PROFILING THE EUROPEAN CONSUMER IN THE INTERNET OF THINGS

HOW WILL THE GENERAL DATA PROTECTION REGULATION APPLY TO THIS FORM OF PERSONAL DATA PROCESSING, AND HOW SHOULD IT?

Sarah Johanna Eskens

29 February 2016

Sarah Johanna Eskens

s.j.eskens@uva.nl

Thesis Research Master Information Law

Supervisor: Frederik Zuiderveen Borgesius

Second reader: Lucie Guibault

Grade: 8,5 out of 10

University of Amsterdam (UvA) / Instituut voor Informatierecht (IViR)

TABLE OF CONTENTS

1. INTRODUCTION

1.1. BACKGROUND

Ever more objects that connect to the Internet surround us. This development is part of the trend towards the "Internet of Things": the 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, coffee machines, toys, cars, streetlights, and factory machines will connect to the Internet as well.

Just because the Internet of Things-*things* are connected to the Internet, private companies can easily collect and combine the data that are generated by these devices to build detailed profiles of the owners of the devices ("profiling").[1] Data that stem from Internet of Things devices are high in quantity, quality and sensitivity. Therefore, the profiles that can be constructed from data generated by Internet of Things devices are much more detailed and sensitive, and identification of individuals through profiles becomes more likely than not.[2]

The Internet of Things changes in particular data quality, in the sense that the Internet of Things increases the range of dimensions covered by captured data, and the possibilities to merge these data. In the Internet of Things potentially all spheres of private or professional activities produce data, as opposed to the current situation in which data generation is generally restricted to the active use of information and communication technologies.[3] Seemingly meaningless data generated by the sensors of Internet of Things devices ("sensor data") can be combined and analysed, resulting in meaningful user profiles. With the use of sensor fusion techniques and big data or machine learning analysis, in the Internet of Things "everything may reveal everything."[4]

---

1 See in general the various contributions to Hildebrandt and Gutwirth (eds.) 2008, and Gutwirth, Poullet and De Hert (eds.) 2009.

2 Mauritius Declaration, p. 1; also see Weber 2015, p. 623.

3 Čas 2011, p. 142-144.

4 Peppet 2014, p. 120-121; also see Weber 2015, p. 623; Mäkinen 2015, p. 269.

Profiling is not per se "bad," but there might be negative effects for consumers when profiles are applied to them.[5] Already in 1993 Gandy showed how "database marketing," essentially an early form of today's profiling, produces discriminatory practices in which companies target some consumers for further advertising and dismiss consumers who are of less value.[6] Furthermore, in 1999 researchers described a practice called "market manipulation" in which case companies make use of the cognitive limitations of consumers to sell products and services. Calo updates the theory of market manipulation to the age of the Internet of Things. He describes how developments such as the Internet of Things increasingly empower companies to exploit how consumers tend to deviate from rational decision-making, and thus to manipulate consumers into purchasing things.[7]

Next to the risks of discrimination and manipulation, profiling generates knowledge about a person's lifestyle, habits and preferences, which raises more general concerns about the loss of personal privacy.[8] This introduction has shown that the concerns about profiling are not entirely new, but that the Internet of Things in particular increases the risks of profiling.[9]

1.2. PROBLEM STATEMENT

To the extent that profiling is based on personal data, in the European Union ("EU") the legal framework for the protection of individuals with regard to the processing of personal data regulates the activity of profiling. This legal framework is currently laid down in the Data Protection Directive ("DPD" or "the Directive").

---

5 Vermeulen summarizes the responses of the industry to the suggestion of the European Commission to regulate profiling: "Many industry stakeholders stress that profiling as such is not a negative practice. Profiling improves or customizes services for consumers (including shopping suggestions, filter search results, and direct marketing advertisements) or prevents fraud. It has been 'fundamental to the success of the Internet and of many new business models;'" see Vermeulen 2013, p. 12; also see Hildebrandt 2008, p. 305.

6 Gandy 1993, as referred to in Lyon (ed.) 2003, p. 1. In a more recent article Gandy in particular addresses the process of automated discrimination in Ambient Intelligence systems (a predecessor to the Internet of Things); see Gandy 2010; also see Peppet 2014, p. 117-118; Korff 2012, p. 22-23.

7 Calo 2014, p. 1003-1018.

8 See for example Sykes 1999; Hildebrandt and De Vries (eds.) 2013.

9 Van den Berg 2016, p. 11.

Similarly, to the extent that data generated by Internet of Things devices are personal data, in the European Union the Data Protection Directive regulates the processing of these personal data.

Both for profiling as well as for personal data processing in the Internet of Things there are uncertainties about the application of the EU data protection framework. Do Internet of Things devices generate "personal data" within the meaning of the Data Protection Directive? Is the Directive applicable to non-EU Internet of Things companies that engage in profiling of European consumers? What do the rules as contained in the Directive, rules that are framed in rather general terms, mean in practice for profiling in the Internet of Things?

These uncertainties were at issue in the Article 29 Working Party opinion on the Internet of Things.[10] The Article 29 Working Party is an independent European advisory body on data protection and privacy.[11] One of the tasks of the Article 29 Working Party is to examine questions about the application of national data protection law adopted under the Data Protection Directive in order to contribute to the uniform application of the EU data protection rules.[12] In its opinion on the Internet of Things the Working Party identified profiling as one of the main six data protection risks that lie within the ecosystem of the Internet of Things.[13] The Working Party then provided guidance on how the EU legal framework should be applied to such data processing activities in the Internet of Things.[14]

However, the relevance of the Article 29 Working Party opinion on the Internet of Things is limited in two ways. First, even though the opinion was issued in 2014, it focuses entirely on the current Data Protection Directive. By the time the Internet of Things will have fully arrived, in the European Union the main legal framework for the protection of individuals with regard to the processing of personal data will be the General Data Protection Regulation ("GDPR" or "the Regulation").[15] This legal

10 Article 29 Working Party 8/2014.
11 Article 29(1) DPD.
12 Article 30(1)(a) DPD.
13 Article 29 Working Party 8/2014, p. 8.
14 Article 29 Working Party 8/2014, p. 3.
15 European Commission 2012a. Note however that the relevant legal framework for data processing in the Internet of Things consists of the DPD/GDPR as well as of Directive 2002/58/EC as

instrument is set to replace the Directive that was adopted in 1995. The General Data Protection Regulation will come into effect two years after its formal adoption, which is expected for beginning 2016,[16] and it will change the EU data protection framework considerably.

Second, the Article 29 Working Party opinion relied on the assumption that "users must remain in complete control of their personal data throughout the product lifecycle," and this assumption about the object of data protection guided the opinion's answer as to how the Data Protection Directive should apply.[17] Some writers have asked whether if individual control over personal data is actually feasible in the Internet of Things.[18] This raises the question how the new legal framework consisting of the Regulation should be applied to profiling in the Internet of Things.

This research continues on the Article 29 Working Party opinion, by focusing on profiling in the Internet of Things, and posing a question that in its essence is of a similar character to the question that the opinion answered:

> How will the General Data Protection Regulation apply to profiling based on data collected in the Internet of Things, and *how should the Regulation apply in this context*, based on an assessment what should be the object of data protection law?

With this, the research aims to contribute to the discussion about profiling and the Internet of Things. In analogy with the Article 29 Working Party opinion on the Internet of Things, this research seeks to explain how the new EU data protection framework will apply to profiling in the Internet of Things. At the same time, this research also purports to present an alternative data protection approach to profiling in the Internet of Things, instead of the Article 29 Working Party approach that concentrates on individual control. Officials of the European Commission expect action from the

---

amended by Directive 2009/136/EC. In particular relevant are the provisions contained therein on the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user ("cookies;" see Art. 5(3) Directive 2002/58/EC). Internet of Things devices qualify as "equipment" within the meaning of these rules.

16 European Commission 2015b.

17 Article 29 Working Party 8/2014, p. 3.

18 See for example Arnold, Hillebrand and Waldburger 2015, p. 64-69; Čas 2005; Thierer 2014; see more in section 3.3.

Commission on the best approach forward for the Internet of Things by mid 2016.[19] The results of this research could feed into the discussion about what is this best approach forward.

1.3. RESEARCH APPROACH

1.3.1. RESEARCH METHODS

The research question can be divided into two parts that require different research methods.[20] To begin with, the research describes the legal framework, by analysing *how the General Data Protection Regulation will apply to profiling based on data collected in the Internet of Things*. After that, the research sets a normative framework, by assessing *what should be the object of data protection law in the Internet of Things*. Within that framework, the research argues *how the Regulation should be applied to profiling based on personal data collected in the Internet of Things*. Essentially, the first part is descriptive and the second part is normative. The following section explains the methods that are necessary to develop these descriptive and normative parts.

Research methods for the descriptive part

To describe the legal framework the research applies classical doctrinal legal methods. Doctrinal legal methods are applied to identify, analyse and synthesise the content of the law.[21]

In this research project the main source to identify the content of EU data protection law is the upcoming General Data Protection Regulation. On 15 December 2015 representatives of the three legislative bodies of the European Union (the European Parliament, the Council of the European Union, and the European Commission) reached agreement on the content of the new data protection rules (the "compromise text").[22] This text is still an informal agreement and now has to be formally adopted by the full

---

19 EurActiv.com reported that a Commission official said he expected a decision from the Commission, probably a Communication, on the best approach forward for the Internet of Things by mid 2016; see EurActiv 2015.

20 In this research, "method" concerns the way in which the research project is pursued, that is, *what the researcher actually does* to answer the research question; see Watkins and Burton 2013, p. 2.

21 Hutchinson 2013, p. 9.

22 European Commission 2015b. The final compromise text was unofficially released by Statewatch in the days thereafter. On 28 January 2016 the Council of the European Union published the official compromise text of the draft GDPR via its institutional website; see Council of the European Union 2016.

European Parliament and Council of the European Union.[23] Nevertheless, this research refers to the compromise text since it is the latest and most definite version of the Regulation.

To interpret the rules of the General Data Protection Regulation, this research refers to the preamble to the Regulation, case law that concerns the previous Data Protection Directive, opinions of the Article 29 Working Party, previous versions of the proposed Regulation, and a Council of Europe Recommendation. The preamble to the Regulation contains over hundred recitals. In general, the recitals of an EU act set out the reasons for enacting the operative provisions.[24] The recitals use "non-mandatory language,"[25] and the Court of Justice of the European Union in Luxembourg ("CJEU" or "the Court") has determined that the recitals in the preamble to an EU act have no binding legal force.[26] In practice, European courts do interpret ambiguous provisions of EU legislation in light of the recitals.[27] This means that the recitals can be used to interpret the operative provisions of the proposed Regulation.

