmer, Linda Kool and Rinie van Est

Rathenau Instituut

Beyond control

Exploratory study on the discourse in Silicon Valley about consumer privacy in the Internet of Things

Sarah Eskens, Jelte Timmer, Linda Kool and Rinie van Est

Beyond control
Exploratory study on the discourse in Silicon Valley about consumer privacy in the Internet of Things

Sarah Eskens, Jelte Timmer, Linda Kool and Rinie van Est

The publication ‘Beyond control’ is a collaboration between the Rathenau Instituut and the Netherlands Network for Innovation, Technology and Science (NL-NITS) of the Consulate General of the Netherlands in San Francisco, United States.

Rijksdienst voor Ondernemend Nederland

Rathenau Instituut
Anna van Saksenlaan 51
P.O. Box 95366
2509 CJ The Hague
The Netherlands
Telephone: +31 70 342 15 42
E-mail: info@rathenau.nl
Website: www.rathenau.nl
Publisher: Rathenau Instituut

Proof reader: Catriona Black
Design cover: Rathenau Instituut
Layout: Rathenau Instituut
Print: Rathenau Instituut

Preferred citation:
Eskens, S., Timmer, J., Kool, L., and Est, R. van, *Beyond control. Exploratory study on the discourse in Silicon Valley about consumer privacy in the Internet of Things*, Rathenau Instituut, Den Haag 2016

Preface

Ever more objects are becoming *smart*; smart Barbies, smart bras and even smart surveillance drones in school playgrounds. These objects connect to the internet and use intelligent software in the cloud to tailor services to consumers. Smart dolls can respond to children's conversations, and smart bras advise us about our activity patterns and calories burned. That also means that smart devices continuously gather information from very personal environments, which raises fundamental questions about the safeguarding of privacy in an Internet of Things era.

This exploratory study aims to inform policy-makers in the Netherlands about privacy protection in the Internet of Things, by mapping the views of stakeholders in Silicon Valley. Although there are differences between privacy perspectives in the United States and Europe, technologies developed in Silicon Valley will influence developments here, and the views of stakeholders there can inform policy debate here. As well as interviews with stakeholders in Silicon Valley, we organised a roundtable meeting in San Francisco with experts from academia, industry, government and civil society. This study is a collaboration with the Netherlands Network for Innovation, Technology and Science of the Netherlands Consulate General in San Francisco. It is part of research on the 'Hyperconnected consumer' within the theme 'Intimate technology' in the Rathenau Instituut Work Programme, 2015-2016.

At this point, the Internet of Things is still in its early stages, but expectations of its potential growth are high. With a growing number of smart objects on the market, data streams are beginning to permeate everyday life to an unprecedented degree. This study shows that stakeholders' existing privacy perspectives place the burden of control over personal data on the consumers themselves. That has limitations in the Internet of Things. Consumers can lose control, as smart devices don't necessarily have screens, and the sheer quantity of them makes it hard to keep control over all the data flows. We see stakeholders searching for new privacy approaches, which shift the burden of control towards companies and supervisory authorities. They aim for trust, shared responsibility and accountability. The Rathenau Instituut believes that fruitful privacy protection in the Internet of Things requires further exploration of such approaches. Smart devices increase the chance that consumers will be subject to profiling and subtle persuasion, thus impacting their freedom. We therefore need a broad discussion with politicians, civil society and industry to find practical ways to safeguard essential human values such as autonomy and human dignity.

We don't know exactly what a world of connected things will look like, or how we will feel about privacy in the future. That will never stand still. But it remains important to monitor emerging practices and to understand how technology influences us: does it empower us or restrict our freedom? We need to keep asking what kind of society we want to live in. To return to the drones surveilling my kids' school playground, I personally prefer that they have human contact. Luckily, the drones turned out to be an April fools'.

Dr. Melanie Peters
Director Rathenau Instituut

Summary

1. Introduction

An increasing number of everyday objects is being connected to the internet. Examples are smart meters, smart Barbies and smart cars. Via the internet, these objects increase their processing power and acquire new capabilities. For instance, smart Barbie is able to respond to children in real time, by analysing recorded conversations with artificial intelligence techniques in the cloud. This means that these networked devices are also continuously gathering information from their surroundings, which raises fundamental questions about safeguarding privacy and responsible use of personal data.

At this point, the Internet of Things is still in its early stages. Scientists and engineers are developing enabling technologies, and companies are creating new products, services, and business models. Meanwhile, policy-makers are exploring the societal benefits, whilst also seeking guidance on data protection. This exploratory study aims to inform policy-makers in the Netherlands. It maps stakeholder discussions on privacy and the Internet of Things in Silicon Valley – the unofficial tech region of the world. Technologies developed there will influence technological development in the Netherlands and Europe, and the views of stakeholders residing in Silicon Valley will also inform discussions here.

The study is based on desk research (literature review) and qualitative empirical research. We held semi-structured interviews and organised an expert roundtable in Silicon Valley with experts from academia, industry, government, and civil society. The scope of this study is confined to privacy in consumer settings.

2. Technical and business perspective

The idea of the Internet of Things has been explored for a few decades, but only in recent years have those visions become a practical reality for consumers and businesses. In the beginning, the Internet of Things was mainly pursued by academic research groups. Now, commercial players like hardware, software, and service providers and companies are pushing the Internet of Things. There is no official definition of the Internet of Things. Consulted stakeholders characterise the Internet of Things in different ways, reflecting their stake in it, but all essentially describe the Internet of Things as devices that are networked, gather information and can communicate.

Expectations of the Internet of Things are high. For example, the OECD estimates that in 2022, households across the OECD area may have around 14 billion connected devices in total (around 50 per family). However, literature review also shows that growth in consumer demand for Internet of Things devices is slower than industry had initially hoped. Important barriers are price, privacy, security, and ease of use. Nevertheless, all stakeholders consulted for this study agree that the real value of the Internet of Things will come from analysing the data that all the networked devices gather. From a business perspective, the Internet of Things can change every activity in the value chain, and data is at the core of reshaping the value chain. How companies will use that data is therefore essential to understanding privacy issues in the Internet of Things.

3. Privacy perspective

Chapter three explores how different stakeholders conceptualise privacy. These conceptions influence how companies operationalise privacy in designing their products and services, and the kind of privacy issues which policy-makers, legal scholars and civil society foresee for the Internet of Things. Privacy has been discussed from different angles, including a social, economic, legal, and philosophical perspective. Our discussions focus on the legal-philosophical discourse, as it is dominant in articulating the concept of privacy, and because the legal framework is central to policy-making.

This chapter distinguishes between broad and narrow concepts of privacy in the United States and Europe. Broad concepts of privacy include ideas like privacy of the home and correspondence, referring to human dignity, autonomy and the development of one's personality. These concepts can be found, for example, in the Universal Declaration of Human Rights (UDHR) and the European Convention on Human Rights (ECHR). Narrow concepts of privacy concern mainly the protection and control of personal data, and come with an economic dimension: assuming that private and public actors need to be able to use personal data for societal reasons. This is apparent, for example, in the EU's Data Protection Directive (DPD), and the General Data Protection Regulation (GDPR) that is set to replace it. The DPD has a double objective: to protect people's right to privacy with respect to the processing of personal data and to ensure the free flow of personal data within the Internal Market. This narrow concept of privacy as control over personal data, and the ability to influence what data is collected about you, is dominant among the stakeholders interviewed for this research.

4. Future perspective

This chapter gives an overview of the privacy issues and solutions identified by stakeholders. The biggest concern is that consumers will lose control over their personal data. Many Internet of Things devices will not have a screen or another user interface via which consumers can exercise control. In addition, the amount of devices collecting data about consumers is expected to grow fast, and it may be too much for consumers to control all these data flows. Still, consulted stakeholders express optimism regarding solutions to address this concern; they expect that there will be new, effective ways to build control into consumer devices, even those without screens (for example via hand movements and other new intuitive interfaces). Another important suggestion made by stakeholders for improving user control was granular permissions. They allow the user to select permissions to access or use data (e.g. from a smart phone's location, camera, contacts, photos, or microphone) specific to each app and device feature. The granular system then requires apps to ask for user permissions only when a particular feature is needed, as opposed to an all-or-nothing choice when the app is installed.

At the same time, the stakeholders we interviewed also (implicitly) recognise that the idea of control over personal data might not be sufficient to address all privacy concerns related to the Internet of Things. Therefore stakeholders are exploring new or additional approaches, for example a risk and trust based approach, in which companies determine beforehand the most sensitive data uses, and subsequently let consumers control the sensitive data flows, thereby showing consumers that companies can be trusted with such data. Other stakeholders see promising or additional approaches in consumer protection law and software liability.

In this chapter, it also becomes clear that the broader concepts of privacy linked to human dignity, autonomy and self-realisation remain underexposed in current stakeholder discussions. During the expert roundtable, participants were asked several times to reflect on such broader notions of privacy. In general, these questions evoked musing among participants about the effect on people's behaviour of being continuously monitored, and the trade-off between privacy and such interests as safety, and the importance of safeguarding these more value-laden aspects of privacy. But it proved difficult to trigger a substantial discussion on notions of privacy beyond the notion of control over personal data.

5. Conclusion

The idea of the Internet of Things has been around for a long time. Today, it seems to be making its way to the consumer market. Based on our consultations with stakeholders, we can conclude that we are still at the early stages of this development, but expectations regarding its potential growth are high. Stakeholders point out that it is evident that when the Internet of Things comes into full bloom, data streams will start to permeate everyday life to an unprecedented degree. This raises questions about whether existing ways of protecting privacy will be sufficient for the Internet of Things.

The stakeholders consulted for this study conceptualise privacy in terms of control over personal data. Their main concern is that in the Internet of Things, users will lose control, and they are starting to recognise that this 'control paradigm' has its limits when it comes to respecting consumers' privacy in the Internet of Things. It places the burden of control over privacy largely in the hands of the consumer, while at the same time it becomes more difficult for the consumer to remain in control. With the arrival of the Internet of Things, stakeholders are searching for new concepts and solutions, such as trust-based approaches and the improvement of software liability and consumer protection oversight. These approaches are beginning to shift the burden of privacy control from the consumer to companies offering Internet of Things services, and to supervisory authorities with strong oversight of these companies. Such approaches are already common for the development of traditional products (think, for example, of safety guidelines for Barbies, televisions and cars). Considering the (practical) limits of control for consumers in the Internet of Things, the Rathenau Instituut believes that similar approaches are needed for Internet of Things services, without the burden of control being placed solely upon the consumers. Concepts like trust, shared responsibility and accountability are essential to such approaches.

However, the privacy concerns of stakeholders are not limited to loss of control. The Internet of Things also impacts upon more value-laden aspects of privacy such as autonomy and self-realisation, for example through detailed profiling and possibilities for persuasion. Consider the smart TV (paragraph 2.1 and 4.2), where the idea of control over data does not take into account the effects of the smart TV's monitoring on other family members and on the unhindered development of their own identities. It is therefore important to include the safeguarding of autonomy, personality development and human dignity in the search for new approaches to the protection of privacy in the Internet of Things.

We also still need to learn how to properly *articulate* the way in which these concepts relate to governing data. In our stakeholder discussions, it proved difficult to step outside of the 'control paradigm' to think of practical solutions for the protection of such aspects of privacy as autonomy. In academia, scholars are discussing how pervasive computing technologies, including the Internet of Things might impact fundamental human values like human dignity, autonomy and identity development. But, we are still a long way from translating such concepts into actual software design practices and practical guidelines. In law-making, privacy is also in flux. New regulations are in the pipeline in Europe and the United States in which policy-makers juggle a variety of developments and interests such as fighting terrorism, preventing monopolies and safeguarding personal freedom.