The Court of Justice of the European Union is the principal body to interpret the Data Protection Directive and will be the principal body to interpret the upcoming General Data Protection Regulation.[28] The Court has ruled in several instances on the interpretation of key concepts and rules in the Directive. For example, in the case of *Google Spain v. Costeja González* the Court was asked to interpret a provision in the Directive that permits the processing of personal data where it is necessary for the purposes of the "legitimate interests" pursued by the controller or by a third party.[29] In so far as the key concepts and rules in the proposed Regulation are similar to the ones in the Directive, the case law of the Court that concerns the Directive can be used to interpret the concepts and rules in the Regulation.

---

23 European Commission 2015b. Once the Regulation receives formal adoption (expectedly beginning 2016), the official texts will be published in the Official Journal of the European Union in all official languages. The new rules will become applicable two years thereafter.

24 European Parliament, the Council and the Commission 2013, para. 10.

25 European Parliament, the Council and the Commission 2013, para. 10.1.

26 CJEU 19 November 1998, C-162/97 (*Nilsson, Hagelgren and Arrborn*), para. 54.

27 Klimas and Vaičiukaitė 2008, p. 92.

28 Article 263 TFEU. Also see Recital 113 GDPR.

29 CJEU 13 May 2014, C-131/12 (*Google Spain v. Costeja González*); see Article 7(f) DPD.

In principle, the opinions of the Article 29 Working Party are not binding in the EU legal order,[30] though the opinions are considered authoritative in the field of EU data protection law. Section 1.2 of this introductory chapter introduced the Article 29 Working Party as the independent European advisory body on data protection and privacy.[31] One of the tasks of the Working Party is to examine questions about the application of national data protection law adopted under the Data Protection Directive.[32] The Working Party opinions have played a significant role in rule development of European data protection law, since many European institutions rely on the opinions' line of argumentation.[33] In a similar vein to which this research uses case law of the Court of Justice of the European Union, this research can use the Working Party opinions to interpret concepts and rules in the proposed General Data Protection Regulation that resemble concepts and rules in the Directive.

This research compares the final "compromise text" of the General Data Protection Regulation with previous versions of the proposed Regulation. The Regulation is the outcome of a lengthy political process that resulted in three preliminary versions for a new data protection framework, before the final compromise text was concluded. First, on 25 January 2012 the European Commission officially made public its Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).[34] Second, on 12 March 2014 the European Parliament voted on a heavily amended version of the Regulation as proposed by the Commission.[35] This version was contained in a report by the rapporteur for the European Parliament.[36] Third, on 15 June 2015 the Council of the European Union agreed on a General Approach on the proposal for a Regulation.[37] This General

30 Kuner and Burton 2014.
31 Article 29(1) DPD.
32 Article 30(1)(a) DPD.
33 Eberlein and Newman 2008, p. 41.
34 European Commission 2012b.
35 European Parliament 2014.
36 The rapporteur was Jan-Phillip Albrecht. On 22 October 2013 he already unofficially published the amended version of the Regulation on which the Parliament voted via his own website; see Albrecht 2013.
37 European Commission 2015a.

Approach also contained amendments on the version of the Regulation as proposed by the Commission.[38]

In some instances, the differences between the versions might contain clues to the interpretation of the final compromise text of the General Data Protection Regulation. For example, the European Commission's 2012 Proposal for a Regulation in one provision used the term "natural persons" instead of the more common data protection parlance of "data subjects." The use of "natural persons" suggested that the concerned provision did not just apply to identifiable persons but also to unidentifiable persons (which would be a novelty in data protection law). However, the final compromise text for the Regulation in the end opted for the common term of "data subjects," which may mean that in the end the provision only concerns identifiable persons.

Finally, this research also compares one particular provision of the General Data Protection Regulation on profiling with a particular provision in the Council of Europe ("CoE") Recommendation on the protection of individuals with regard to automatic processing of personal data in the context of profiling.[39] Recommendations of the Council of Europe are not binding,[40] yet work of the Council of Europe has been of great influence on data protection policy in the European Union.[41] In this research, the provision in the CoE Recommendation shows how the concerned provision in the Regulation also *could* have been formulated, and thus a contrario can *not* be interpreted.

Throughout the research the Nest thermostat is used to illustrate various points, because this thermostat comes with a relatively elaborate privacy statement, and because the thermostat is typical for smart homes. Analysts predict that smart homes will be the largest consumer sector for Internet of Things applications.[42] These predictions signify the importance of research into data protection in the smart home environment.

38 The Council of the European Union unofficially made public the General Approach via its institutional website; see Council of the European Union 2015.
39 Council of Europe 2010.
40 Council of Europe 2015.
41 Bennett and Raab 2006, p. 84-87.
42 Harvard Business Review 2014; Business Insider 2015; GSMA 2014.

Research method for the normative part

To make a normative argument about how the General Data Protection Regulation should be applied to profiling based on personal data collected in the Internet of Things, this research constructs the object of data protection law along three lines.

First, the research tracks how the concept of data protection in the EU legal order has historically developed since the Data Protection Directive was enacted in 1995, to the Charter of Fundamental Rights of the European Union ("the Charter") was proclaimed in 2000, and the General Data Protection Regulation was proposed in 2012. The previous sections already expounded on the relevance of the Directive and the Regulation for EU data protection law. In 2000 the European Parliament, the Council of the European Union and the European Commission proclaimed the Charter of Fundamental Rights of the European Union.[43] What sets the Charter apart from other human rights instruments is that it recognizes a separate fundamental right to data protection, next to the right to privacy.[44] The research hopes to find insights into the object of data protection law by comparing how the Directive, the Charter, and the Regulation frame the right to data protection.

Second, the research analyses what is the origin of the Article 29 Working Party assumption that "users must remain in complete control over their personal data throughout the product lifecycle,"[45] and sees if this assumption can be countered. To find a counterargument to this assumption, the research in particular looks into what is considered to be the source of all current data protection law: the 1973 report by the United States Department of Health, Education & Welfare titled *Records, Computers, and the Rights of Citizens* ("the HEW report").[46] If this report conceives of data protection in a way that deviates from the Article 29 Working Party assumption, this could mean that we can understand the object of data protection differently, while retaining the substance of data protection law.

Third, the research considers factual arguments about the feasibility of individual control over personal data in the Internet of Things. These arguments are based on the

43 Charter of Fundamental Rights of the European Union (*OJ* 2000, C 364/1). The Charter is legally binding since the entry into force of the Treaty of Lisbon in December 2009.
44 Article 8 Charter; see further in section 4.1.
45 Article 29 Working Party 8/2014, p. 3.
46 U.S. Department of Health, Education & Welfare 1973; Gellman 2015, p. 1.

technical description of the Internet of Things in chapter 2 of this research, as well as on empirical research into the more general limitations of individual control over personal data. In particular the work of Acquisti and his colleagues at Carnegie Mellon University's Heinz College critiques the assumption of perfect rationality in consumers' data protection decision making.[47]

The findings of these three parts are then combined to make an argument about how the General Data Protection Regulation *should* apply to profiling in the Internet of Things.

1.3.2. SCOPE OF THE RESEARCH

The scope of the research is confined to the processing of personal data by private companies in consumer settings. This delineation means that the research does not look into the Industrial Internet of Things. The Industrial Internet of Things refers to the use of Internet of Things technologies to optimize operations and make processes more efficient in industrial sectors, like manufacturing, energy, agriculture, and transportation. This research presumes that the data protection challenges with profiling in industrial sectors will be minimal, apart from questions related to the use of personal data of factory workers, for example to optimize their productivity. Nor is the research concerned with Internet of Things-based profiling by governments or employers. In these contexts questions of data protection would require more attention for the particular power relationship between government and citizens, and employers and employees.

As appears from the above, this research analyses the General Data Protection Regulation in light of the Internet of Things, yet the author of this research believes that the core of the argument as contained in the second sub question will hold for other the other two much discussed technologies of big data and cloud computing.[48]

1.4. CHAPTER STRUCTURE

The chapters are structured as follows. Chapter 2 shows how ideas for the Internet of Things developed over the last twenty-five years, and explains the technical aspects of

47 Acquisti and Grossklags 2005.

48 According to research by Deloitte, "[t]he Internet of Things is pulling up alongside cloud and big data as a rallying cry for looming, seismic IT shifts;" see Deloitte 2015, p. 35.

the Internet of Things with a view to data protection. Chapter 3 determines the legal framework as laid down by the General Data Protection Regulation. The chapter looks into the general provisions that define the scope of application of the Regulation, the provisions that contain the principles related to personal data processing, and the provisions that formulate specific rules for profiling. The chapter then analyses how these provisions apply to profiling in the Internet of Things. Chapter 4 sets out three competing visions on the object of data protection law, namely that data protection law should be about individual control over personal data, about risk regulation, or about fair processing, that is, general obligations for the data controller and the data processor. The chapter then argues that individual control over personal data is not feasible in the Internet of Things. With this argument, the research reacts against the position taken by the Article 29 Working Party that in the Internet of Things, users must remain in complete control of their personal data. The implication of the argument is that in the Internet of Things, the object of data protection law should be risk regulation and fair processing. The last section of chapter 4 thinks through what this conclusion means for the application of the Regulation to profiling in the Internet of Things: How should this new EU legal framework actually be applied in to profiling in the context of the Internet of Things? Chapter 6 summarizes the results and concludes that not the data subjects, but rather civil society should be "in control" over profiling in the Internet of Things. Armed with this conclusion, the research at last looks back to the initial research aim.

2. THE INTERNET OF THINGS

What we now call the "Internet of Things" is not so much one specific technology; rather the Internet of Things is a vision or a paradigm for (networked) computing.[49] The idea for an Internet of Things has developed over the last twenty-five years. This chapter introduces the Internet of Things by means of the early visions that have inspired its development and describes the technical characteristics of the Internet of Things with a view to data protection (section 2.1), and gives a future outlook for the Internet of Things (section 2.2).[50]

2.1. A DEVELOPMENT TOWARDS THE INTERNET OF THINGS

The origins of the idea for an Internet of Things can be traced back to the late 1980s when computer scientist Mark Weiser at Xerox Palo Alto Research Center (Xerox PARC) articulated his vision for "ubiquitous computing." Weiser described a new wave of computing in which computers would become part of the environment and available everywhere and anywhere, with almost every object containing a tiny computer.[51] Weiser's idea was born before the commercialization of the Internet, but the Internet was later integrated into concepts that resembled and/or built on ubiquitous computing (namely, pervasive computing and Ambient Intelligence).

The year 1999 was a defining year for the Internet of Things. Neil Gershenfeld from the Massachusetts Institute of Technology ("MIT") New Media department published a book in which he foresaw a future where "things start to use the Net so that people don't need to."[52] According to Gershenfeld, information technology was underdeveloped, because it was not yet able to anticipate people's needs.[53]

---

49 Van den Berg even calls the Internet of Things a "movement," because she feels it has taken on a life of its own, up to the point that almost all consumer technology now enters the market with an Internet connection, without critical reflection on the necessity and desirability; see Van den Berg 2016, p. 9.

50 For some good overview articles of the Internet of Things vision, technologies and general research challenges see Al-Fuqaha et al.2015; Atzori, Iera and Morabito 2010; Gubbi et al. 2013; Miorandi et al. 2012; Manwaring and Clarke 2015; Olson et al. 2015; Borgia 2014. For a less academic, but very readable overview see Evans 2011.

51 Weiser 1991.

52 Gershenfeld 1999, p. 213.

53 Gershenfeld 1999, p. 7-8.

At the same time, a group of manufacturers and standardization organizations set up the Auto-ID Center at the MIT in Cambridge, Massachusetts. Their goal was to research and develop so-called "Auto-ID technologies."[54] These are technologies used in the world of commerce that enable computers to automatically recognize and identify everyday objects,[55] such as barcodes and Radio Frequency ID ("RFID") systems. The Auto-ID Center had an important role in making the enabling technologies for the Internet of Things commercially attractive to the industry. And, in 1999 Kevin Ashton, one of the cofounders of the Auto-ID Center, incidentally coined the term "Internet of Things" in a business presentation.[56] In the years thereafter the Internet of Things was recognized by the International Telecommunication Union ("ITU")[57] and embraced by the European Commission with a dedicated action plan.[58]

All in all, what emerged over these years was the idea that billions and billions of every-day 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, and be enabled to sense, think, communicate, and act for us. A more formal description of the Internet of Things is given by the European Internet of Things Research Cluster ("IERC"): "A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual 'things' have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network."[59]

From a technical perspective the Internet of Things is built of "things" that are equipped with sensors and often also actuators, communication and network technology, a processing unit, a unique identifier, and usually a connection to the cloud.[60] Sensors give the thing context awareness and the ability to collect data about its user and its physical environment. Actuators enable the thing to actually perform actions in the

54 Sarma, Brock, and Ashton 2000, p. 4.
55 Meloan 2003.
56 Ashton 2009.
57 ITU 2005.
58 European Commission 2009.
59 Vermesan and Friess 2015, p. 25; also see International Telecommunication Union 2012. Another term heard in this context is "cyber-physical systems" ("CPS"), but this concept has more of an industrial connotation, and describes an engineering discipline. By contrast, the Internet of Things includes the consumer side, and research into the Internet of Things is mostly computer science driven.
60 The points in the following paragraphs are all taken from Al-Fuqaha et al. 2015.

physical world, for example by moving something or adjusting settings. In other words, a sensor can be used to *sense* the environment, and an actuator can be used to *manipulate* the environment. A processing unit (a chip) gives the thing the capability to do small computing on the data it has collected with its sensors and operate without human intervention. This makes the connected objects smart, in the sense that with their embedded sensors, actuators, and chips they can operate autonomously and interactively to a certain extent.

An Internet of Things device needs communication and network technology to connect to the Internet, eventually via a local network or a gateway device between the object and the Internet. Through these connections data are exchanged with other connected objects, dedicated servers or the cloud.

With unique identifier technology such as RFID or the newer technology of Near Field Communication ("NFC") the thing can be identified in the network and is not mixed up with other connected objects in the network. Technology researchers expect that in the longer term all machine-to-machine communication (which is the communication between objects in the Internet of Things) will use IP addresses as identifiers.[61]

Internet of Things systems often encompass a larger number of connected devices that together generate big data, which requires complex computations to extract meaningful information. The storage and computing resources for big data are commonly located in the cloud.

In conclusion, with the Internet of Things, devices that operate on the basis of the processing of personal data will pervade the everyday lives of consumers even more, after the smart phones, tablets and laptops they carry everywhere.

2.2. FUTURE OUTLOOK FOR THE INTERNET OF THINGS

Expectations for consumer uptake of the Internet of Things are high, even though the Internet of Things faces barriers to adoption such as issues with standardization and interoperability.[62] Market research firm Gartner predicts that by 2020 about 13,5 billion of smart consumer objects will be connected, against the current 3 billion in

61 Scherer and Heinickel 2014, p. 146.
62 GSMA 2015; Accenture 2014.

2015.[63] The Organisation for Economic Co-operation and Development ("OECD") estimates that in the year 2022, households across the OECD area may have around 14 billion connected devices in total, with around 50 per four-person family.[64]

If we focus on Internet of Things consumer applications for in the home, we already see all kinds of personal devices and household appliances that collect, use, and disseminate personal data. For instance, the Internet of Things thermostat Nest determines when a homeowner is at home, when she is away, and what time she usually wakes up. On the basis of this information the thermostat adjusts the setting to a preferred room temperature. Nest Labs, Inc. (the company behind the thermostat) may receive and process data from third parties and associate these data with a Nest account.[65] The thermostat stores all the data locally on the device or on servers until the user deletes it or for as long as she remains a user. The company may share personal data with third parties with consent of the user, or without permission for among others external storage or technical problem solving.[66]

63 Gartner 2015.
64 OECD 2013, p. 10.
65 Google, Inc. (the company group is now called "Alphabet") acquired Nest Labs, Inc. in 2014.
66 Nest Labs 2015a.

3. THE GENERAL DATA PROTECTION REGULATION

This chapter look at the provisions in the General Data Protection Regulation that determine its scope of application,[67] and the provisions that contain general principles relating to personal data processing.[68] For both parts, the research points out how the new provisions differ from the Data Protection Directive's provisions that were at issue in the Article 29 Working Party opinion on the Internet of Things, and then determines how the new provisions will apply to profiling in the Internet of Things (section 3.1). The Regulation also contains some dedicated provisions on profiling.[69] The rest of this chapter analyses these provisions and how they will apply to profiling in the Internet of Things (section 3.2).

3.1. SCOPE OF APPLICATION OF THE REGULATION

In short, the question whether profiling based on data collected in the Internet of Things will fall within the scope of application of the General Data Protection Regulation hinges on two questions: Is there a *processing* of *personal data*? And, are the controller and processor *established in the European Union*, or do they *offer services to or monitor* EU data subjects?

3.1.1. MATERIAL SCOPE OF APPLICATION

The starting point to determine whether data processing in the Internet of Things will fall within the scope of application of the General Data Protection Regulation is the activity of data processing:

> *Article 2*
>
> 1. This Regulation applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.
>
> (...)

67 Chapter I of the Regulation – general provisions.
68 Chapter II of the Regulation – principles.
69 Chapter III of the Regulation – rights of the data subject. Note that Chapter III is not solely concerned with profiling.

This provision should be read in conjunction with the following definitions:

> *Article 4*
>
> (1) 'personal data' means any information relating to an identified or identifiable natural person 'data subject'; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.
>
> (...)
>
> (3) 'processing' means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
>
> (...)
>
> (3aa) 'profiling' means any form of automated processing of personal data consisting of using those data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;
>
> (...)

"Profiling"

As appears from the above, under the General Data Protection Regulation profiling will by definition be a form of processing.[70]

Furthermore, the definition of profiling in the Regulation recognizes that profiling consists of both the *construction* of profiles ("processing ... consisting of using those data to evaluate certain personal aspects"), as well as the *application* of profiles ("to analyse or predict aspects concerning" a person).[71] This interpretation is confirmed by the preamble to the Regulation, which states that data subjects should be informed about the existence of profiling (that is, the construction of profiles), and the consequences of such profiling (that is, the consequences of applying such profiles).[72]

---

70 Kuner critiques the definition of profiling, because it "seem[s] to cover many routine data processing operations that may also benefit the individuals concerned, such as, for example, routine operations to evaluate the performance of employees," and also because "[m]uch of the terminology used in this article is unclear and likely to be difficult to implement in practice;" see Kuner 2012, p. 11.

71 Hildebrandt 2008, p. 17.

72 Recital 48 GDPR.

"Personal data"

The General Data Protection Regulation slightly widens the concept of personal data when compared to the definition in the Data Protection Directive.[73] In the Directive as well as in the Regulation the definition of personal data implies that the data must concern a person, and the data must facilitate the identification of that person.[74] New in the Regulation are the examples of identifiers such as a name, location data, online identifiers, or factors specific to the genetic identity of a person. The preamble to the Regulation states that to determine whether a person is identifiable, account should be taken of "all the means reasonably likely to be used, such as singling out, either by the controller or any other person."[75] In addition, the preamble specifies that individuals may be associated with online identifiers provided by their devices, such as IP addresses, cookies, or RFID tags.[76] With this specification the Regulation recognizes that processing – such as profiling – might affect an individual who will never be identified by her name.[77] The mentioning of RFID tags is particularly relevant for the Internet of Things.

Despite the clarifications in the preamble, the concept of personal data remains a bit ambiguous under the General Data Protection Regulation. The concept as defined in the Data Protection Directive was uncertain and Member States showed diversity to its interpretation.[78] For example, there was discussion about the question whether IP addresses count as personal data.[79] The preamble of the Regulation clearly aims to solve such uncertainties. However, the preamble indicates the identifiers *may* identify a person, which is not to say they do so necessarily.[80] Next to that, the preamble suggests

---

73 Article 2(a) DPD: "personal data' shall mean any information relating to an identified or identifiable natural person (' data subject'); an identifiable person is one who can be identified, directly or indirectly , in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."

74 Bygrave 2002, p. 42.

75 Recital 23 GDPR.

76 Recital 24 GDPR.

77 Costa and Poullet 2012, p. 255. Also see Article 29 Working Party 4/2007.

78 Article 29 Working Party 4/2007, p. 3.

79 This question is now before the CJEU in the pending case of *Patrick Breyer v. Bundesrepublik Deutschland*. In this case the German Supreme Court made a preliminary reference to the CJEU, in which it asks whether "personal data" should be be interpreted as meaning that an IP address which a service provider stores when his website is accessed already constitutes personal data for the service provider if a third party (an access provider) has the additional knowledge required in order to identify the data subject.

80 Burton et al. 2016, p. 3.

that "singling out" means identification off a person, but the preamble does not say singling out always leads to identification.[81] Section 1.3.1 on research methods also indicated that the preamble to an EU act does not have binding legal force,[82] even though in practice European courts interpret ambiguous provisions of EU legislation in light of the preamble.[83] Given these reservations, the question whether data generated in the Internet of Things constitute personal data within the meaning of the Regulation can be debated – at least theoretically.[84]

In practice the particular characteristics of the Internet of Things will often necessitate the conclusion that personal data are being processed. This research distinguishes three situations. First, Internet of Things devices will collect and upload data that unquestionably relate to a person who can be identified, such as contact information that a user enters during set up and that is necessary for an online account or troubleshooting.