New discussion on ethics

An important step in the articulation of new concepts is to activate discussions related to the Internet of Things involving politicians, civil society, consumers and tech companies. A recent initiative of the European Data Protection Supervisor (EDPS) is a case in point. EDPS established an Ethics Advisory Group, calling for broader discussion on a new digital ethics to safeguard human values in the context of new technologies such as the Internet of Things – implying that such discussion should not merely be conducted in terms of data protection. The Rathenau Instituut believes that such initiatives can help in the search for valuable new approaches to safeguarding privacy, autonomy, self-realisation and human dignity, where companies, consumers and public supervisory authorities share the responsibility.

Contents

1 Introduction

1.1 The further merging of physical and digital worlds

We are surrounded by ever more objects that connect to the internet. This is part of the development towards an “Internet of Things”: the (further) merging of the physical and the digital worlds through connecting things to the internet and to each other. Our computers and smart phones are already connected, and in this new wave of the internet, things like security cameras, light bulbs, toys, and cars are connected as well. The Internet of Things will be comprised of smart objects that, to a certain extent, can operate autonomously and interactively. An early example is the internet-connected refrigerator. As early as 2000, LG unveiled a fridge that featured a scanner to track what was inside it and which could automatically send out orders to online grocery stores. The electronics company was too early with this model and it failed on the market, but the idea of connecting a wide array of things to the internet persisted. Now, the Internet of Things is having its moment and expectations for its uptake are high. If we look at the consumer sector alone, Gartner predicts that by 2020, about 13.5 billion things will be connected, compared with 3 billion in 2015 (Gartner 2015a). The OECD estimates that in 2022, households across the OECD area may have around 14 billion connected devices in total, with around 50 per four-person family (OECD 2013).

How the Internet of Things unfolds will be determined by the collective interplay of a wide range of stakeholders. At this point, the Internet of Things is still in its early stages (Greengard 2015). Various players are working hard to realise its infrastructures and possible applications. Software and hardware engineers and scientists are developing the enabling technologies. Companies are creating new products, services, and business models. Meanwhile, policy-makers are exploring the societal benefits, and regulators are issuing guidance on data protection. In addition, legal, social, and ethical scholars are studying new issues that arise from the Internet of Things. Non-profits such as digital rights organisations are advocating for strong privacy and security protection. All these stakeholders exercise influence on the type of Internet of Things technologies and applications that will find their way into our daily life.

Many applications for the Internet of Things will affect our personal privacy. If we focus on the domain of smart homes, the Internet of Things will bring us all kinds of personal devices and household appliances that collect, process, and distribute data related to our private life, and that can monitor our daily behaviours.[1] For instance, the Internet of Things thermostat, Nest, determines when you are at home, when you are away, and what time you usually wake up. On the basis of this information, it will adjust the setting to a preferred temperature. Nest may receive data from third parties and associate these with your Nest account. The thermostat stores all the personal data locally on the device or on servers until you delete it, or for as long as you remain a Nest user. Another example in the home domain is the security camera, Simplicam. This Wi-Fi connected camera with face recognition technology can tell you who is home and lets you see video feeds on

[1] By far the largest opportunity in the home setting is in automating routine household tasks (McKinsey 2015, p. 50).

your smart phone when you are away. These two examples show that the Internet of Things will not just affect privacy because a large amount of personal data is processed, but also because it enables new ways of directly monitoring the private sphere. And moving beyond privacy, with predictive analytics and computational interventions, Internet of Things devices may even pre-empt user intent (Hildebrandt 2015). If your smart bathtub gathers data about daily usage patterns and combines these with data from other devices it may be able serve you a hot bath when you feel stressed, before you have actually formed the intention to take a bath.

In general, there is widespread concern about privacy-infringing activities by organisations. In a recent PEW survey, 91% of Americans agreed or strongly agreed that “consumers have lost control over how personal information is collected and used by companies” (PEW 2014). The latest special Eurobarometer on data protection showed that 31% of European respondents feel they have no control at all over their personal data online. Two thirds indicated that they were concerned about this situation (TNS Opinion & Social 2015). In another survey, 47% of consumers worldwide cited privacy risks and security concerns as a barrier to the purchase of Internet of Things devices (Accenture 2014). This raises the question of how stakeholders approach privacy in the Internet of Things, and how they give shape to the Internet of Things with a view to privacy.

1.2 Research aim, scope and methodology

Our aim is to map Silicon Valley’s discussion on privacy in the era of the Internet of Things. Silicon Valley is the unofficial tech capital of the world. Technologies being developed there will influence technological development in the Netherlands and Europe, and the views of stakeholders residing in Silicon Valley will also inform debate here. We want to explore the main topics for debate regarding privacy in the Internet of Things for an audience of policy-makers in the Netherlands. The Rathenau Instituut intends to use this exploratory study as input for further research. This goal brings us to the following research question:

What are the various viewpoints of Silicon Valley-based stakeholders in the Internet of Things with respect to privacy in the Internet of Things?

This question is broken down into three sub-questions:

1. What is the Internet of Things, who are its commercial stakeholders, and how do they define the Internet of Things and monetise it?
2. What are the different ways to conceptualise privacy and how do stakeholders in Silicon Valley in particular define privacy?
3. What issues and solutions do stakeholders identify for privacy in the Internet of Things?

The scope of this exploratory study is confined to privacy in consumer settings. This means that we will not look into the Industrial Internet of Things. That notion describes the use of Internet of Things technologies to optimise operations and make processes more efficient in industrial sectors such as

manufacturing, energy, agriculture, and transportation.[2] Nor will we address privacy concerns that may occur when governments or employers start utilising the Internet of Things to monitor citizens or employees. Our scope also excludes privacy issues arising on the back end of the Internet of Things, such as through the international flow of personal data. Obviously the privacy discussion in Silicon Valley does not take place within a vacuum, but this research focuses on stakeholders headquartered in, or with a strong affiliation to, this region. We do occasionally cite European views as a means of providing contrast.

For this exploratory study we combined desk research and qualitative empirical research. We performed a literature review (focusing on technical and business perspectives of the Internet of Things, and focusing on the legal-philosophical discourse on the concept of privacy), held semi-structured interviews with eight stakeholders residing in Silicon Valley, and organised an expert roundtable with eleven participants from that region and abroad. For both the interviews and the roundtable we selected people from academia, industry, government, and civil society. The results of the interviews have been incorporated throughout the texts. A complete list of those interviewed is attached as Annex I to this study. A complete list of participants of the roundtable meeting can be found in Annex II. It was promised that the results of the roundtable would be used anonymously to encourage free and open discussion during the meeting. A full, anonymised report of the discussion can be found in Annex III. The questions used for the interviews and the expert roundtable correspond with our research questions and with the chapter structure.

Reading guide

Chapter 2 looks at the Internet of Things from a technical and business perspective. Chapter 3 sets out how privacy is conceptualised by theorists and stakeholders in Silicon Valley. Chapter 4 gives an overview of the privacy issues and solutions identified during the interviews and expert roundtable. Chapter 5 reflects on our findings and concludes with a recommendation for future debate about privacy in the Internet of Things.

---

[2] The “Industrial Internet (of Things)” is in fact a campaign launched by General Electric in 2012, when the industrial corporation realised that there was a lucrative business in servicing machines with software. See Regalado 2014.

2 Technical and business perspective

What we now call the “Internet of Things” is not so much a specific technology but rather a vision or a paradigm. There is no official definition of the Internet of Things (Minerva 2014, p. 3). Stakeholders characterise the Internet of Things in different ways, reflecting their stake in it, but there is a general understanding of what it entails. This chapter describes the early visions that inspired the development of the Internet of Things (2.1), current developments in the field (2.2.), who today’s commercial stakeholders are and how they describe the Internet of Things (2.3). As will be shown, Internet of Things-like ideas have been explored for a few decades, but only in recent years have those visions become a practical reality for consumers and businesses.

2.1 Visions of an Internet of Things

Towards the next step in the development of the Internet

An important predecessor to the Internet of Things is the vision for “ubiquitous computing” that was articulated by Mark Weiser in the late 1980s at Xerox Palo Alto Research Center (Xerox PARC).[3] In the computer scientist’s view, computers would become part of the environment in this new wave of computing, available everywhere and anywhere (Weiser 1991). He reasoned that when computers became invisible to common awareness, or disappeared into the background, people could use them unconsciously, free to focus on new goals such as giving attention to other people instead of computer screens. However, the idea of ubiquitous computing was born before the commercialisation of the internet, so it did not yet reference the net.

By the end of the 1990s, researchers at the MIT New Media Department explored a vision comparable to ubiquitous computing, but this time involving the internet. Physicist Neil Gershenfeld and his colleagues were working on technologies to merge the digital and the physical world. They noted that people’s interaction with computers often resulted in irritation, and concluded that computers should provide solutions to problems everywhere, without people having to attend to the computers. Gershenfeld found that the real promise of connecting computers was to free people, by embedding computing capabilities in the things around us. He foresaw a future where “things start to use the Net so that people don’t need to” (Gershenfeld 1999). Later, the researcher dubbed his project “Internet-0”, to relate it to the then current Internet-1 and high-speed Internet-2 project. Internet-0 would be about devices that did not need broadband speeds for movie-watching and online streaming, but just an Internet connection for low bandwidth data transfer (Gershenfeld, Krikorian and Cohen 2004).

The idea of an Internet of Things also has roots in the Auto-ID Center which opened at the Massachusetts Institute of Technology (MIT) in Cambridge, Massachusetts in 1999. A group of

[3] Research in this field was continued with research into the comparable notion of “pervasive computing” (Olson, Nolin and Nelhans 2015)

manufacturers and standardisation organisations set up the lab to research and develop “Auto-ID technologies” (Sarma, Brock and Ashton 2000). Auto-ID (Automatic Identification) refers to technologies used in the world of commerce that enable computers to automatically recognise and identify everyday objects (Meloan 2003), such as barcodes and Radio Frequency ID (RFID) systems. The Auto-ID Center focussed on the development of RFID tags and an Electronic Product Code (EPC) for supply chain management, which played an important role in making Internet of Things technologies commercially attractive.

All in all, what emerged was the idea that billions of everyday things such as personal devices (not just computers and smartphones), household appliances, and industrial machines can be connected to the internet and to each other via other networks, enabled to sense, think, communicate, and act for us. The International Telecommunications Union sees this as an ongoing development of how we use the internet (ITU 2005, p. 3). Initially we had to sit in front of a personal computer to make use of the internet, dialling it up over the telephone line. Today, we can connect to the internet via mobile internet services at any time and from any location. The next step is the Internet of Things, in which the internet can be used *any time, anywhere, by anyone and anything*. Think, for example, of the newest Samsung SUHD TVs. The electronics company’s entire 2016 smart TV line-up will be ready for the Internet of Things and can connect with Samsung’s SmartThings platform. SUHD TVs will apply Internet of Things “hub technology”, so that you can use your TV as the controller for your entire smart home. The TVs can connect with, and control, Samsung devices and sensors, as well as connected lights, locks, thermostats, and cameras. Applications that run on the SmartThings platform, for instance, can automatically adjust ambient lighting and sound when you start a movie, and video streams from outside the home can pop up directly on the TV screen (Samsung 2015).