Second, the Internet of Things will involve data about objects that nonetheless can be considered personal data within the meaning of the General Data Protection Regulation. In its opinion on the concept of personal data the Article 29 Working Party analysed the four elements of the concept (any information / relating to / an identified or identifiable / natural person), and concluded that data about objects indirectly may relate to individuals when its purpose is to treat an individual in a certain way, or because the data result in the person being treated differently.[85] Given that the purpose of almost all Internet of Things services is to anticipate the needs of the user and act on that, much of the data that concerns Internet of Things devices or their environment will in fact relate to individuals who can be identified in the sense of the Article 29 Working Party opinion. For example, with several sensors the Nest thermostat collects data such as current temperature, humidity, ambient light, and whether something in the room is moving. From these data the smart thermostat will infer you have just woken up, returned home,

81 Zuiderveen Borgesius 2016, p. 12.
82 CJEU 19 November 1998, C-162/97 (*Nilsson, Hagelgren and Arrborn*), para. 54.
83 Klimas and Vaičiukaitė 2008, p. 92.
84 Schwartz for example concludes that also under the GDPR it will be difficult to decide prior to certain kinds of cloud data processing whether or not personal data will be implicated; see Schwartz 2013, p. 1646.
85 Article 29 Working Party 4/2007, p. 9-10.

or entered the room, and accordingly the thermostat will adjust the setting to a preferred temperature.[86]

Third, the Internet of Things will also concern data that relate to objects and are purely meant for functionality of the device itself. The Nest thermostat for instance registers whether it is connected to a heating and cooling system or a heating-only system.[87] Still, these data may later lead to the result that someone is treated differently, for example when she is sent offers for a heating system upgrade. What is at stake is not the data itself but the possibility to contact the owner of the Nest thermostat in order to have an impact on her rights or interest.[88]

The Article 29 Working Party also concluded that someone might be indirectly *identifiable* when a unique combination of identifiers can be used to single her out – a criterion that is now officially recognized in the preamble to the General Data Protection Regulation (see above).[89] Since all connected devices have a unique identification number and are of course connected to the Internet, data relating to these objects may be used to identify someone within the meaning of the Regulation. This opportunity to identification will especially be apparent when the data are combined with other bits of data, and the possibility of identification is relevant even when a person's name is not known (see above). For Internet of Things objects the combining of data resembles device fingerprinting, a technique that can be used to track the behaviour of the device owner over time.[90]

In October 2014 an international group of data protection and privacy commissioners presented the Mauritius Declaration on the Internet of Things, in which they simply assumed that Internet of Things' sensor data "should be regarded and treated as personal data."[91] The Mauritius Declaration did not include an analysis like the

86 Nest Labs 2016a.
87 Nest Labs 2015a.
88 Poullet 2009, p. 14-15.
89 Article 29 Working Party 4/2007, p. 12-14.
90 Article 29 Working Party 9/2014, p. 5-6.
91 Mauritius Declaration 2014.

foregoing. At first sight the Mauritius Declaration contained indeed a rather "simplistic assumption,"[92] yet as shown the assumption can be substantiated.

"Anonymous information"

The preamble to the General Data Protection Regulation states the principles of data protection should not apply to anonymous information.[93] The preamble defines "anonymous information" as "information which does not relate to an identified or identifiable natural person or data rendered anonymous in such a way that the data subject is not or no longer identifiable."[94] This means that when the data generated by Internet of Things devices are collected anonymously or directly anonymized, either on the device or in the cloud, the Regulation will not be applicable to profiling based on these data.

However, the Article 29 Working Party identified the risk of re-identification of personal data as one of the main six data protection challenges for the Internet of Things.[95] It is outside of the scope of this research to go into the discussion about reliable anonymisation techniques in an Internet of Things context.[96] Therefore, this paper proceeds on the assumption that *all* data generated in the Internet of Things are in fact personal data.

3.1.2. TERRITORIAL SCOPE OF APPLICATION

When the processing of personal data generated by the Internet of Things has been established, the question arises whether profiling based on these data will fall within the territorial scope of application of the General Data Protection Regulation:

> *Article 3*
>
> 1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

---

92 Out-law.com 2014.

93 Recital 23 GDPR.

94 *Ibid.*

95 Article 29 Working Party 4/2014, p. 8. also see Weber 2015, p. 623; Čas 2011, p. 145-146; Peppet 2014.

96 For example, Ohm warns that reidentification or deanonymization of personal data is often very easy for computer scientists; see Ohm 2010. Peppet cites preliminary research that suggests that in particular Internet of Things data are easy to reidentifiy; see Peppet 2014, p. 129-131.

2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behaviour as far as their behaviour takes place within the European Union.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where the national law of a Member State applies by virtue of public international law.

In connection to these provisions it is thus necessary to know that:

Article 4

(...)

(5) 'controller' means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data (...).

(6) 'processor' means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

(...)

"Controllers" and "processors"

The definitions of "controller" and "processor" are exactly alike in the General Data Protection Regulation and the Data Protection Directive. For example, Nest Labs, Inc. will be the controller within the meaning of the Regulation, because they determine the purpose of the profiling within their smart thermostat system, and they determine that profiling is used as a means of personal data processing. The service providers that Nest Labs, Inc. uses for external processing and storage of personal data collected by the thermostat will be processors within the meaning of the Regulation.[97]

Aside from this straightforward example, for this research it is not necessary to analyse in depth who is the controller and who is the processor in an Internet of Things system.[98] Under the Regulation an establishment in the EU of both a controller and a

97 Nest Labs 2015a.

98 According to the Article 29 Working Party, the first and foremost role of the concepts of controller and processor is to determine who shall be responsible for compliance with the data protection rules, and how data subjects can exercise their rights in practice; see Article 29 Working Party 1/2010.

processor will trigger the application of EU data protection law, just like profiling by both a non-EU based controller or processor will.[99]

Application of the Regulation within the EU

Article 3, paragraph 1, of the General Data Protection Regulation on EU controllers and EU processors resembles the corresponding provision in the Data Protection Directive.[100] Both provisions require there is an establishment, and that processing takes place in the context of the activities of that establishment. Like in the Directive, the preamble to the Regulation makes clear that the term "establishment" implies the effective and real exercise of activity through stable arrangements, for which the legal form is not a determining factor.[101] In the case of *Weltimmo* the Court of Justice of the European Union held that the presence of only one representative of a company can suffice to constitute a "stable arrangement," if that representative acts with a sufficient degree of stability for provision of the specific services of the company.[102] Next to that, in *Google Spain v. Costeja González* the Court found that processing of personal data is carried out "in the context of the activities" of an establishment when the activities of the company are inextricably linked to the activities of its establishment.[103]

Notwithstanding the overall similarity of the provisions on EU organizations, the General Data Protection Regulation does contain two minor novelties when compared to the Data Protection Directive. Under the Regulation, the establishment of a processor in the European Union will also trigger the application of EU data protection law, which creates a basis within the Regulation for independent obligations for processors.[104] Next to that, the provision in the Regulation explicates that the rules will apply irrespective of where the data are processed.

---

99 By contrast, for the Article 29 Working Party opinion on the Internet of Things, it was important to determine the role of the different stakeholders in the Internet of Things. Article 4 of the Data Protection Directive makes the applicability of national data protection law depended on the question who is the controller and who is the processor; see Article 29 Working Party 8/2014, p. 10.

100 Article 4(1)(a) DPD: [National law adopted pursuant to this Directive shall apply where] "the processing is carrier out in the context of the activities off an establishment of the controller on the territory of the Member State (...)."

101 Recital 19 GDPR; Recital 19 DPD.

102 CJEU 1 October 2015, C-230/14 (*Weltimmo*), para. 30.

103 CJEU 13 May 2014, C-131/12 (*Google Spain v. Costeja González*), para. 56,

104 For example, the GDPR imposes general obligations on the processor (Art. 26). Next to that, the Regulation obliges the controller and the processor to maintain records of processing activities (Art. 28), and the to take security measures (Art. 30). Also see Cuijpers, Purtova and Kosta 2014, p. 2.

Under Article 3, paragraph 1, of the General Data Protection Regulation the data protection rules will apply to profiling based on data collected in the Internet of Things when either the controller or the processor has an establishment in the European Union. For example, Nest Labs, Inc. is headquarted in Palo Alto, California, the United States, yet has an office in London with its own General Manager of Europe.[105] The company offers goods in the EU, such as the Nest thermostat that will learn within a few days at what room temperature "you like eating breakfast."[106] The Regulation will thus apply to data-processing activities by Nest Labs, Inc. regarding data subjects who are in the EU, even if the European office only represents its parent company when bringing the thermostat to the European market. [107] Another example is, Tado GmbH, who makes the tado° smart thermostat and is based in München.[108] This company will be subject to the Regulation as a controller, regardless of whether the company outsources the actual data processing to non-EU based data analytics companies.

Extra-territorial application of the Regulation

On the basis of Article 3, paragraph 2, of the General Data Protection Regulation EU data protection law will regulate non-EU controllers and non-EU processors. That is, the Regulation will have extra-territorial scope of application, like the Data Protection Directive has as well. However, the test in the Regulation to determine its extra-territorial effect is different from the test in the Directive. The latter stated that non-EU controllers were subjected to EU data protection law if they made use of equipment situated on EU territory.[109] In the Regulation, extra-territorial application of EU data protection law is linked to offering things or monitoring people.

The preamble to the General Data Protection Regulation states that "order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller

105 Nest Labs 2015b.

106 Nest Labs 2016a.

107 Note that in this example there is an overlap. Nest Labs, Inc. will also be subject to the extra-territorial effect of the General Data Protection Regulation in so far as the company profiles data subjects in the EU.

108 Tado GmbH 2016.

109 Article 4(1)(c) DPD: [National law adopted pursuant to this Directive shall apply where] "the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise , situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community."

is envisaging the offering of services to data subjects in one or more Member States in the Union."[110] In addition, the preamble gives a couple of factors to determine whether a controller has the intention to offer services to data subjects in the Union, such as the use of a language or a currency, with the possibility of ordering services in that language.[111] Under the renewed provision more non-EU companies that offer services over the Internet will be subjected to the EU data protection rules.[112]

The preamble to the Regulation further clarifies that "monitoring" refers to the tracking of individuals on the Internet, "including potential subsequent use of data processing techniques which consist of profiling an individual, particularly in order to take decisions concerning her of him or for analysing or predicting her or his personal preferences, behaviours and attitudes."[113]

There is uncertainty whether if monitoring by non-EU parties will concern just individual profiling, or group profiling as well. The version of the General Data Protection Regulation that the European Parliament voted on in 2014 deleted "an individual" after "profiling" in the preamble.[114] This deletion might suggest that the European Parliament intended to leave open the possibility of applicability of the Regulation in the case of group profiles.[115] Now that the final compromise text in the end still does mention "an individual" this could mean that monitoring does not include group profiling.