Technological elements of the Internet of Things

At its basis, the Internet of Things comprises “things” that are equipped with sensors and actuators, communication and network technology, a processing unit, and a unique identifier (Al-Fuqaha et al. 2015). To begin with, sensors give the thing context awareness and the ability to collect data about its user and its physical environment. Actuators enable it to perform actions in the physical world. Next, communication and network technology are essential to connect the thing to the internet, if necessary, via a local network or a gateway device between the object and the internet. Through these connections, data is exchanged with other connected objects, dedicated servers, or the cloud. Furthermore, a processing unit (on a chip or as a software service) gives the thing the capability to do small computing on the data it has collected and operate without human intervention. Finally, a unique identifier ensures that the thing can be found in the network and is not mixed up with the billions of other objects connected to the net.

The Internet of Things can go by other names. Some focus on “smart objects” (Vasseur and Dunkels 2010), or “cyber-physical systems” (CPS), but these terms have slightly different meanings. In particular the notion of CPS has more of an industrial connotation, and it really describes an engineering discipline.[4] By contrast, the idea of an Internet of Things includes the consumer side,

[4] http://cyberphysicalsystems.org/

and research into it is mostly computer science-driven (Jeschke 2013). In Japan and South Korea, the Internet of Things is embodied in programmes for a Ubiquitous Network Society.

Over time, the notion of the Internet of Things has broadened considerably (Olson, Nolin and Nelhans 2015). Kevin Ashton, one of the co-founders of the Auto-ID Center, originally coined the term in 1999 (Ashton 2009). Widespread attention for the phenomenon took off when the International Telecommunications Union published a report on the topic (ITU 2005), and the European Commission subsequently put it on the agenda (European Commission 2006). Taking into account its long history, and the fact that the underlying technologies are under continuous development and debate, we asked how stakeholders today understand the Internet of Things.

2.2 The Internet of Things today

A moving market

Over the past few years we have seen visions of the Internet of Things becoming a practical reality for consumers and businesses, with an increasing amount of smart and connected household devices coming to the market. The previous section has shown that at first the Internet of Things was pursued largely by academic research groups. Today, it is pushed by commercial players such as hardware, software, and service providers, and companies that use Internet of Things technologies for their own business. Our literature review and stakeholder conversations brought attention to several shifts in the Internet of Things market.

To begin with, an increasing share of the value of the Internet of Things will go to the software industries (McKinsey Global Institute 2015, p. 33). In this respect, Gartner notes that a market for Internet of Things algorithms is emerging, creating opportunities for companies to use third-party analytics to create business value. In such an “algorithm economy”, Internet of Things algorithms are created by third parties and then sold or provided as a service where end-users upload their data to cloud algorithms (Gartner 2015b). Nevertheless, in the current stage of the Internet of Things, the fastest developments are to be seen on the hardware side. Participants in the expert roundtable pointed to the dropping prices for chips, tags, and sensors, and more efficient batteries. This makes it feasible to equip everyday devices with these elements and to bring them to the Internet of Things consumer market.[5]

The favourable future for software causes the blurring of lines between hardware and software markets. Hardware companies create semiconductors (chips), sensors and actuators, networking and communication technologies, memory products, batteries, and so on, for the digital industries. Internet of Things software companies offer applications, big data analytics, middleware, cloud services, security, and the like. With the prospect of smart objects and the Internet of Things, hardware companies are advised to “go software”, using software to differentiate their products (Harter and Böckmann 2010). Intel, the chipmaker, for instance, already delivers processors for the Internet of Things that come with a cloud suite and analytics capabilities.[6] Software companies are

5 Expert roundtable, 12 November 2015, San Francisco.

6 http://newsroom.intel.com/community/intel_newsroom/blog/2015/11/03/new-intel-iot-platform-makes-more-things-smart-and-connected

also crossing the boundaries of their own discipline by making hardware products.[7] For example, Microsoft, a software provider by origin, now makes phones, laptops, and the Microsoft Band, a health and fitness tracker to wear on your wrist.

Finally, the Internet of Things is expected to increase the power of platforms (Regalado 2014, p. 3). A platform can be defined as a foundation of products, services, or technologies upon which other parties can build further products, services, and technologies (Kreijveld et al. 2014). An Internet of Things platform can typically connect, monitor, and manage or control various types of objects via applications that third party developers build on the platform, and is delivered as a software suite or a cloud service (Platform as a Service) (Gartner 2015b). Other platform capabilities include data aggregation and analysis, device communications, cyber security, and event processing (Gartner 2015b). Apple's HomeKit, for instance, is a software platform for communicating with, and controlling, connected accessories in the home. Developers can build apps for smart phones that enable users to configure or control those home products, such as turning on a light or opening a garage door, and make them available in the App Store. To promote HomeKit, Apple partners with brands of physical home products to provide products with a label that signals compatibility with the HomeKit platform.

Monetising data generated by the Internet of Things

In order to understand how the Internet of Things will affect privacy, we need to know how companies will use personal and non-personal data generated by the Internet of Things to monetise their initiatives. It is expected that the Internet of Things will give rise to new business models both for organisations that use Internet of Things systems for their own business, and for those that supply Internet of Things technology (McKinsey 2015, p. 33). Organisations indicate the need for increased understanding of business models if the Internet of Things is to support business development (ITU 2005, p. 64-71; OECD 2012, p. 25). Such knowledge may also be of help to the privacy community. Still, at this point, nobody knows what the winning business models are going to be (The Economist 2013). A complicating factor is that the business model is a fairly new unit of analysis, and scholars have different ideas about what it entails (Zott 2011).[8]

During the expert roundtable it was suggested that the four common revenue models for digital platforms could apply to the Internet of Things: direct payment, advertising, access to services, and acquisition (the typical Silicon Valley startup idea). In the direct payment model, a platform or an Internet of Things company offers services directly to users and charges them for that. The advertisement model is a set up in which a company offers services to consumers, and the consumers provide revenues indirectly by being exposed to advertising. A business based on an access model connects applications and digital content to users, in which case the company may charge the app and content developers as well as the users. In the acquisition model, platforms or Internet of Things companies create value by the development of technology and by amassing

---

7 http://www.techrepublic.com/article/the-two-reasons-why-software-companies-are-making-hardware/; http://techcrunch.com/2014/06/30/with-software-eating-hardware-silicon-valley-enters-hard-times/

8 For a more extensive analysis of business models in the Internet of Things see Fan and Zhou 2011; Liu and Jia 2010; Sun et al. 2012; Bucherer and Uckelmann in Uckelmann et al. 2011; Li and Xu 2013; Fleisch et al. 2014; Dijkman et al. 2015; Perera et al. 2014; Westerlund et al. 2014; Mazhelis et al. 2013; Leminen et al.2012.

users for this technology, with the aim of being acquired by a third company (also see Van Eijk et al. 2015).

2.3 What the Internet of Things means to today's stakeholders

The stakeholders we interviewed understand the Internet of Things in a similar fashion to the description in paragraph 2.1, emphasising the computing and networking aspects. Among them is Mike Liebhold, tech researcher at the Institute for the Future (IFTF), a Silicon Valley-based non-profit research group. In his view, the Internet of Things means especially that computational tasks can be executed at the very ends of the networks ("edge computing").[9] For instance, a connected security camera could analyse a video stream itself, instead of sending the data to a central server for processing.

For most of the people we consulted, the Internet of Things is essentially about things that are networked and enabled to communicate. In that respect, Liebhold stresses that the Internet of Things concerns things not only connected through the Internet Protocol but also through other protocols, such as Wi-Fi, Bluetooth, Zigbee, or LTE.[10] A spokesperson from Google mentions that even within the company, people may have different understandings of the Internet of Things, but that on a general level it is seen as devices that are networked and connected to each other, and which gather information out of that.[11] Elaine Sedenberg, PhD student at Berkeley School of Information, would add that the Internet of Things is also about things that may be plugged in later.[12] For example, LG's SmartThingQ sensor can turn a normal, unconnected object into an Internet of Things-device. The sensor can simply be attached to many traditional home appliances such as washing machines or refrigerators to make them aware and smart.[13] This aspect of the Internet of Things was mentioned during the expert roundtable as well.[14] It calls for attention to the fact that many daily objects may be made part of the Internet of Things retroactively.

The stakeholders involved in this project also understand the Internet of Things as an extension or phenomenon of various other technological developments. Lee Tien, Senior Staff Attorney at the Electronic Frontier Foundation (EFF), places the Internet of Things in the context of two other changes. He sees a rise of intermediaries in the offline and online world, from payment intermediaries (eg credit card companies) to Internet intermediaries such as Internet Service Providers and social media platforms. Tien also notes that today, data capture and the tracking of a particular person can be done without any substantial extra spending, at least with respect to anyone who carries a smart phone or another device that is connected to the internet. Therefore, in

9 Mike Liebhold, 20 August 2015, Palo Alto. Also see http://www.govtech.com/transportation/Is-Edge-Computing-Key-to-the-Internet-of-Things.html
10 Mike Liebhold, 20 August 2015, Palo Alto.
11 Google, 11 September 2015, Mountain View.
12 Elaine Sedenberg, 21 August 2015, Berkeley.
13 http://www.lgnewsroom.com/2015/08/lg-to-unveil-smart-sensor-alljoyn-smart-home-products-at-ifa-2015/
14 Expert roundtable, 12 November 2015, San Francisco.

the Internet of Things, data collection will be the default, and all kinds of data will be available by default.[15]

Similarly, Marcia Hofmann, private attorney in the Bay area focussed on technology law, thinks the Internet of Things is a continuation of technological innovations that have existed for a long time. She observes that a lot of the fears and concerns around the Internet of Things in terms of privacy and security are not new problems. In Hofmann's view, it is the scale of the Internet of Things which is new.[16] Then finally for Chris Maresca, founder and CTO of Sherbit, an app for personal analytics, the Internet of Things is part of a trend towards more and more data generation. He sees how everything, from household appliances to personal services, is going to have an app, which leads to more and more entities producing data about people.[17]

2.4 Conclusion

Although interviewed stakeholders might have differing definitions of the concept of the Internet of Things, for most of those we consulted, the Internet of Things is essentially about devices that are networked, that gather information and that are able to communicate. In general, the Internet of Things is considered a continuation of several earlier technological innovations, such as wireless internet connections, sensor technology and platforms. These aspects strengthen the trend of increasing importance of data collection and data use.

The Internet of Things is attracting a lot of attention, but no one can foretell its future. According to predictions by analysts and consultants, the number of consumer devices connected to the internet is set to rise spectacularly over the coming years. At the same time, in 2015, Gartner itself placed the Internet of Things at the top of its Hype Cycle for Emerging Technologies (Gartner 2015c). This suggests that it may take some five to ten years more before mainstream adoption of the Internet of Things will take off. Mike Liebhold said he was a bit sceptical about the development of technology in general, and pointed to several problems on the path to adoption of the Internet of Things (interoperability and standardisation among others). Experts in a PEW survey expressed scepticism about the importance of the Internet of Things for consumers, predicting that it would mainly serve special purposes in environments such as hospitals and battlefields, but not in everyday life (PEW 2014, p. 8-9). In fact, the growth in consumer demand for Internet of Things devices is much slower than the industry had initially hoped, with price, privacy and security, and ease of use as the three main roadblocks (Accenture 2016).

Nevertheless, the real value of Internet of Things solutions will unquestionably lie in the analysis of data from multiple sensors and decision-making based on those data (McKinsey Global Institute 2015, p. 104). The changes enumerated in section 2.1 all point to the increasing importance of data collection and data use. From a business perspective the Internet of Things can change every activity in the value chain, and data is at the core of reshaping the value chain (Porter and

---

15 Lee Tien, 3 December 2015, San Francisco.
16 Marcia Hofmann, 19 August 2015, San Francisco.
17 Chris Maresca, 30 September 2015, San Francisco.

Heppelman 2015, p. 99). This means that for policy-making, it is crucial to understand how companies and other stakeholders position themselves in the discussion about privacy in the Internet of Things. This is explored in the next three chapters.

3 Privacy perspective

To understand the privacy implications of the Internet of Things it is essential to know how different stakeholders in the debate conceptualise privacy; that is, define (descriptive) and/or value (normative) privacy (Gavison 1980, p. 424). The ways in which companies interpret the concept of privacy affect how they operationalise it in the designing of their Internet of Things products and services. Similarly, the manner in which policy-makers, legal scholars, digital rights organisations, and other participants to the debate approach privacy determines what types of privacy issues they foresee for the Internet of Things and what type of solutions they propose. This chapter gives an account of how legal scholars and philosophers conceptualise privacy (3.1) and how it is viewed by other stakeholders in the debate, such as companies and regulators (3.2). The next chapter applies these ideas to the Internet of Things.

3.1 Legal scholars and philosophers on privacy

Privacy has been discussed from various perspectives including social, economic, legal, and philosophical. The legal-philosophical discourse is dominant when it comes to articulating the concept of privacy (Roessler 2008).[18] Most sociological theories are interested mainly in the public sphere and understand privacy as the realm of intimacy or the family household (Roessler 2005). The sociology branch of surveillance examines privacy regimes as a means to limit surveillance (Ball et al. 2012, p. 3), but for the definition of privacy, surveillance studies scholars rely on legal and philosophical notions (g.e. Rule in Ball et al. 2012, p. 65). In economics, privacy is usually conceived of as the disclosing or withholding of personal information (Posner 1978), which, as will be demonstrated, does not cover all dimensions of privacy. Given these considerations, and because the legal framework is central to policy-making, this chapter adopts a legal-philosophical perspective on privacy in the Internet of Things.

Origins of the discussion about privacy in the United States

The modern discussion about privacy started in 1890 when Samuel D. Warren and Louis D. Brandeis posited that it was time to secure for individuals a right to privacy, which they defined as “the right to be let alone” (Warren and Brandeis 1890). In their now famous law review article, the jurists noted how new technologies such as instant photography and the rise of the gossip press had invaded private and domestic life. They found that existing common law afforded the principle of “inviolate personality” that could be invoked to protect the individual against privacy violations caused by things like the unauthorised circulation of portraits of private persons, or the publication of the sexual relations of the elite in the daily papers. Warren and Brandeis laid the basis for three quarters of a century of privacy litigation in the United States (Bloustein 1964, p. 962), which culminated in a complex of four privacy torts (Prosser 1960). Nevertheless, major (philosophical) discussion of the value of privacy only arose in the late sixties (Schoeman 1984, p. 1).

---

18 See for example the overview of privacy theories in the International Encyclopedia of the Social & Behavioral Sciences (Hughes 2015). It refers almost exclusively to legal and philosophical interpretations of the concept of privacy.

In response to scientific and technological advances in the 1960s and 1970s, American jurists and philosophers adopted the concept of privacy as control over personal information (in the United States this is commonly called “information(al) privacy”). New techniques for surveillance, electronic eavesdropping and psychological testing, and in particular the invention of data banks and computerised processing of personal data, raised fears among the public over privacy. Against this background Allan F. Westin developed the idea that “[p]rivacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others” (Westin 1967, p. 7). According to the legal scholar, the value of privacy lay in achieving individual goals of self-realisation (Westin 1967, p. 39). Over the years, his notion of privacy as control over personal data became the predominant theory for public policy (Solove 2002, p. 1109).

Privacy discussions on an international level

Another storyline shows how the concept of privacy relating to the house, family life, and (personal) correspondence was firmly established on an international level in the mid-nineteenth century. From the 14th to the 18th centuries, people went to court for eavesdropping or for opening and reading personal letters (Holvast 2007, p. 740). But nowhere was “privacy” used as an umbrella term for all these private spheres (Diggelman and Cleis 2014, p. 448). The Fourth Amendment to the United States Constitution, ratified in 1791, is considered to contain the most comprehensive reference to privacy, albeit not explicitly. It secured “the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures [by government officials]”. National constitutions in Europe and elsewhere in the Americas protected the privacy of the home and correspondence in a more fragmented way (Diggelman and Cleis 2014, p. 448). Then, spurred by the Second World War, the United Nations drafted the Universal Declaration of Human Rights (UDHR), which was subsequently adopted in 1948. The UDHR protected everyone’s “privacy, family, home or correspondence, [and] honour and reputation” (Article 12). This perpetuated a broad notion of privacy connected to the values of human dignity and freedom (Preamble of the UDHR).

A similar concept of privacy became embodied in the European Convention on Human Rights (ECHR), the first multi-country binding agreement on human rights. On a regional level, the two world wars had also led to the foundation of the Council of Europe (CoE). This human rights organisation initiated the ECHR, which came into effect in 1953. The convention declared that “[e]veryone has the right to respect for his private and family life, his home and his correspondence” (Article 8, paragraph 1). The ECHR itself intentionally avoided references to values such as liberty, human dignity, autonomy, or self-determination, because of the constitutional differences among the European Member States (De Hert and Gutwirth 2009, p. 14). Nevertheless, via case law of the European Court of Human Rights, the principle of personal autonomy and other values gained importance within the human right to privacy (De Hert and Gutwirth 2009, p. 15).

The concept of control spreads through Europe

In the 1970s, Europe was also confronted with the advent of computers and electronic data filing, and in response adopted the concept of privacy as control over personal data (in Europe this field is usually denoted as “data protection”). The debate on these issues in the United States exercised

considerable influence (Bygrave 2010, p. 167). European experts paid great attention to the early works of Alan Westin and Arthur Miller (Bennett 1992, p. 140-141), and framed their concerns over the new information and communication technologies (ICTs) mainly in terms of control. These concerns, and the increasing flow of personal data across borders, made the Council of Europe realise that the protection of privacy should be more specific and systematic than provided for by Article 8 of the European Convention on Human Rights.[19] This led to the conclusion of the *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108)* in 1981. Convention 108 lay down principles for fair and lawful collection and automatic processing of data and provided individual data subjects measures of control, such as the right to know that information is stored on her and, if necessary, to have it corrected.[20]

Fair information practices with an economic dimension

The idea of privacy as control over personal data led to the formation of the fair information practices (FIPs).[21] In the United States a government advisory committee established by the Department of Health, Education and Welfare tried to formulate a Westin-like concept of privacy that was consistent with electronic records. The committee observed that records were usually made for purposes that are shared by institutions and individuals. They concluded that personal privacy had to be understood in terms of mutuality, meaning that the individual should share her control over her information with the record-keeping organisation (HEW report 1973, p. 40). Based on this concept, the committee developed certain fundamental principles of fair information practices that should safeguard personal privacy in the context of electronic record keeping (HEW report 1973, p. 41-42). These fair information practices formed the basis for data protection initiatives all around the world, with the OECD Privacy Guidelines being the version most often cited (Gellmann 2015, p. 8).

Since the formulation of the fair information practices, informational privacy or data protection became pragmatic and acquired an economic dimension. The doctrine now assumes that private and public actors need to be able to use personal data because this is often necessary for societal reasons (De Hert and Gutwirth 2009, p. 3). This is apparent in the EU's Data Protection Directive (DPD), and the General Data Protection Regulation (GDPR) that is set to replace it. The DPD has a double objective: to protect people's right to privacy with respect to the processing of personal data and to ensure the free flow of personal data within the Internal Market. Similarly, the OECD Privacy Guidelines, adopted in 1980 and updated in 2013, aim to protect privacy and also to ensure that differing national privacy laws do not unduly restrict transborder data flows and the economic and social benefits which they bring (OECD 2013, p. 69). By contrast, concepts of privacy as a right to be let alone, privacy as a human right, or privacy as focussed on the protection of individuality and human dignity (Bloustein 1964) function more as a defence shield against invasions by public and private entities, and cater for a more value-based approach towards privacy.

---

19 https://www.coe.int/t/dghl/standardsetting/dataprotection/History_more_en.asp

20 Also see Handbook on European data protection law, available via http://fra.europa.eu/en/publication/2014/handbook-european-data-protection-law

21 Also denoted as fair information principles (FIPs), or fair information practice principles (FIPPs).

3.2 Views on privacy from the field

The notion of privacy as control over personal data is dominant among the stakeholders interviewed. Marcia Hofmann, private attorney in the Bay area, thinks that the real flash-point of privacy today is the question of control. She recognises that people can have different conceptions of privacy, and may mean something different when they state that privacy is important for them. But in her view, privacy is (increasingly) about the right to have control over data.[22] Similarly, Brendon Lynch, Chief Privacy Officer at Microsoft, understands privacy as control. He describes a development from twenty to thirty years ago when privacy was more akin to secrecy, to the present, where it is much more about control and the ability to influence what data is collected about you. For Microsoft this led to the concept of trust, since the company thinks that consumers will only use technology they trust. And now that technology is becoming more integrated into our physical world and our daily lives, Microsoft concludes that an important driver of that trust relates to data collection and use.[23] Chris Maresca from Sherbit and Mike Liebhold from the IFTF also talk about privacy mainly in terms of control and consent.[24] This observation is backed up by Chris Hoofnagle, Faculty Director of the Berkeley Center for Law and Technology, who states that much of US privacy is about control over data.[25] For Google, privacy is about giving users control over the relationship they want to have with Google. This is achieved by giving users information and the opportunity to adjust privacy settings in a central place.[26]

Among the stakeholders we interviewed there seemed to be agreement that computer/information security is a precondition to privacy, but it has not yet been decided how exactly the two relate to each other. People with a technologist or security frame of mind may tend to equate the two. Mike Liebhold, tech researcher at the Institute for the Future, takes the strongest stance, maintaining that privacy and cyber security are the same thing.[27] Marcia Hofmann, who has a strong foothold in the computer security community, holds that privacy and security are two sides of the same coin. She gives the following example: it is a privacy protective step to collect and store less personal data. At the same time, this is a security protective step, because if there is a hack or a security breach there will be less personal data that can be leaked.[28] Yet, during the expert roundtable it was posited that privacy and security are really two separate things. One participant explained it as follows: for companies, security is an internal matter, focussed on keeping personal data within the organisation and aided by measures at the technical level. Privacy, then, is a matter of public representation, focussed on the question of how the organisation uses and monetises personal data. In that sense, security is largely about technology and privacy largely about policy.[29]

Finally, some of the stakeholders we interviewed have the impression that tech companies in Silicon Valley may conceptualise privacy in a particular way for their own benefit. Clearly, they were

---

22 Marcia Hofmann, 19 August 2015, San Francisco.
23 Brendon Lynch, 22 September 2015, *via Skype*.
24 Chris Maresca, 30 September 2015, San Francisco.
25 Chris Hoofnagle, 21 August 2015, Berkeley.
26 Google, 11 September 2015, Mountain View.
27 Mike Liebhold, 20 August 2015, Palo Alto.
28 Marcia Hofmann, 19 August 2015, San Francisco.
29 Expert roundtable, 12 November 2015, San Francisco.

careful in articulating such observations and emphasise that they are based on anecdotal evidence. Chris Hoofnagle, Director of the Berkeley Center for Law and Technology, observes how, for example, Facebook explains privacy as about control, and thus gives its users lots of opportunities to customise their privacy settings. At the same time, the company sits back and waits for the consumer to give up masses of personal data.[30] The question is then whether this kind of control translates into privacy. Marcia Hofmann speculates that some companies feel that privacy is about not publicly exposing people. From that perspective, an organisation can collect tremendous amounts of personal data and draw inferences from it, as long as they do not open up the information to peers.[31] Lee Tien, Senior Staff Attorney at the Electronic Frontier Foundation (EFF), explains perceived differences between the standpoints of companies and privacy advocates differently. He does not think big tech companies have a very particular concept of privacy. He expects that they (the companies) might agree with him on what privacy entails, but that they will hold that consumers are trading some of their privacy in return for getting the benefits of new devices. While Tien may conclude that this is a bad bargain for the end user, companies might consider it a good trade-off.[32]

3.3 Conclusion

On the basis of the overview above, we can distinguish broader and narrower concepts of privacy in the United States and in Europe. Broader concepts of privacy include ideas like privacy of the home and correspondence, and references to human dignity and the development of one's personality. Narrow concepts of privacy frame it mainly as the protection and control of personal data, and these conceptions come these days with an economic dimension. This narrow concept of privacy as control over personal data was dominant among the stakeholders that we interviewed for this research. The next chapter thinks through what this might mean for the discussion about privacy in the Internet of Things.