The development of one of the provisions that specifically address profiling also indicates that the General Data Protection Regulation will not regulate group profiling, neither by EU or non-EU organizations. The European Commission's 2012 Proposal for a Regulation provided that natural persons would have the right not to be subject to purely profiling-based measures.[116] The use of the term "natural persons" instead of the regular term "data subjects" suggested that the right applied not only to identifiable

110 Recital 20 GDPR.
111 Recital 20 GDPR.
112 Kuner 2012, p. 6.
113 Recital 21 GDPR.
114 European Parliament 2014.
115 Cuijpers, Purtova and Kosta 2014, p. 3.
116 Article 20(1) GDPR in European Commission 2012b.

persons but also to unidentifiable persons in groups.[117] However, the final compromise text for the Regulation prescribes that "data subjects" shall have the right not to be subject to purely profiling-based measures.[118] This could mean that monitoring does not include group profiling.

The extra-territorial effect of EU data protection law with regard to profiling in the Internet of Things will be the same under the General Data Protection Regulation and the Data Protection Directive. All connected objects that are used to collect and further process personal data qualified as equipment in the meaning of the Directive.[119] Since an Internet of Things company with users in the EU can hardly avoid having equipment in this sense, the Directive already had full extra-territorial effect with regards to profiling of EU residents in an Internet of Things context. The Regulation will reach full extra-territorial effect in this context as well, because under Article 3, paragraph 2, it applies to non-EU entities that monitor EU residents, which by definition includes profiling (see above).[120]

3.1.3. EXCEPTIONS TO THE SCOPE OF APPLICATION

To balance the wide scope of application of EU data protection law, the General Data Protection Regulation, like the Data Protection Directive, excludes certain data processing operations from its scope. These exceptions relate to the processing by national or European authorities, processing in the course of activities outside the scope of Union law, and processing by natural persons in the course of purely personal or household activities.[121] Since this research focuses on profiling in the Internet of Things in the private sector, the research continues on the assumption that none of the exceptions does apply.

---

117 Koops 2014, p. 257.

118 Article 20(1) GDPR.

119 Article 29 Working Party 8/2014, p. 10: "This qualification obviously applies to the devices themselves (...). It also applies to the users' terminal devices (e.g. smartphones or tablets) on which software or apps were previously installed to both monitor the user's environment through embedded sensors or network interfaces, and to then send the data collected by these devices to the various data controllers involved."

120 Imagine for example an US-based company that collects personal data of European coffee drinkers via smart coffee machines, with the intention to profile these people according to their coffee needs and work schedule. Under the current Directive, the company is subjected to EU data protection law via the coffee machine ("equipment"). Under the upcoming Regulation, the company will be subject to EU data protection law because the data collecting activities are related to profiling ("monitoring of behaviour").

121 Article 2(2) GDPR.

3.2. General principles of the Regulation governing personal data processing

The General Data Protection Regulation contains specific provisions on profiling, yet the preamble to the Regulation stipulates that profiling as such is also subject to the general principles of the Regulation governing processing of personal data.[122] Article 5 of the Regulation contains these principles.[123]

Lawfulness, fairness and transparency

The principles of lawfulness, fairness and transparency require that:

> *Article 5*
>
> 1. Personal data must be:
>
> (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency");
>
> (...)

The preamble clarifies that in order for processing to be lawful, personal data should be processed on a legitimate basis laid down by law, either in the Regulation (see below), or in other EU or national law as referred to in the Regulation.[124]

There is some overlap between the fairness and transparency principles.[125] The General Data Protection Regulation does not further specify what is "fair," but the Article 29 Working Party and other writers take "fair processing" to mean that data should only be collected with the knowledge of the individual,[126] and that data subjects are informed of their rights to data protection.[127] The preamble to the Regulation links to two by stating that "[a]ny processing of personal data should be lawful and fair. It should be transparent for the individuals that personal data concerning them are collected, used, consulted or otherwise processed and to which extent the data are

---

122 Recital 58a GDPR.

123 Compare Article 6 DPD. The second part of this section discusses how the principles apply to profiling in the Internet of Things, and in that discussion follows the same order (principles of lawfulness, fairness and transparency; purpose limitation; data minimisation; data quality; security safeguards; accountability).

124 Recital 31 GDPR.

125 In fact, the preamble and the substantive provisions of the Regulation consistently refer to "lawful and fair" (4 times) or "fair and transparent" (7 times) processing, and nowhere to "fair processing," so it could be questioned if the fairness principle has any independent meaning at all.

126 Article 29 Working Party 8/2014, p. 16; Bygrave 2002, p. 59; Costa and Poullet 2012, p. 256.

127 Article 29 Working Party 10/2004, p. 2.

processed or will be processed."[128] Furthermore, according to the preamble such information should be given at the time of collection, or where the data are not obtained from the data subject but from another source, within a reasonable period.[129]

The principle of transparency is elaborated in a set of information and access rights for the data subject, with specific information rights regarding profiling (see next section).[130]

For the profiling of consumers in the Internet of Things to be lawful within the meaning of the General Data Protection Regulation, one of the six legitimate bases as provided by Article 6, paragraph 1, of the Regulation will have to apply. The legal basis could be that the data subject has given consent to the profiling for one or more specific purposes (sub a), the profiling is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract (sub b), or the profiling is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data (...) (sub f).[131] That last "except where"-clause limits the legitimate interest ground.

---

128 Recital 30 GDPR.

129 Recital 49 GDPR. Also see Recitals 46-48 on the transparency principle.

130 Some of these rights are actually formulated as obligations for the controller. The General Data Protection Regulation *obliges the controller to provide* a minimum of information relating to the processing of personal data to the data subject, and the Regulation specifies the manner in which the information should be provided (Art. 12 in conjunction with Artt. 14 and 14a). Next to that, the Regulation gives the data subject *the right to obtain from the controller*: the confirmation as to whether or not personal data concerning him or her are being processed, and access to the data and certain information ("right of access"; Art. 15); the rectification of inaccurate personal data (Art. 16); the erasure of personal data concerning him or her ("right to be forgotten"; Art. 17); the restriction of the processing of personal data under certain conditions (Art. 17a); and, the personal data concerning him or her ("right to data portability"; Art. 18). The information and access rights in the Regulation are stronger than the information rights in the Data Protection Directive, which will cause companies to review and revise their privacy polices; see Kuner 2012, p. 10. This research only discusses the rights of information and access in so far they relate to profiling.

131 The preamble declares that the processing of data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security constitutes a legitimate interest of the data controller concerned (Recital 39). This should improve the level of information security in the EU; see Kuner 2012, p. 10. Furthermore, the preamble to the Regulation also provides that "Indicating possible criminal acts or threats to public security by the controller and transmitting the relevant data in individual cases or in several cases relating to the same criminal act or threats to public security to a competent authority should be regarded as being in the legitimate interest pursued by the

With regard to profiling in the Internet of Things, the legitimate interest ground is further limited by the Court of Justice of the European Union in *Google Spain v. Costeja González*. In that case the Court pointed out that the processing of personal data at issue (a search engine finding information on the Internet, indexing it, storing it, and making it available to Internet users) was liable to affect significantly the fundamental rights to privacy and the protection of personal data of individuals, because the processing enabled the establishment of a more or less detailed profile of the data subject, and because the Internet rendered the information "ubiquitous."[132] In the light of the potential seriousness of that interference, the Court found it clear that the processing by the search engine could not be justified by merely the economic interest which the operator of such an engine has in that processing.[133] The implication of this judgment could be that profiling in the Internet of Things cannot rely on the legitimate interest ground if this is solely for the economic interest of the responsible company.

The other three legal bases for lawful data processing in Article 6, paragraph 1, of the General Data Protection Regulation are not of interest for this research. Under no circumstances profiling of consumers will be necessary for compliance with a legal obligation to which the controller is subject (sub c),[134] or necessary in order to protect the vital interests of the data subject or of another natural person (sub d). Since this research is confined to profiling by private companies in consumer settings, profiling will neither be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (sub e).

Profiling based on data generated in the Internet of Things will be fair and transparent within the meaning of the General Data Protection Regulation if the data subjects are aware that data about them is collected, and if information about the profiling is given at the time of collection of the data. The Article 29 Working Party found that the fairness principle required that data controllers acting in the Internet of Things must inform all

---

controller" (Recital 40). This may imply that profiling consumers to find criminal acts would be legitimate under Article 6(1)(f) GDPR.

132 CJEU 13 May 2014, C-131/12 (*Google Spain v. Costeja González*), para. 80.

133 CJEU 13 May 2014, C-131/12 (*Google Spain v. Costeja González*), para. 81.

134 Unless one could devise a situation in which a private company is ordered to profile its customers in order to track down a suspect according to a suspect profile created by law enforcement.

individuals in the vicinity of connected devices when their personal data is collected.[135] Later on, this research problematizes this finding of the Working Party, and concludes differently as regards fair and transparent profiling in the Internet of Things.

Purpose limitation

The purpose limitation principle implies that personal data must be:

> (...)
>
> (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; further processing of personal data for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes shall, in accordance with Article 83(1), not be considered incompatible with the initial purposes; ("purpose limitation");
>
> (...)

Overall, the provisions on purpose limitation in the General Data Protection Regulation and the Data Protection Directive are alike.[136] A novelty in the Regulation is the list of factors that the controller should take into account to ascertain whether further processing for another purpose is compatible with the purpose for which the data are initially collected.[137]

Compliance with the principle of purpose limitation in the General Data Protection Regulation will require in particular that controllers specify the purposes for which they intend to profile the data subject prior to, or not later than, the time when the personal data are collected. To be clear, when operations of the data controller involve profiling of individuals, the profiling as such is not the "purpose" within the meaning of the EU data protection rules. The Data Protection Directive provides that personal data shall be "*collected* for specified, explicit and legitimate purposes." From this formulation the Article 29 Working Party inferred that the purposes should be specified *before* the data collection starts.[138] Therefore, Internet of Things companies should have a clear

---

135 Article 29 Working Party 8/2014, p. 15.

136 Article 6(b) DPD: [Personal data must be] "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards."

137 Article 6(3a) GDPR.

138 Article 29 Working Party 03/2013, p. 15.

business model before they start collecting personal data via Internet of Things devices.[139]

Data minimisation, data quality, and data security

The data minimisation principle entails that personal data must be:

> (...)
>
> (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimisation");
>
> (...)

There are two small changes in the data minimisation principle in the General Data Protection Regulation when compared to the Data Protection Directive. These changes make the new data minimisation principle a little bit stronger.[140] Under the Directive, personal data must be "not excessive" in relation to the purpose for which they are processed. Under the Regulation, personal data must be "limited to what is necessary" in relation to the purpose for which they are processed. Next to that, the preamble to the Regulation now states that personal data should only be processed if the purpose of the processing cannot be fulfilled by other means.[141] The preamble to the current Directive contains no such statement.