30 Chris Hoofnagle, 21 August 2015, Berkeley.
31 Marcia Hofmann, 19 August 2015, San Francisco.
32 Lee Tien, 3 December 2015, San Francisco.

4 Future perspective

4.1 A loss of control over personal data

From the perspective that privacy is about control, the biggest concern for privacy in the Internet of Things is that consumers will lose control over their personal data. Many Internet of Things devices will not have a screen or another user interface via which consumers can exercise control (Ziegeldorf et al. 2015). Also, if houses are filled with up to fifty devices that collect and process personal data, it could be too much for consumers to control all these data flows. These concerns were shared by the stakeholders at the roundtable and in the interviews.[33]

A recurrent theme in our stakeholder consultations was optimism about user control. Brendon Lynch, Chief Privacy Officer at Microsoft, thinks that people want to benefit from new technologies, while being able to influence what data is collected about them and what is done with that data. The types of control he suggests include enabling people to place limits on data collection, or to opt out of particular uses, or sharing of data.[34] In our one-to-one interview, Google acknowledges that the manner in which organisations currently provide control, such as through a screen and with click buttons, might not work in the Internet of Things. But they point out that that is not the only viable way to provide control to end users, and they think there will always be ways to build user control into Internet of Things devices,[35] such as Google's Project Soli.[36] This team works on technologies in which hand movements in the air can be used to interact with wearables and other digital devices. Alternatively, the ability could be built in for consumers to turn off data streams, or systems could be designed with local storage and processing where data is highly sensitive.[37]

During the expert roundtable, participants suggested improvements for providing user control, the most important being granular permissions (also called "incremental authorisations").[38] This is a new approach for apps for mobile operating systems and could be applied to the Internet of Things. Granular permissions systems allow the user to select permissions to access or use data (eg from a smart phone's location, camera, contacts, photos, or microphone) specific to each app and device feature. The granular system then requires apps to ask for user permissions only as a particular feature is needed, as opposed to an all-or-nothing choice when the app is installed.[39] Both Chris Maresca from the personal analytics app Sherbit and Lee Tien from the Electronic Frontier Foundation also argue that granular permissions are an improvement for the consumer.[40] One study found that users are indeed better able to comprehend the associated trade-offs in granular permission systems for mobile sensing applications, and are ready to invest time to configure each

---

33 See expert roundtable in Annex II, 12 November 2015, San Francisco.

34 Brendon Lynch, 22 September 2015, *via Skype*.

35 Google, 11 September 2015, Mountain View.

36 https://www.google.com/atap/project-soli/

37 Chris Hoofnagle, 21 August 2015, Berkeley

38 Expert roundtable, 12 November 2015, San Francisco.

39 https://fpf.org/2015/06/23/android-m-and-privacy-giving-users-control-over-app-permissions/

40 Chris Maresca, 30 September 2015, San Francisco; Lee Tien, 3 December 2015, San Francisco.

setting manually (Christin et al. 2014). Next, user control could be aided with machine-readable privacy policy statements (e.g. statements that can be checked automatically by software to see if they match with a user's defined set of privacy preferences). Some participants to the roundtable also saw value in the development of taxonomies for data in order to design frameworks for user control. Taxonomies of personal data by origin could indicate which categories of data require additional protections, such as explicit consent by the user before the data can be collected.

4.2 Beyond a narrow concept of privacy

On the other hand, the stakeholders we interviewed also (implicitly) look beyond the idea that privacy is about full consumer control. For example, for Brendon Lynch from Microsoft, providing user control is connected to a risk-based approach to privacy. He foresees that consumers will be overwhelmed if the organisation provides choice for everything.[41] Instead, in a risk-based approach, the organisation determines beforehand what the most sensitive data is, and the most sensitive sort of data uses, to provide people with meaningful control. Various participants in the expert roundtable stated that they support risk-based approaches. For Microsoft, the control notion also led to the concept of trust, since the company thinks that consumers will only use technology that they trust. And now that technology is becoming more integrated into our physical world and our daily lives, Microsoft concludes that an important driver of that trust relates to data collection and use.[42]

In addition, stakeholders recognise that the Internet of Things may necessitate a refocus on software liability and consumer protection to complement the control notion. Chris Hoofnagle observes that recently in the United States, the Federal Trade Commission has been taking more of a consumer protection stance.[43] He thinks consumer protection is an efficient way to protect consumer privacy, if it is done right. Hoofnagle supposes that regulators and policy-makers will realise that privacy policies are inadequate and that they should issue norms to be followed instead.

Participants to the workshop also discussed software liability with a view to privacy. In their line of reasoning, ordinary consumers should not be asked to decide about certain types of risks of data collection and data use. They note that in certain cases, consumers will not be able to evaluate the risks involved, and in other cases consumers will just not care to make those decisions. The participants of the roundtable concluded that the manufacturers of Internet of Things devices should be responsible for performing complicated risk assessments of certain types of data collection and data use, incentivised by liability and consumer protection law.

Some privacy concerns of interviewees relate to the broader notions of privacy discussed in 3.1, including value-laden aspects like the idea that privacy is in essence about human dignity, autonomy, or self-realisation. Elaine Sedenberg, for example, raises questions about the effects on self-realisation and self-development for children in particular, if vast data repositories and data legacies could potentially follow them around for years to come.[44] Even if all data protection

---

41 Brendon Lynch, 22 September 2015, *via Skype*.

42 Brendon Lynch, 22 September 2015, *via Skype*.

43 Chris Hoofnagle, 21 August 2015, Berkeley; also see Hoofnagle 2016.

44 Elaine Sedenberg, 21 August 2015, Berkeley.

requirements are met, a permanent data archive combined with predictive capabilities can still be highly privacy invasive. Think for example of smart TVs with internet connections, and the possibility of using the TV as a controller for all smart devices in a household. Such TVs have implications not just for the family member who is watching the news, but for everyone in and around the house. In theory the consumer may be in total control of the TV and the smart home system, but questions arise about the effect on her sense of self-determination, and about the ethical boundaries if Samsung were to use and repurpose the sensor data where she has consented that her personal data may be used for aggregation and analysis. How will systems like these, in which everything in the home is hooked up to a central controller, affect the unhindered identity development of all five of her family members? These questions cannot be answered under the current 'control paradigm'.

4.3 Conclusion

From our interviews and roundtable meeting it becomes clear that most stakeholders, including tech companies, recognise that the perspective of privacy as control over personal information will have its limits when the Internet of Things comes into full bloom. In that sense, Microsoft's shift to the notion of trust and the risk-based approach can be regarded as a search for new or additional approaches for safeguarding privacy that they feel will be required in the era of the Internet of Things. Other stakeholders see promising or additional approaches in consumer protection law and software liability. Tech companies might not think the Internet of Things requires radical new privacy solutions and legal regimes, but it is also clear to them that current privacy solutions won't be sufficient for addressing privacy issues related to the Internet of Things.

Looking at academic perspectives on privacy (see 3.1), it also becomes clear that the broader concepts of privacy remain underexposed in current stakeholder discussions. These are more value-laden aspects like the idea that privacy is in essence about human dignity, autonomy, or self-realisation. During the expert roundtable, participants were asked several times to reflect on such broader notions of privacy (Questions 2.4, 3.3, and 3.4). In general, these questions evoked musing among participants about such issues as the effect on people's behaviour of being continuously monitored and the trade-off between privacy and interests such as safety. But it proved hard to trigger a more substantial discussion on notions of privacy which are not confined to control over personal data.

5 Conclusion

Goal of the study

The idea of connecting everyday devices to the Internet has long been a fascination of projects in technology labs. Today, the Internet of Things actually seems to be making its way to consumer households. All these smart devices collect detailed information about their surroundings, which raises questions about the ways in which we can safeguard privacy in an Internet of Things era. This exploratory study aims to inform policy-makers in the Netherlands about privacy implications, and potential solutions for privacy in the Internet of Things. It maps stakeholder views on privacy and the Internet of Things in Silicon Valley – the unofficial tech region of the world – and explores the kinds of privacy issues and solutions which stakeholders foresee. We held semi-structured interviews in Silicon Valley and organised an expert roundtable in Silicon Valley with experts from academia, industry, government, and civil society.

Data taking central position

On the one hand, stakeholders consider the Internet of Things as a continuation of existing developments in information technology, increasing networking capabilities and the growing pervasiveness of computing technologies. On the other hand, they think it heralds a new phase of internet development, where the digital and physical worlds come together. At this point, the Internet of Things is still in its early stages, but expectations of its potential growth are high. Stakeholders point out that when it comes into full bloom, data streams will start to permeate everyday life to an unprecedented degree. This raises questions about whether existing ways of protecting privacy will prove sufficient for the Internet of Things.

Conceptualisations of privacy

The legal-philosophical discourse in Chapter Two shows that it is possible to distinguish between broader and narrower concepts of privacy in both the United States and Europe. Broad concepts of privacy include ideas like privacy of the home and correspondence, and references to human dignity, autonomy and self-realisation. These concepts can be found, for example, in the Universal Declaration of Human Rights (UDHR) and the European Convention on Human Rights (ECHR). Narrow concepts of privacy mainly frame it as the protection and control of personal data (e.g. information privacy or data protection) and can be found in the OECD privacy principles and in the EU's Data Protection Directive (DPD), along with the General Data Protection Regulation (GDPR) which will replace it. These narrow conceptions of privacy have become an important, practical way for policy-makers and companies to think about privacy, and they include an economic dimension. The doctrine now assumes that private and public actors need to be able to use personal data because this is often necessary for economic and societal reasons.[45]

---

[45] This is apparent in the EU's Data Protection Directive. It has a double objective: to protect people's right to privacy with respect to the processing of personal data and to ensure the free flow of personal data within the Internal Market. It is also dominant among the stakeholders interviewed for this research.

Limits of control: in search of new approaches that shift the burden of control
The stakeholders consulted for this study all conceptualise privacy in terms of control over personal data. Their main concern is that users will lose control in the Internet of Things. Many smart devices will not have a screen or any kind of user interface through which consumers can exercise control. In addition, the amount of devices collecting data about consumers is expected to grow fast, and it may be too much for consumers to control all these data flows. Some stakeholders do express optimism about finding new ways to offer control to consumers, via new intuitive interfaces and granular permissions. Nevertheless, most consulted stakeholders recognise that the concept of privacy as control over personal information (e.g. information privacy or data protection) has its limits when it comes to respecting consumers' privacy in the Internet of Things. It places the burden of control over privacy largely in the hands of the consumer, while at the same time it becomes more difficult for that consumer to remain in control.