The data quality principles encompass accuracy and storage limitation norms, in the sense that personal data must be:[142]

> (...)
>
> (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ("accuracy");
>
> (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; (...) ("storage limitation");
>
> (...)

---

139 Mäkinen 2015, p. 273; Article 29 Working Party 8/2014, p. 16.

140 Article 1(c) DPD: [Personal data must be] "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed."

141 Recital 30 GDPR.

142 The GDPR does not use the term "data quality principles," except for in a provision on the transfer of personal data by way of binding corporate rules (Art. 43(2)(d)). However, the requirement of accuracy and storage limitation are generally understood as the principles of data quality; see for example European Union Agency for Fundamental Rights and Council of Europe 2014, p. 70-73.

Again, the preamble gives further clarification. It provides that every reasonable step should be taken to ensure that inaccurate personal data are rectified or deleted.[143] In connection with the accuracy norm, the data subject shall have the right to obtain from the controller the rectification of personal data concerning him or her which are inaccurate.[144]

The security safeguards principle demands that personal data must be:

> (...)
>
> (eb) processed in a way that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ("integrity and confidentiality");
>
> (...)

This provision is elaborated with data security obligations for the controller *and* the processor.[145] According to the preamble the security safeguards principle also requires "preventing unauthorised access to or the use of personal data and the *equipment* used for the processing" [emphasis added].[146]

The data minimisation, data quality, and security principles are strongly interconnected, and related to the principles of data protection by design and by default and the required data protection impact assessments.[147]

This research highlights two requirements for profiling in the Internet of Things that follow from the principles of data minimisation, data quality (that is, accuracy and storage limitation), and security safeguards in the General Data Protection Regulation. Under the new Regulation, the strengthened data minimisation principle implies that Internet of Things companies should only perform profiling if the purpose of the profiling cannot reasonably be fulfilled by other means. Next to that, under the new Regulation the security safeguards will also concern the equipment, that is, the Internet of Things devices. The inclusion of equipment in the security principle will also involve

143 Recital 30 GDPR.
144 Article 16 GDPR.
145 See Articles 30, 31, and 32 GDPR.
146 Recital 30 GDPR.
147 Respectively Article 23 and Recital 61 GDPR; Article 33 and Recital 71 GDPR; see Kosta and Cuijpers 2014, p. 21.

manufacturers of Internet of Things devices in the process to ensure compliance with the Regulation. They will have to ensure that data protection compliant Internet of Things technology is available for the companies that deploy the technology.[148]

Accountability

Finally, the accountability principle means that:

> *Article 5*
>
> (...)
>
> 2. The controller shall be responsible for and be able to demonstrate compliance with paragraph 1 ("accountability").

Later, the Regulation specifies the exact responsibility of the controller:

> *Article 22*
>
> 1. Taking into account the nature, scope, context and purposes of the processing as well as the risks of varying likelihood and severity for the rights and freedoms of individuals, the controller shall implement appropriate technical and organisational measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation. These measures shall be reviewed and updated where necessary.
>
> (...)

The controller needs to consider such "technical and organisational measures" as part of a data protection by design and by default approach:

> *Article 23*
>
> 1. (...) the controller shall, both *at the time of the determination of the means for processing* and *at the time of the processing itself*, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, which are designed to implement data protection principles, such as data minimisation (...);
>
> 2. The controller shall implement appropriate technical and organisational measures for ensuring that, *by default*, only personal data which are necessary for each specific purpose of the processing are processed (...). In particular, such measures shall ensure that *by default* personal data are not made accessible without the individual's intervention to an indefinite number of individuals.
>
> [emphasis added]

148 Article 29 Working Party 2005, p. 12.

The concept of accountability is new to EU data protection law.[149] It requires that controllers *adopt* measures, and are able to *demonstrate* that these measures ensure compliance.[150] The Regulation adds that accountability requires the implementation of data protection policies (before called "privacy policies"), and that adherence to approved codes of conduct or an approved certification mechanisms may be used as an element to demonstrate compliance with the obligations of the controller.[151] The preamble also points to guidelines of the European Data Protection Board (the new name for the Article 29 Working Party) to provide guidance for compliance.[152]

The new accountability principle in the General Data Protection Regulation in general will mean that the Internet of Things controllers will have to adopt technical and organisational measures to ensure that the profiling is consistent with the Regulation, and be able to demonstrate such compliance. Via the privacy by design and by default requirements in the Regulation, companies that produce the hardware and software for consumer Internet of Things devices will be increasingly involved ensuring compliance with data minimisation and purpose limitation.[153]

3.3. Specific rules in the Regulation concerning profiling

An important innovation of the General Data Protection Regulation is that it expressly addresses profiling. The previous section already indicated that the general principle of transparency in the Regulation is elaborated in a set of information and access rights for the data subject, with specific elements regarding profiling. Next to that, the right to object and the right not to be subjected to automated decision-making address profiling.

Rights of information and access regarding profiling

First of all, the right of information explicitly refers to profiling:

> *Article 14*

149 Burton ea 2016, p. 7. Even though the principle of accountability is not a new idea in the field of data protection. The OECD Privacy Guidelines from 1981 already contained an accountability principle, and Article 29 Working Party suggested this principle for European data protection law in 2010; see Article 29 Working Party 3/2010; De Hert and Papakonstantinou 2012, p. 134; Gumzej 2012, p. 94-95.

150 Cuijpers, Purtova and Kosta 2014, p. 9. According to Hustinx, this separate obligation "is designed to work as an incentive for controllers and a tool for data protection authorities to supervise data management practices, without necessarily having to go into time consuming analysis of substantive issues;" see Hustinx 2014, p. 47.

151 Articles 22(2a) and (2b) GDPR.

152 Recital 60c GDPR.

153 Kuner 2012, p. 13.

(...)

1a. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

(...)

(e) the existence of the right (...) to object to the processing of such personal data;

(...)

(h) the existence of automated decision making including profiling referred to in Article 20(1) and (3) and at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

(...)

A similar rule holds when personal data are not obtained from the data subject.[154] The preamble to the Regulation summarizes that "the data subject should be informed about the existence of profiling, and the consequences of such profiling," but does not clarify this right any further.[155] In practice, the data subject's right of information is thus an obligation to inform for the controller.

Similarly, the right of access for the data subject includes a provision on profiling:

Article 15

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and where such personal data are being processed, access to the data and the following information:

(...)

(e) the existence of the right (...) to object to the processing of such personal data;

(...)

(h) the existence of automated decision making including profiling referred to in Article 20(1) and (3) and at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

(...)

In anticipation on the right to object (see next paragraphs), it should be added that:

154 Article 14a(2)(h) GDPR.
155 Recital 48 GDPR.

Article 19

(...)

2b. At the latest at the time of the first communication with the data subject, the right [to object to processing, including profiling] referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

(...)

The preamble to the Regulation explains that in general the right of access aims to enable the individual "to be aware of and verify the lawfulness of the processing."[156] The preamble adds that right of access should not adversely affect the rights and freedoms of others, including trade secrets or intellectual property protecting the software.[157] However, according to the preamble the result of these considerations should not be that in the end all information is refused to the data subject.[158] The preamble to the Data Protection Directive contains the same general considerations.[159]

In the Internet of Things, the controller will thus have to provide the data subject information – at its own initiative and at the request of the data subject – about the existence of profiling, meaningful information about the logic involved in this profiling, as well as the significance and the expected consequences of such profiling for the data subject. In particular, the controller will have to inform the data subject *explicitly* about her right to object to the profiling, and the controller must present this information at the latest at the time of the first communication with the data subject, and clearly and separately from any other information.[160] The counterpart of these obligations to inform is the data subjects right's of access to information about the profiling.[161]

Traditionally, controllers that collect and process personal data via the Internet inform the consumer with an online privacy policy, but in the Internet of Things privacy policies are unpractical for several reasons. To begin with, in an Internet of Things era

156 Recital 51 GDPR.
157 *Ibid.*
158 *Ibid.* Malgieri concludes that although it "it might appear that European data protection law generically accepts a prevalence of trade secret rights on data protection rights," in fact there is a "preference toward data protection rights;" see Malgieri 2016.
159 Recital 41 DPD.
160 Article 19(2b) GDPR.
161 Article 15(1)(h) GDPR.

consumers will interact with a large number of connected devices that collect and process personal data.[162] As noted above, the OECD estimates that in 2022, household will have around 50 connected devices per family.[163] That means 50 privacy policies, which are also updated. For example, Nest Labs, Inc. updated the privacy policy for the Nest thermostat every year since they launched the thermostat in 2011.[164] The consumer will have to read each privacy policy, and where necessary give consent for the collection and processing of her personal data, or the profiling on the basis of her personal data.

Next to that, many of these Internet of Things devices will have only a small screen, or even lack a screen or another user interface where consumers can read privacy policies and give consent.[165] As a result, the consumer should be informed via another channels. For example, the third generation Nest thermostat has an LCD screen with a diameter of 5,3 centimetre. Nest Labs, Inc. provides a privacy policy for Nest product and services online.[166] This means that a consumer buys an object, installs it in her home, and then assumingly also reads the privacy policy online via her smart phone or computer. Research into the privacy policies of other Internet of Things manufacturers has indicated that these policies are hard to find and read for the consumer, and often are incomplete.[167]

Furthermore, a key aspect of the Internet of Things that follows from its origins in ubiquitous computing is that the technologies will "fade into the background"[168] and become "unobtrusive and invisible."[169] The invisibility of sensors and computing devices increases the likelihood that a consumer loses track of data flows running in the background on the connected devices she actively uses.[170] In connection to the invisibility of the apparatus, many Internet of Things devices will be always on to process audio, visual, or other sensor data even while the more powerful compute

162 Atzori, Iera and Morabito 2010, p. 2802.
163 OECD 2013, p. 10; see section 2.2.
164 Nest Labs 2016b.
165 Peppet 2014, p. 140-141.
166 Nest Labs 2015a.
167 Peppet 2014, p. 140-146.
168 Weiser 1991.
169 Gershenfeld 1999, p. 44.
170 Arnold, Hillebrand and Waldburger 2015, p. 65-66.

resources in the system are turned off.[171] In these circumstances, a one-time publication of an online privacy policy may technically inform the consumer, but after a while the data subject may be less "aware of and [able to] verify the lawfulness" of the profiling,[172] such as whether the settings of the devices still respect the data minimisation principle.[173]

Right to object against profiling

Furthermore, the right to object includes profiling:

> *Article 19*
>
> 1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to the processing of personal data concerning him or her which is based on points (e) or (f) of Article 6(1), *including profiling based on these provisions*. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.
>
> 2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to the processing of personal data concerning him or her for such marketing, *which includes profiling to the extent that it is related to such direct marketing*.
>
> (...)
>
> [emphasis added]

In other words, the General Data Protection Regulation provides the data subject with the right to object to profiling, if the profiling is necessary for a public task, or for the purposes of the legitimate interests pursued by the controller or by a third party. If the profiling is based on consent of the data subject, or is necessary for the performance of a contract to which the data subject is party, no such right to object exists.[174]

In a general manner, the preamble to the General Data Protection Regulation further specifies that "[m]odalities should be provided for facilitating the data subject's exercise of their rights provided by this Regulation, including mechanisms to request and if applicable obtain, free of charge, in particular access to data, rectification, erasure and to exercise the right to object. Thus the controller should also provide means for

171 Andrews and Przywara 2015.
172 Recital 51 GDPR; see cited above.
173 Čas 2011, p. 141.
174 In those two cases, if the data subject does not agree with the profiling (any longer), she could withdraw her consent under Article 7(3) of the Regulation, or break up the contract.

requests to be made electronically, especially where personal data are processed by electronic means."[175]

The right to object to profiling in the Internet of Things is limited in the situations that this research considers. Section 3.2 concluded that the legal basis for profiling of consumers in the Internet of Things may be that data subject has given consent to the profiling for one or more specific purposes, or that the profiling is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. The section also concluded that it is unlikely that profiling of consumers will be lawful because it is necessary for the purposes of the legitimate interests pursued by the controller or by a third party. As appears from above, the right to object does not exist in the case of consent or a contract.

Right not to be subject to decisions based on profiling

Last, the right not to be subject to decisions based on automated processing is tailored to profiling:

> *Article 20 GDPR*
>
> 1. The data subject shall have the right not to be subject to a *decision* based solely on automated processing, *including profiling*, which produces legal effects concerning him or her or similarly significantly affects him or her.
>
> 1a. Paragraph 1 shall not apply if the decision:
>
> (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller ; or
>
> (b) is authorized by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
>
> (c) is based on the data subject's explicit consent.
>
> 1b. In cases referred to in paragraph 1a (a) and (c) the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.
>
> (...)
>
> [emphasis added]

175 Recital 47 GDPR.

The General Data Protection Regulation's right not to be subject to a decision based solely on profiling is modelled on the old article on automated individual decisions in the Data Protection Directive:

> *Article 15 DPD*
>
> 1. Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.
>
> 2. Subject to the other Articles of this Directive, Member States shall provide that a person may be subjected to a decision of the kind referred to in paragraph 1 if that decision:
>
> (a) is taken in the course of the entering into or performance of a contract (...);
>
> (b) is authorized by a law (...).

The right is also inspired by the Council of Europe ("CoE") Recommendation on the protection of individuals with regard to automatic processing of personal data in the context of profiling, containing the following provision:[176]

> *Article 3 CoE Recommendation*
>
> (...)
>
> 3.4. Collection and processing of personal data in the context of profiling may *only* be performed:
>
> a. if it is provided for by law; or
>
> b. if it is permitted by law and:
>
> - the data subject (...) has given her or his free, specific and informed consent;
>
> - is necessary for the performance of a contract to which the data subject is a party (...);
>
> - is necessary for the performance of a task carried out in the public interest (...);
>
> - is necessary for the purposes of the legitimate interests of the controller or the third party or parties to whom the profiles or data are disclosed, except where such interests are overridden by the fundamental rights and freedoms of the data subjects;
>
> - is necessary in the vital interests of the data subject.
>
> [emphasis added]

176 Council of Europe 2010.

The preamble repeats and thus stresses that the right not to be subject to a decision based on profiling exists "as long as [the decision] produces legal effects concerning him or her or significantly affects him or her."[177] Furthermore, the preamble adds that the controller should implement safeguards including "specific information of the data subject and the right to obtain human intervention (...), to express his or her point of view, to get an explanation of the decision reached after such assessment and the right to contest the decision."[178]

Instead of applying the right not to be subject to a decision solely based on profiling in a general manner to profiling in the Internet of Things, this research points out the major problem with this right.

The problem with the new Article 20, paragraph 1, of the General Data Protection Regulation is that it ultimately depends on action from the data subject, just like the right to object in Article 19 of the Regulation. Both under the Regulation as well as under the Data Protection Directive the data subject "shall have the right not to be subject to a decision." As Bygrave notes, this formulation leaves "the actual exercise of the right to the discretion of each person, and allow[s], in effect, the targeted decision making to occur in the absence of the right being exercised" (provided that the profiling involved meets the other requirements of the Regulation).[179] The Regulation could also have formulated the right in terms of a prohibition.

Furthermore, the European Commission's original 2012 Proposal for a Regulation provided that a person could be subjected to a measure based solely on automated processing *only* if the processing was carried out in the course of the performance of a contract, was expressly authorized by the law, or was based on the data subject's consent.[180] Hildebrandt reviewed the original Proposal for a Regulation and concluded that the addition of "only" implied that the protection against profiling was not merely a right to object.[181] The CoE Recommendation may confirm Hildebrandt's conclusion, because the Recommendation provides that profiling may be performed "only" under

177 Recital 58 GDPR.
178 *Ibid.*
179 Bygrave 2001, p. 18.
180 Article 20(2) GDPR in European Commission 2012b.
181 Hildebrandt 2012, p. 50.

certain conditions, and does not characterize this provision as a right of the data subject.[182]

In the final compromise text for the Regulation this provision including the word "only" has been deleted, and is replaced by the provision that the right not to be subject to a decision does not apply if the concerned decision is based on the data subjects consent, is necessary for a contract, or is authorized by the law (see above). This deletion and change of provisions suggests that the protection against profiling in the end is in fact merely a right to object, and thus depends on action from the data subject.

[182] This can be inferred from the fact that the provision on profiling in the Council of Europe Recommendation is contained in the section "Conditions for the collection and processing of personal data in the context of profiling," not in the later section titled "Rights of data subjects;" see Council of Europe 2010.

4. THE OBJECT OF DATA PROTECTION IN THE INTERNET OF THINGS

The Article 29 Working Party opinion relied on a particular conception of data protection, even though there are alternative ways to conceive of data protection. In a brief historical overview, this chapter notes that the right to data protection is now separated from the right to privacy (section 4.1). The chapter than explains what is the origin of the Article 29 Working Party assumption that "users must remain in complete control over their personal data,"[183] and explores two alternative ways of conceiving of data protection (section 4.2). Under reference to findings in the previous chapters, this chapter then argues that in the Internet of Things, the object of data protection law should not be individual control, but general obligations of fair and transparent processing for the data controller (section 4.3). Finally, the chapter considers what this means for the question how the General Data Protection Regulation should apply to profiling in the Internet of Things (section 4.4).

4.1. AN INDEPENDENT RIGHT TO DATA PROTECTION

Initially, European Union law placed the protection of personal data in the service of the right to privacy. This approach is apparent in the objective of the 1995 Data Protection Directive. The objective of the Directive is to protect "the fundamental rights and freedoms of natural persons, and in particular *their right to privacy with respect to the processing of personal data*."[184]

With the proclamation of the Charter of Fundamental Rights of the European Union in 2000, the right to data protection is now formally separate and independent from the right to privacy under European Union law.[185] Article 8 of the Charter recognizes the fundamental right to the protection of personal data, next to the fundamental right to privacy in Article 7.

Nevertheless, the Court of Justice of the European Union implicitly still upholds the idea that the right to data protection is part of the right to privacy – at least in some cases. In the case of *Promusicae* the Court considered that the situation at issue involved "the

183 Article 29 Working Party 8/2014, p. 3.
184 1 Article 1(1) DPD.
185 On the emergence of personal data protection as a fundamental right of the EU see in general González Fuster 2014.

right that guarantees protection of personal data *and hence of private life*" [emphasis added].[186] The Court decided the case of *Promusicae* before the Charter became legally binding in 2009, but also thereafter the Court continues to link the right to data protection to the right to privacy. For example, in the 2010 case of *Volker und Markus Schecke*, the Court found that the right to the protection of personal data as contained in Article 8, paragraph 1, of the Charter "is closely connected with the right to respect of private life expressed in Article 7 of the Charter."[187]

By contrast, the General Data Protection Regulation that was proposed in 2012 just aims to protect the "fundamental rights and freedoms of natural persons and in particular *their right to the protection of personal data*."[188] What's more, the Regulation only states in the preamble that it in general respects other rights, among which is the right to respect for private and family life, home, and communications.[189] The Regulation does not introduce the right to data protection under reference to the right to privacy. In line with this, the Regulation talks about "data protection by design" instead of "privacy by design," and "data protection impact assessment" instead of "privacy impact assessment."[190] The idea that EU data protection law serves the right to the protection of personal data thus replaced the idea that this data protection law promotes the right to privacy.[191] This approach is consistent with the fact that the Charter also separates the two fundamental rights.

The question then is, how should we understand data protection under the Regulation if we disconnect it from privacy (acknowledging that data protection law is of course still partly instrumental to the protection of privacy)? Because the Court of Justice of the European Union still inclines to link the two, this research looks at other sources.

---

186 CJEU 29 January 2008, C-275/06 (*Promusicae*), para. 63.

187 CJEU 9 November 2010, in joined cases C-92/09 and C-93/09 (*Volker und Markus Schecke*), para. 47. González Fuster and Gellert are concerned about this "privacy thinking" of the CJEU; see González Fuster and Gellert 2012, p. 79-80.

188 Article 1(2) GDPR. Actually, both the DPD and the GDPR have a dual objective: protect rights, and enable the free flow of personal data between Member States (Art. 1, para. 1).

189 Recital 3a GDPR.

190 Respectively Articles 33 and 34 GDPR.

191 González Fuster 2014, p. 243.

4.2. COMPETING VISIONS ON DATA PROTECTION LAW

4.2.1. DATA PROTECTION AS INDIVIDUAL CONTROL OVER PERSONAL DATA

The Article 29 Working Party and many legal scholars say that the object of data protection always has been and should be about individual control over personal data.[192] In its opinion on the Internet of Things the Working Party stressed that "[i]n particular, users must remain in complete control of their personal data throughout the product lifecycle, and when organisations rely on consent as a basis for processing, the consent should be fully informed, freely given and specific."[193] According to the Working Party, providing users control over their personal data is also in the interest of the commercial stakeholders in the Internet of Things, since "empowering individuals by keeping them informed, free and safe is the key to support trust and innovation, hence to success on these markets."[194]

This idea that data protection is and should be about individual control can be traced back to Alan F. Westin,[195] who stated that information privacy (a type of privacy that corresponds to the European concept of data protection) "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."[196] Westin situated the value of information privacy in achieving individual goals of self-realization.[197]

The idea of data protection as individual control is also linked to the right of informational self-determination that was formulated in the 1983 "Census decision" of the Constitutional Court of Germany.[198] According to the German Constitutional Court the right of informational self-determination protects the individual from borderless collection, storage, use, and transmission of personal data.[199] Underlying the ideas of

192 Bygrave 2002, p. 130, who by the way himself conceives of data protection differently.
193 Article 29 Working Party 8/2014, p. 3.
194 *Ibid.*
195 Solove 2002, p. 1109-1110.
196 Westin 1967, p. 7.
197 Westin 1967, p. 39. Also see Bloustein 1964, p. 971, and Schwartz 1999.
198 65 BVerfGE 1 (1983), as discussed in Schwartz 1989. Paul Schwartz remarks that the term of informational self-determination was not new at the time of the Census decision; *ibid.*, p. 687.
199 Schwartz 1989, p. 689-690, quoting 65 BVerfGE 1, at 42.

individual control over personal data and informational self-determination is a liberal ideal of man being able to lead a self-determined, autonomous, authentic life.[200]

European data protection law realises the idea of individual control or informational self-determination by giving the data subject certain subjective rights (of information and access to data, to rectification, to erasure, etcetera), by listing consent as a basis for lawful collecting of data, and by prohibiting further processing without the data subject's consent.[201] The rights of information and access are in particular intended to support the exercise of individual control over data flows, and in the Internet environment these rights are developed via online privacy policies.