With the arrival of the Internet of Things, we see stakeholders searching for new concepts and solutions, such as trust-based approaches and the improvement of software liability and consumer protection oversight. These approaches are beginning to shift the burden of control of privacy from the consumer to the companies offering Internet of Things services, and to supervisory authorities with strong oversight of these companies. Such approaches are already common in the development of traditional products (think, for example, of safety guidelines for Barbies, televisions and cars). Considering the (practical) limits of control for consumers in the Internet of Things, the Rathenau Instituut believes that similar approaches should be explored for Internet of Things services, where the burden of control is not placed solely upon consumers. Concepts like trust, shared responsibility and accountability are essential to such approaches.

In search of new approaches: safeguarding autonomy, self-realisation and human dignity
However, privacy concerns are not limited to loss of control. The Internet of Things also impacts on more value-laden aspects of privacy, such as autonomy and self-realisation, via detailed profiling and possibilities for persuasion, for example. Consider the smart TV mentioned in paragraph 4.2 where the idea of control over data does not take into account the effects of the smart TV's monitoring on other family members, and on the unhindered development of their identities. It is therefore important to include the safeguarding of autonomy, self-realisation and human dignity in the search for new approaches to the protection of privacy in the Internet of Things.

At the same time, we still need to learn how to properly *articulate* the way in which these concepts relate to governing data. In our stakeholder discussions, it proved difficult to step outside of the 'control paradigm' to think of practical solutions for the protection of aspects of privacy such as autonomy. In academia, scholars are discussing how pervasive computing technologies, including the Internet of Things might impact fundamental human values like human dignity, autonomy and identity development (Van Est et al. 2016). But, we are still a long way from translating such concepts into actual software design practices and practical guidelines. In law-making, privacy is also in flux. New regulations are in the pipeline in Europe and the United States in which policy-makers juggle with different developments and interests such as fighting terrorism, preventing monopolies and safeguarding personal freedom.

New discussion on ethics

An important step in the articulation of new concepts is the activation of discussions related to the Internet of Things, involving politicians, civil society, consumers and tech companies. A recent initiative of the European Data Protection Supervisor (EDPS) is a case in point. EDPS established an Ethics Advisory Group, calling for a broader discussion on a new digital ethics to safeguard human values in the context of new technologies such as the Internet of Things (EDPS 2015; 2016) – implying that such discussion should not merely be conducted in terms of data protection. The Rathenau Instituut believes that such initiatives can help in the search for valuable new approaches to safeguard privacy, autonomy, self-realisation and human dignity, where companies, consumers and public supervisory authorities share the responsibility.

Bibliography

All hyperlinks were last accessed on 28 March 2016.

Accenture, *Digital Consumer Survey: Igniting Growth in Consumer Technology*, 2016, available at <https://www.accenture.com/_acnmedia/PDF-3/Accenture-Igniting-Growth-in-Consumer-Technology.pdf>.

Accenture, *The Internet of Things: The Future of Consumer Adoption*, 2014, available at <https://www.accenture.com/t20150624T211456__w__/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Technology_9/Accenture-Internet-Things.pdf>.

Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari and Moussa Ayyash, 'Internet of Things: A Survey on Enabling Technologies, Protocols and Applications', *IEEE Communications Surveys & Tutorials*, 2015 (4), p. 2347-2376.

René Arnold, Annette Hillebrand and Martin Waldburger, *Personal Data and Privacy* (study for Ofcom), Bad Honnef: WIK-Consult GmbH, 2015, available at <http://stakeholders.ofcom.org.uk/binaries/internet/personal-data-and-privacy/Personal_Data_and_Privacy.pdf>.

Kevin Ashton, 'That "Internet of Things" Thing', *RFID Journal*, 22 June 2009, available at <http://www.rfidjournal.com/articles/view?4986>.

Colin J. Bennett, 'In Defence of Privacy: The concept and the regime', *Surveillance & Society*, 2011 (4), p. 485- 496, available at <http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/4184>.

Colin J. Bennett and Charles Raab, *The Governance of Privacy: Policy Instruments in Global Perspective*, Cambridge, MA: MIT Press, 2006.

Colin J. Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*, Ithaca: Cornell University Press, 1992.

Edward J. Bloustein, 'Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser', *New York University Law Review*, 1964 (6), p. 962-1007.

Eva Bucherer and Dieter Uckelmann, 'Business Models for the Internet of Things', in: Dieter Uckelmann, Mark Harrison and Florian Michahelles (eds.), *Architecting the Internet of Things*, Berlin: Springer, 2011, p. 253-278.

Giovanni Buttarelli, *European Data Protection Supervisor Decision of 3 December 2015 establishing an external advisory group on the ethical dimensions of data protection ('the Ethics*

Advisory Group'), Brussels: European Data Protection Supervisor, 3 December 2015, available at <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Advisory%20Group/15-12-03_EthicsGroup_Decision_EN.pdf>.

Lee A. Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits*, The Hague: Kluwer Law International, 2002.

Oliver Diggelman and Maria N. Cleis, 'How the Right to Privacy Became a Human Right', *Human Rights Law Review*, 2014 (3), p. 441-458.

Remco M. Dijkman, Bram Sprenkels, Thijs Peeters and Alexandre Janssen, 'Business models for the Internet of Things', *International Journal of Information Management*, 2015 (6), p. 672-678.

Nico van Eijk, Ronan Fahy, Harry van Til, Pieter Nooren, Hans Stokking and Hugo Gelevert, *Digital platforms: an analytical framework for identifying and evaluating policy options*, Den Haag: TNO, 2015, available at <http://www.ivir.nl/publicaties/download/1703>.

Rinie van Est, Jelte Timmer, Linda Kool, Niels Nijsingh, Virgil Rerimassie and Dirk Stemerding, *Rules for the digital human park. Two paradigmatic cases of breeding and taming human beings: Human germline editing and persuasive technology*. Background Paper prepared for 11th Global Summit of National Ethics/ Bioethics Committees. 16-18 March, Berlin, 2016, available at <https://www.globalsummit-berlin2016.de/documents-and-links>.

European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Internet of Things: an action plan for Europe* (COM(2009) 278 final), Brussels, 18 June 2009.

Peng-fei Fan and Guang-zhao Zhou, *Analysis of the Business Model Innovation of the Technology of Internet of Things in Postal Logistics*, Changchun: IEEE, 2011.

Elgar Fleisch, Markus Weinberger and Felix Wortmann, *Business Models and the Internet of Things*, Zurich: Bosch IoT Lab, 2014, available at <http://www.iot-lab.ch/wp-content/uploads/2014/11/EN_Bosch-Lab-White-Paper-GM-im-IOT-1_3.pdf>.

Gartner, 'Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015', 10 November 2015, available at <http://www.gartner.com/newsroom/id/3165317>.

Gartner, *Market Guide for IoT Platforms*, 2 July 2015.

Gartner, Gartner's 2015 Hype Cycle for Emerging Technologies Identifies the Computing Innovations That Organizations Should Monitor, 18 August 2015, available at <http://www.gartner.com/newsroom/id/3114217>.

Ruth Gavison, 'Privacy and the Limits of Law', *Yale Law Journal*, 1980 (3), p. 421-471 <http://ssrn.com/abstract=2060957>.

Bob Gellman, *Fair Information Practices: A Basic History*, 2015, available at <http://bobgellman.com/rg-docs/rg-FIPShistory.pdf>.

Neil Gershenfeld, Raffi Krikorian and Danny Cohen, 'The Internet of Things', *Scientific American*, 2004 p. 76-81.

Neil Gershenfeld, *When Things Start to Think*, New York, NY: Henry Holt and Company, 1999.

Samuel Greengard, *The Internet of Things*, Cambridge, MA: MIT Press, 2015.

Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile de Terwange and Sjaak Nouwt (eds.), *Reinventing Data Protection*, Dordrecht: Springer, 2009.

Gregor Harter and Jörg Böckmann, *Hardware Goes Software: How Manufacturers Can Think and Act Like Software Companies*, Booz & Company, 20 December 2010.

Mireille Hildebrandt, *Smart Technologies and the End(s) of Law*, Cheltenham: Edward Elgar Publishing, 2015.

Jan Holvast, 'History of Privacy', in: Karl d. Leeuw and Jan Bergstra (eds.), *The History of Information Security: A Comprehensive Handbook*, Amsterdam: Elsevier, 2007, p. 737-768.

Kirsty Hughes, 'The social value of privacy, the value of privacy to society and human rights discourse', in: Beate Roessler and Dorota Mokrosinska (eds.), *Social Dimensions of Privacy: Interdisciplinary Perspectives*, Cambridge: Cambridge University Press, 2015, p. 225-243.

Chris Hoofnagle, *Federal Trade Commission Privacy Law and Policy*, Cambridge: Cambridge University Press, 2016.

International Telecommunication Union, *The Internet of Things*, Geneva: International Telecommunication Union, 2005, available at <https://www.itu.int/net/wsis/tunis/newsroom/stats/The-Internet-of-Things-2005.pdf>.

Maurits Kreijveld, Jasper Deuten and Rinie van Est (eds.), *De kracht van platformen: Nieuwe strategieën voor innoveren in een digitaliserende wereld*, Den Haag: Rathenau Instituut, 2014.

Seppo Leminen, Mika Westerlund, Mervi Rajahonka and Riika Siuruainen, 'Towards IoT Ecosystems and Business Models', in: Sergey Andreev, Sergey Balandin and Yevgeni Koucheryavy (eds.), *Internet of Things, Smart Spaces, and Next Generation Networking*, Berlin: Springer, p. 15-26.

Huan Li and Zheng-zhong Xu, 'Research on Business Model of Internet of Things Based on MOP', in: Ershi Qi, Jiang Shen and Runliang Dou (eds.), *Proceedings of the International Asia Conference*

on Industrial Engineering and Management Innovation (IEMI2012), Berlin: Springer, 2013, p. 1131-1138.

Liran Liu and Wei Jia, 'Business model for drug supply chain based on the Internet of Things', in: *Proceedings of 2nd IEEE International Conference on Network Infrastructure and Digital Content (IC-NIDC2010)*, IEEE, 2010, p. 982-986.

Oleksiy Mazhelis, Henna Warma, Seppo Leminen, Petri Ahokangas, Pasi Pussinen, Mervi Rajahonka, Riika Siuruainen, Hanna Okkonen, Alexey Shveykovsky and Jenni Myllykoski, *Internet of Things Market, Value Networks, and Business Models: State of the Art Report*, Jyväskylä: University of Jyväskylä, 2013, available at <http://www.internetofthings.fi/extras/IoTSOTAReport2013.pdf>.

McKinsey Global Institute, *The Internet of Things: Mapping the Value Beyond the Hype*, McKinsey Global Institute, June 2015, available at <http://www.mckinsey.com/insights/business_technology/the_internet_of_things_the_value_of_digitizing_the_physical_world>.

Steve Meloan, *Toward a Global Internet of Things*, Sun Microsystems, 11 November 2003, available at <http://wenku.baidu.com/view/16859b26ccbff121dd368320.html>.

Roberto Minerva, Abyi Biru, Domenico Rotondi, *Towards a Definition of the Internet of Things (IoT)*, IEEE Internet Initiative, 27 May 2015, available at <http://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf>.

OECD, *Machine-to-Machine Communications: Connecting Billions of Devices,* OECD Digital Economy Papers, No. 192, Paris: OECD Publishing, 2012, available at <http://dx.doi.org/10.1787/5k9gsh2gp043-en>.

OECD, *Building Blocks for Smart Networks*, OECD Digital Economy Papers, No. 215, Paris: OECD Publishing, 2013, available at <http://dx.doi.org/10.1787/5k4dkhvnzv35-en>.

Nasrine Olson, Jan M. Nolin and Gustaf Nelhans, 'Semantic Web, Ubiquitous Computing, or Internet of Things? A macro-analysis of scholarly publications', *Journal of Documentation*, 2015 (5), p. 884-916.

Charith Perera, Arkady Zaslavsky, Peter Christen and Dimitros Georgakopoulos, 'Sensing as a service model for smart cities supported by Internet of Things', *Transactions on Emerging Telecommunications Technologies*, 2014 (1), p. 81-93.

PEW, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, Pew Research Center, 12 November 2014, available at <http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/>.

Michael E. Porter and James E. Heppelman, 'How Smart, Connected Products are Transforming Companies', *Harvard Business Review*, October 2015, p. 96-114 <https://hbr.org/2015/10/how-smart-connected-products-are-transforming-companies>.

William L. Prosser, 'Privacy', *California Law Review*, 1960 (3), p. 383-423 <http://scholarship.law.berkeley.edu/californialawreview/vol48/iss3/1/>.

Antonio Regalado, 'Business Report: The Internet of Things', *MIT Technology Review*, 2014.

Beate Roessler, 'New Ways of Thinking about Privacy', in: John S. Dryzek, Bonnie Honig and Anne Phillips (eds.), *The Oxford Handbook of Political Theory*, Oxford: Oxford University Press, 2008, p. 694-713.

Samsung, 'Samsung Reveals Entire 2016 Smart TV Line-Up will be IoT Ready', Korea, 29 December 2015, available at <http://news.samsung.com/global/samsung-reveals-entire-2016-smart-tv-line-up-will-be-iot-ready>.

Sanjay Sarma, David L. Brock and Kevin Ashton, *The Networked Physical World: Proposals for Engineering the Next Generation of Computing, Commerce & Automatic-Identification*, Cambridge, MA: MIT Auto-ID Center, 2000, available at <http://cocoa.ethz.ch/downloads/2014/06/None_MIT-AUTOID-WH-001.pdf>.

Ferdinand D. Schoeman, *Philosophical Dimensions of Privacy: An Anthology*, Cambridge: Cambridge University Press, 1984.

Paul Schwartz, 'Privacy and Democracy in Cyberspace', *Vanderbilt Law Review*, 1999 (6), p. 1609-1701, available at <http://ssrn.com/abstract=205449>.

Daniel J. Solove, 'Conceptualizing Privacy', *California Law Review*, 2002 (4), p. 1087-1156, available at <http://ssrn.com/abstract=313103>.

Yunchuan Sun, Hongli Yan, Cheng Lu, Rongfang Bie and Peter Thomas, 'A holistic approach to visualizing business models for the internet of things', *Communications in Mobile Computing*, 2012 (1:4), available at <http://muxjournal.springeropen.com/articles/10.1186/2192-1121-1-4>.

The Economist, *The Internet of Things Business Index: A Quiet Revolution Gathers Pace*, ARM, 2013, available at <https://www.arm.com/files/pdf/EIU_Internet_Business_Index_WEB.PDF>.

TNS Opinion & Social, *Special Eurobarometer 431: Data Protection*, Brussels: European Commission, June 2015, available at <http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_sum_en.pdf>.

U.S. Department of Health Education & Welfare, *Records, Computers and the Rights of Citizens*, 1973.

United Nations, *Universal Declaration of Human Rights (UDHR)*, Paris: United Nations, 10 December 1948, available at <http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf>.

Jean-Philippe Vasseur and Adam Dunkels, *Interconnecting Smart Objects with IP: The Next Internet*, Amsterdam: Morgan Kaufmann, 2010.

Samuel D. Warren and Louis D. Brandeis, 'The Right to Privacy', *Harvard Law Review*, 1890 (5), p. 193-220.

Mark Weiser, 'The Computer for the 21st Century', *Scientific American*, September 1991, p. 94-104.

Mika Westerlund, Seppo Leminen and Mervi Rajahonka, 'Designing Business Models for the Internet of Things', *Technology Innovation Management Review*, 2014 (7), p. 5-14.

Alan Westin, *Privacy and Freedom*, New York: Atheneum, 1967.

Jan H. Ziegeldorf, Oscar G. Morchon and Klaus Wehrle, 'Privacy in the Internet of Things: Threats and Challenges', *Security and Communication Networks*, 2004 (7), p. 2728.

Appendix 1 Interviewed stakeholders

Chris Hoofnagle, Faculty Director, Berkeley Center for Law & Technology, 21 August 2015, Berkeley.

Elaine Sedenberg, PhD Student, Berkeley School of Information, 21 August 2015, Berkeley.

Google Public Policy and Government Relations, 11 September 2015, Mountain View.

Mike Liebhold, Senior Researcher and Distinguished Fellow, Institute for the Future (IFTF), 20 August 2015, Palo Alto.

Marcia Hofmann, Private Attorney, 19 August 2015, San Francisco.

Chris Maresca, Founder and Chief Technologist Officer, Sherbit, 30 September 2015, San Francisco.

Stefan Witkamp, Co-Founder and Commercial Director, Athom, 9 July 2015, Enschede, Netherlands

Lee Tien, Senior Staf Attorney, Electronic Frontier Foundation, 3 December 2015, San Francisco.

Brendon Lynch, Chief Privacy Officer, Microsoft, 22 September 2015, via skype.

Jaap-Henk Hoepman, Associate Professor of PETs and PbD, Radboud University Nijmegen, 6 July 2015, via skype.

Appendix 2 Participants Roundtable

Laura Berger, Attorney in the Division of Privacy and Identity Protection, Federal Trade Commission (FTC).

Jill Bronfman, Director of the Privacy and Technology Project at the Institute for Innovation Law and Adjunct Professor of Law in Data Privacy, UC Hastings College of the Law.

Steffi Bryson, Public Policy and Government Relations Senior Analyst, Google.

Eric Butler, Software Engineer in the Cloud and Service Computing group, IBM Research.

Nico van Eijk, Professor of Media and Telecommunications Law and Director of the Institute for Information Law (IViR), University of Amsterdam.

Sarah Johanna Eskens, Research Intern, Rathenau Instituut & Consulate General of the Netherlands.

Rinie van Est, Coordinator and Researcher, Rathenau Instituut.

Lauren Gelman, Founder of Blurry Edge Strategies and non residential fellow at the Center for Internet and Society, Stanford Law School.

Mark Nelson, Founder and Co-Director of the Peace Innovation Lab, Stanford.

Chris Maresca, Founder and Chief Technologist Officer, Sherbit.

Jasper Smit, Assistant Director at the Netherlands Foreign Investment Agency (NFIA), Consulate General of the Netherlands.

Bart van der Sloot, Privacy Researcher at the Institute for Information Law (IViR), University of Amsterdam.

Nina Taft, Senior Research Scientist on the Privacy Team, Google.

Lee Tien, Senior Staff Attorney, Electronic Frontier Foundation (EFF).

Jelte Timmer, Researcher, Rathenau Instituut.

Robert Thijssen, Attaché for Innovation, Technology, and Science, Consulate General of the Netherlands.

Appendix 3 Report Roundtable

Session 1 What is the Internet of Things?

What are the most important factors that will affect the development of the Internet of Things over the next few years? Will they foster or inhibit the development of the Internet of Things?

Various factors are highlighted. Enabling hardware technologies for the Internet of Things are advancing very fast. New technologies are becoming cheaper and smaller in size, and batteries more efficient. Open hardware speeds up development as well. This refers to a movement similar to open source, but now the *design* of hardware, along with permission to create a physical product from the design, is made available free of charge with an open licence (for example Arduino). On the software side, the use of high-level programming languages makes programming easier. It is stressed that many of the technologies that power the Internet of Things have in fact been around for a while.

In this context, there is discussion about the usefulness of Internet of Things applications. Participants to the roundtable foresee a challenge in analysing all the data. The question is how to make this data useful, not just for companies but for consumers as well. It is agreed that developers have to provide useful applications for the user. But what are useful applications? Some mention that there is a growing focus on letting users see and control their data. Others argue that simply giving users the opportunity to see their data will not the typical application in the Internet of Things. In their view, the Internet of Things is essentially about connecting the digital to the physical world. Arguably that should determine what application is useful for the user.

What new or existing business models will be used to monetise the Internet of Things? Will we see a further schism between data-driven business models and business models built on the sale of products?

It is suggested that revenue models for digital platforms might also apply to the Internet of Things: direct payment, advertising, access to services, or acquisition (the typical Silicon Valley startup idea). In reply, it is added that there might also be an interesting business model for transactional data, comparable with what credit card companies do. Some argue that we should not just look at business models from a privacy perspective. They point out that there are many business models for the Internet of Things based on the use of non-personal data. With respect to the platform aspect, it is noted that the network effects and scaling could be tremendous.

The topic leads to more debate about the value of the Internet of Things. According to some participants, its value is in society's new ability to access all this daily sensor data. For other participants, the value is not so much in the individual pieces of data, but in the capacity to link all the data together. It is also suggested that the value of the Internet of Things lies not so much in the sensor data, as in the metadata. This means that those business models which use Internet of Things metadata are most important for discussions of privacy.

Participants are unsure whether users will be willing to pay for privacy. Some stakeholders are sceptical about this and refer to work by Alessandro Acquisti to support their view. Participants see generational and geographical differences with respect to people's willingness to pay for privacy. The question of whether people are willing to pay for privacy is not seen as an all or nothing discussion. If about 30% of people are willing to pay, then companies should be able to explore that market. Furthermore, some observe that people's willingness to pay for privacy also depends on their understanding of risk. This would mean that as soon as users get a better understanding of the privacy risks in the Internet of Things, the dynamics around paying for privacy may change. Still others argue that ordinary consumers should not be asked to decide about certain types of risks of data collection and data use. They think that in certain cases, consumers will not be able to evaluate the risks involved, and in other cases consumers will just not care about making those decisions. As an example it is pointed out that car buyers in general are not knowledgeable or interested in what types of valves the cars have. The participants conclude that the manufacturers of Internet of Things devices should be responsible for performing complicated risk assessments of certain types of data collection and data use, and that at that point, liability and consumer protection should kick in. Still, some participants are clearly in favour of a risk-based approach instead of a tick-box mentality towards privacy compliance.

Session 2 Conceptualisations of privacy

What are the consequences of understanding privacy solely in terms of control over personal data? What are the implications for the division of responsibilities between the user and the company, when 'improved privacy' is operationalised as 'giving the user more control over her personal data'?

Whether or not individual control is appropriate for the Internet of Things is a dividing question. Some participants maintain that providing users with control is unpractical and missing the point. It would be unpractical because everyone's data is being collected on such a large scale that it will be impossible for individuals to exercise control. It would be missing the point because the real problem is not a matter of control over data, but of companies and governments using their power to collect data without any specific reason. It is also seen as a problem that in the Internet of Things many of the data may seem meaningless for the individual to control. However, the data will be processed until it creates value for other parties, at which point user control may become desirable. As an alternative, participants posit that we should be thinking about a new paradigm, such as duties of care for those who are collecting the data. Others strongly disagree and hold that user control is not impossible in the Internet of Things. They say that tools for individual control are being, and will be, developed; privacy assistants for example.

The control discussion is a reason for participants to bring up the issue of transparency. Discussants acknowledge that it is detrimental for companies to be completely open and transparent about their data practices (for example in privacy statements) as long as other companies are not transparent. But with less information, consumers are in less of a position to exercise control.

How should we understand the relation between privacy and security? What are the consequences when privacy is viewed solely as a matter of information security?

There seems to be agreement among participants that privacy and security are two separate things (even though they are of course related), and that device insecurity is a big issue in the Internet of Things. Someone explains it as follows: security would be an internal matter, focussed on keeping personal data within the organisation, aided by measures at the technical level. Privacy would then be a matter of public representation, focussed on the question of how you use and monetise personal data. On that basis, it is argued that there is a lack of incentive for companies to protect security. It is added that reputational harm as a consequence of data breaches often disappears over time. Participants draw attention to the fact that Internet of Things device makers do not see themselves as data collecting entities, and hence do not care about the security issues of the devices they produce. It is observed that for a lot of tech companies, privacy and security are merely an afterthought.

What are the effects on individuals and society when companies develop their privacy programmes with the aim of obtaining consumer trust? In that case, what should 'trust' mean and how can we ensure that this is real, enforceable trust?

Participants see both positive and negative aspects in the trend to understand privacy in terms of trust. On the one hand it may force companies to improve their communication and information provision for users. It is noted that trust is in fact already enforceable. Companies gain consumer trust if they make certain promises towards consumers. Regulators oversee whether companies live up to promises made.[46] On the other hand gaining consumer trust should also involve informing consumers about the risks of data collection. The problem for companies is knowing the risks and communicating this effectively on a mass basis. Discussants also point out that it is widely known that users do not read (privacy) notices. According to some, privacy policies should not even be used as a way to inform users. This would mean we should not focus the discussion on improving privacy policies. In conclusion, participants agree that stakeholders need to figure out how to inform users about data practices and privacy risks. It is suggested that consumers could be educated in new ways, for instance with games and comics.

Should we, and if so how can we, engage a broader concept of privacy in engineering and design practice? Can we expect engineers and designers to understand privacy in the same way as academics?

Initial disagreement about the question turns out to be agreement among some participants that privacy should not just mean information privacy. For some, this means that privacy should be understood as a trade-off with security, safety, and so forth. From that perspective, decreasing privacy may sometimes improve safety. Others are of the view that privacy should be valued for its importance to social relationships, democracy, and the like. They claim that this is the direction in which academic discussion about privacy is moving. Finally it is also posited that privacy may be better understood with the use of data taxonomies. Others dispute this for the reason that taxonomies will make access control too complex.

Session 3 Privacy issues in the Internet of Things

46 https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises

How can we provide for control over personal information if the typical Internet of Things-device lacks a user interface and is 'always on' by default? For example, how can we provide for notice and consent, or transparency about data collection?
This discussion follows up on the debate that developed under question 2.1 (about the pros and cons of individual control over personal data). Participants list different ways to implement user control: asking for consent at the moment a user chooses to use a certain feature of an Internet of Things device, that is in a granular fashion, instead of asking for a binary yes or no when the device is activated; asking for consent at the device level or the platform level; aiding consent with machine-readable privacy policies like those being developed at Carnegie Mellon University.

Nevertheless, participants again remind each other of the fact that just like control, consent may not work in an Internet of Things environment. Users might not want or might not be able to manage all the interactions with those connected devices in their living environment when they are asked for consent all of the time. In that respect, reference is made to research by Lorry Cranor.

How can companies comply with the principle of data minimisation (limiting the amount of personal data collecting only to what is directly relevant and necessary to accomplish a specified purpose) while also pursuing the benefits of the Internet of Things for their customers and their own business interests? Is data minimisation still possible in an Internet of Things era, or should we focus on responsible data use?
First and foremost, discussants argue that responsible data use and data minimisation is not an either or question. It is maintained that these notions play different roles and should both be respected. The group thinks aloud about ways to ensure data minimisation. Some put forward the idea that data minimisation could be enforced by public grading systems, in which companies or applications are publicly rated on data minimisation. This will also result in more public awareness. Furthermore it is stated that data minimisation may happen in preplanning, in the device (locally), or in the cloud.

Discussants share critical views on the data minimisation principle. They point out that data minimisation is just one of the options available for the protection of privacy. It is expected that advances in computing on encrypted data could be a game-changer in the debate. Besides, it is pointed out that data minimisation does not necessarily equal 'good' from a privacy perspective. For example, if users give up personal data to a privacy agent, this may in turn increase their personal privacy. Finally, some stakeholders see a problem of the commons: people do not want to give up their data (they desire data minimisation) whereas the use of the aggregate of lots of user data could be beneficial to the collective.

Can we expect this notion of physical or spatial privacy to play a role in the Internet of Things debate? Can we articulate such a notion of privacy? Is it possible to account for such a concept of privacy?
This question evokes musings among participants. One wonders how the feeling of being watched will affect people's behaviour. Another connects the question to the notion of a "reasonable expectation of privacy", which is essentially based on your physical location, and foretells that in the Internet of Things we will have to evaluate whether things are operating as expected based on our expectations of privacy. Still others reason that in the Internet of Things you cannot expect privacy

in relation to other peers in the network. The takeaway is that in the Internet of Things, the networked sharing of data is changing the dynamics and is the multiplier of privacy issues. This will affect reasonable expectations of privacy.

Will, and if so how will, the Internet of Things affect human agency and the capacity to develop one's identity? Should we be worried about the amount of information that is stored about young people growing up in an Internet of Things environment?
Like the previous question, this discussion point brings up varied responses. Participants think that the world changes when a lot more data about us becomes knowable due to the Internet of Things. They recognise that this can be beneficial, say for example where connected cameras in dorms increase security, but they also find that this may not be a good thing in terms of autonomy. In the dorm example, the presence of connected cameras may deter students from doing things that are part of being in college. Other participants reason the other way around. They expect that people will get used to the Internet of Things when they grow up with it, so that it will no longer affect their behaviour. Still others fear that connected devices tailored to your habits could get you trapped in a feedback loop.

The discussion moves towards the question of what privacy is about. Some participants hold that privacy is about the idea of having a space where you can experiment. They fear that with the Internet of Things, the private sphere as such becomes obsolete, which may result in people ending up in their own feedback loop or under the strong influence of companies or the government. Some agree that privacy is fundamental to autonomy. All participants acknowledge this is not a new question. Still, it is noted that the Internet of Things brings a new element to the discussion. According to some, the scale of the Internet of Things makes this technology qualitatively different from preceding technologies. Others add that the Internet of Things is different because of its widespread availability. It is ambient, and people will not be able to walk away from it. It is also argued that the Internet of Things is really a societal issue, because people will not experience direct harm on an individual level.

Session 4 Future solutions for privacy and the Internet of Things

How should we understand these opposing trends, and what will the outcome be in the long run? Will people be prepared to pay for privacy, either as a standalone product or service, or as a premium feature, or will people only be willing to pay for privacy indirectly as a part of the brand?
This topic has already partly been discussed in the context of question 1.2, but participants add some more considerations. Some discussants note that users are asking for more tools to control their data. Therefore it is expected that companies which embrace privacy will come out on top in the Internet of Things market. In their view it will not be that hard for consumers to switch between companies. By contrast, other discussants think that the companies who create the most value for users will win in the Internet of Things market. They maintain that people will use services that diminish their privacy as long as they get value out of them.

Furthermore, participants do not expect that it will be viable for big companies or startups to monetise privacy directly. At the very least, people may be prepared to pay for privacy indirectly, by

being willing to pay more for brands that market themselves on their privacy policy. Finally, some think that a trend of paying for privacy might result in an economic divide, in which there will be a class of people that is able to pay for privacy and a group of people that is not. Again others disagree and consider this a red herring argument against paying for privacy.

Given the legal differences between the US and the EU, could enhanced cooperation between US and EU regulators be a venue for a streamlined response to privacy issues in the Internet of Things? What is the right approach for a regulator?
Discussants agree that regulators could play a larger role, and that the Internet of Things is in fact a perfect field for further cooperation. One of the reasons given is that (Internet of Things) devices are often made outside the US, then white-labelled, and brought back into the country. For regulators it is necessary to obtain information from other countries in order to evaluate these imported products. In this context some participants wonder whether certifications could be of any help. However, it is concluded that certifications are not helpful to regulatory oversight because regulators have to be able to look underneath those certificates, to know how the product was actually made.

Which technical solutions are you aware of that seem to be promising? How can the development and uptake of such solutions be stimulated?
Various technical and business solutions for privacy in the Internet of Things are discussed. Certifications are mentioned again, but rejected by others because obtaining them is very costly and time-intensive for startups. It is suggested that consumers should get security update reminders, or that security updates should be forced upon the devices. Participants remark that a lot of Internet of Things technologies will not be supported for long enough. In response, participants remark that the key element of the Internet of Things is connectivity to the internet. There should always be a possibility to update devices, and consumer protection could ensure that companies are required to provide support for Internet of Things applications for their expected lifetime. It is added that there should be mechanisms to make companies internalise the costs of supporting their products. Furthermore, technical solutions could include notice and consent mechanisms at platform level, consent via a peering system in which one device asks permission for other devices, and incremental permission requests so that devices only ask for permission when the user wants to use a certain feature. Finally it is noted again that too many notices will not help the user.

Final comments

In the final round, some new considerations are raised and previous points returned to. Participants share dystopian views of where Internet of Things developments are going, but at the same time they are optimistic about the sophistication of the discussions. It is reiterated that privacy and security should be addressed upfront, and not as an afterthought. Some discussants are of the opinion that companies have a responsibility to build better privacy protections for users. At the same time, some discussants acknowledge that users are very unaware and to a large extent not interested in privacy. Others disagree on that point and argue that many users actually do make use of privacy controls. Participants hope that new and emerging technologies will be of help in this area. The timing factor is mentioned, in the sense that we should discuss the point at which we want certain developments to take off. Next, participants do not expect that adequate privacy protection is anything we can ever solve. Rather, they think it will be a continuous negotiation. Individual consent is critiqued again and it is suggested that maybe some Internet of Things

products should just not be allowed on the market (instead of giving the consumer the option to choose yes or no).

Some comment on the privacy discussion per se and argue that we should put more emphasis on improving society, in the sense that we should create a society in which people do not have to be concerned about their own privacy any longer.

Finally, participants agree that this is a very timely discussion and a pivotal time for the Internet of Things. They remark that a characteristic of the Internet of Things is that the technologies move into the background. With that we may conclude that it is ever more important to move the debate into the foreground, and to engage all stakeholders with these questions.

Who was Rathenau?
The Rathenau Instituut is named after Professor G.W. Rathenau (1911-1989), who was successively professor of experimental physics at the University of Amsterdam, director of the Philips Physics Laboratory in Eindhoven, and a member of the Scientific Advisory Council on Government Policy. He achieved national fame as chairman of the commission formed in 1978 to investigate the societal implications of micro-electronics. One of the commission's recommendations was that there should be ongoing and systematic monitoring of the societal significance of all technological advances. Rathenau's activities led to the foundation of the Netherlands Organization for Technology Assessment (NOTA) in 1986. In 1994 this organization was renamed 'the Rathenau Instituut'.

The Rathenau Instituut promotes the formation of political and public opinion on science and technology. To this end, the institute studies the organization and development of science systems, publishes about social impact of new technologies, and organizes debates on issues and dilemmas in science and technology.

Anna van Saksenlaan 51
2593 HW Den Haag
Postbus 95366
2509 CJ Den Haag
070 342 1542
info@rathenau.nl
www.rathenau.nl