4.2.1. DATA PROTECTION AS RISK REGULATION OR OBLIGATIONS OF FAIR PROCESSING

However, the above concept of data protection law is one-sided. Next to individual control over personal data or informational self-determination, the object of data protection law could also be described as the regulation of risks stemming from the development of information and communication technologies,[202] or as general principles of fair processing (obligations for the controller to process data legitimately, fairly, and transparent).[203]

In fact, what is considered the source of all current data protection law demonstrates a view of data protection that is about risk regulation and fair processing.[204] In the 1960s and the 1970s the United States and subsequently Europe saw a convergence of two societal and technological developments. There was a growth of the amount of data held and used by public and private organizations in centralized databanks, and an expansion of possibilities for computerized collecting, linking, and accessing of personal data.[205] Against this background the United States Department of Health, Education & Welfare ("HEW") issued a report in which it set out a new approach to deal with computerized data processing ("the HEW report").[206]

---

200 Roessler 2005, p. 15.
201 Zie Bygrave 2002, p. 154. In the US information privacy laws prescribe notice and choice (also called notice and consent) systems for data processing.
202 Gellert 2015.
203 Van der Sloot 2015.
204 Gellman 2015.
205 Bygrave 2002, p. 94; Bennett 1992.
206 U.S. Department of Health Education & Welfare 1973.

The HEW report focused not just on the consequences of these trends for privacy, but more general on the consequences for individuals, organizations, and society as a whole. It found that the adverse effects of computerized record keeping ranged from inaccurate files leading to unfair decisions about individuals, and abuses of authorized access resulting in a loss of confidence in governmental institutions, to technicians treating social policy questions as if they were nothing more than questions of efficient technique.

The report committee concluded what was needed was the development of "legal principles comprehensive enough to accommodate a range of issues"[207] and therefore they developed the now well-known "principles of fair information practice" ("FIPPs").[208] These principles were based on the assumption that people must expect to share (with organizations) rather than "monopolize" control over their personal data.[209]

In sum, the principles of fair information practice were intended to regulate certain risks stemming from computerized record keeping, and concentrated on general obligations for the data controller, instead of on individual rights to control data flows. Since the FIPPs appear in all national and international data protection frameworks, including the General Data Protection Regulation (see all the "general principles" concerning data processing),[210] this means we can understand the object of data protection differently, while retaining the substance of data protection law.

4.3. WHAT DATA PROTECTION LAW *SHOULD* BE ABOUT IN THE INTERNET OF THINGS

The most comprehensive theory of data protection admits that data protection is about individual control over personal data, as well as about risk regulation and fair processing. In fact, the General Data Protection Regulation reflects all three elements. The Regulation operates on the assumption that individuals should have control of their own personal data,[211] and it contains new rules to improve individuals' ability to control

207 U.S. Department of Health Education & Welfare 1973, p. 38. Also see Gellert 2015, p. 6.
208 U.S. Department of Health Education & Welfare 1973, p. 41-42.
209 U.S. Department of Health Education & Welfare 1973, p. 40.
210 Bennett and Raab 2006, p. 12.
211 Recital 6 GDPR.

their data.[212] The Regulation also explicitly introduces a risk-based approach to data protection.[213] For example, the Regulation obliges controllers to take into account the *risks of varying likelihood and severity for the rights and freedoms of individuals* when implementing compliance measures, data protection by design, and security measures.[214] And, the Regulation demands that personal data must be processed fairly and transparent.[215]

This research nevertheless proposes that in the context of the Internet of Things data protection first and foremost *should* be about principles of fair processing that impose obligations on the parties responsible for the data processing.[216] The main reason is that individual control over personal data is practically unfeasible in the Internet of Things due to the following characteristics of this technology.[217] Section 3.3 already showed that the rights of information and access regarding profiling are untenable in an Internet of Things environment.

Furthermore, in many instances individuals are subjected to data collection and processing by other people's things,[218] for example if they stand in front of a connected security camera attached to their neighbour's doorbell, or if a resident in a communal living project installs a smart TV in the shared living room.[219] This means that whereas in the traditional Internet data protection problems arise mostly for active Internet users, in the Internet of Things scenarios for data protection issues arise even for people who are not using any Internet of Things device or service.[220]

In addition to these considerations, this research refers the more general limitations of control and consent mechanisms, as follow from the work of Acquisti and his colleagues.

---

212 European Commission 2012a, p. 6. Also see European Commission 2015b: "The new rules address [concerns about a loss of control] by strengthening the existing rights and empowering individuals with more control over their personal data."

213 Burton et al. 2016, p. 7.

214 Respectively Articles 22, 23, and 30. An other indicator of the risk based approach is the required communication of personal data breaches (see Costa and Poullet 2012, p. 256).

215 Article 5(1) GDPR.

216 In other contexts one could argue that the individual control aspect should be emphasized.

217 See in general on the impossibility of personal control in the Internet of Things Čas 2005. Other authors argue that because control is unfeasible, data protection in the Internet of Things should turn towards regulating personal data *use* instead of *collection*. See for example Wolf and Polonetsky 2013; Thierer 2014, p. 67. This path is not taken here.

218 Jones 2015.

219 The Guardian 2015; Jones 2015.

220 Atzori, Iera and Morabito 2010, p. 2802.

In one research, Acquisti and Grossklags demonstrate how decisions about data protection are affected by incomplete information, bounded rationality, and systematic psychological deviations from rationality. [221] If we translate their findings to profiling in the Internet of Things, this could mean the following.

Consumers in the Internet of Things are likely to attribute incorrect values to the likelihood of data protection risks, such as how easily they can be profiled and identified if a company knows the unique address of their Internet of Things device, and has monitored their day to night rhythm for a month.[222]

Next to that, even if consumers in the Internet of Things would have access to complete information, they might be unable to understand all the information and make a rational decision about whether or not to connect their smart TV to their toaster and thermostat. The explanation that Acquisti and Grossklags would give is that consumers use simplified mental models, such as "the device sends the data over a secured connection to the cloud, so the data is not transferred to other parties."[223]

Finally, even with access to complete information and unbounded ability to understand the information, consumers may be subject to psychological deviations from rational data protection decision-making. For example, someone may highly value the convenience of a connected coffee machine, and disregard the fact that a profile of her coffee drinking behaviour may also show at what times of the day she usually looses concentration and is more receptive to manipulative marketing offers.[224]

4.4. How the Regulation should be applied to profiling in the Internet of Things

The conclusion from the foregoing sections is that data protection law in the Internet of Things should mainly about fair processing obligations for the data controller and processor. With regard to the regulation of profiling under the General Data Protection Regulation, this would mean the following.

The question whether profiling in the Internet of Things is lawful within the meaning of the Regulation, is the least important question, since the two viable legal bases both

221 Acquisti and Grossklags 2005.
222 Acquisti and Grossklags 2005, p. 29-30.
223 Acquisti and Grossklags 2005, p. 30-31.
224 Acquisti and Grossklags 2005, p. 31-32.

presume rational data protection decision making from the consumer (consent or a contract).

Fair and transparent profiling in the Internet of Things requires that the consumer is informed of the profiling, and that the consumer is informed of her rights to object and not to be subjected to the profiling. These rights of information and access will be a less effective method of data protection.

However, transparency about profiling in the Internet of Things is also relevant for civil society "control" over data processing and in that regard information duties for the controller should not be disregarded. The General Data Protection Regulation states that where a type of processing is likely to result in a high risk for the rights and freedoms of individuals, the controller shall carry out a data protection impact assessment ("DPIA").[225] In any case, the Regulation already provides that such a data protection impact assessment shall in particularly be required in the case of profiling.[226] The Regulation further suggests that controllers that carry out a data protection impact assessment shall seeks the views of data subjects or their representatives on the intended processing.[227] These representatives could be civil society groups, who may inform themselves about the profiling via privacy policies and other information that controllers are required to make available to data subjects.[228]

The Regulation further provides that national supervisory authorities may establish a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment.[229] To preclude any uncertainty, these authorities should establish this with regard to profiling in the Internet of Things.

Just like the principle of lawful processing, the principle of purpose limitation is linked to individual control over personal data. In its opinion on purpose limitation the Article 29 Working Party noted that individual control is only possible when the purpose of data processing is sufficiently clear.[230] In its opinion on the Internet of Things, the

225 Article 33(1) GDPR.
226 Article 33(2)(a) GDPR.
227 Article 33(4) GDPR.
228 For a similar argument, see Zarsky 2013.
229 Article 33(2a) GDRP.
230 Article 29 Working Party 03/2013, p. 14.

Working Party therefore concluded that if data subjects understand the purposes of the data collection and profiling, they can decide whether to entrust an Internet of Things data controller with their data.[231]

However, in an Internet of Things environment, the purpose limitation, like the principles of fair and transparent processing, is of more value for civil society control.

The data minimisation, data quality, data security, and accountability principles are not directly tied to individual control, and therefore should be central to regulating profiling in the Internet of Things. The General Data Protection Regulation connects these principles to data protection by design and by default, and the required data protection impact assessments. In that respect, the preamble to the Regulation suggest that in certain circumstances "it may be sensible" that a data protection impact assessment is broader than a single project, for example "where several controllers plan to introduce a common application or processing environment across an industry sector or segment."[232]

The above comments could be repeated with regard to the specific rules in the General Data Protection Regulation concerning profiling. As far as the profiling provisions in the Regulation aim to enhance individual control over personal data, by giving the data subject rights of information and access, and the right to object and not to be subject to decisions based on profiling, their relevance in the Internet of Things will be minimal. Nevertheless, the detailed transparency requirements about profiling could be of use for civil society control over profiling. An oft-heard complaint by civil society organisation such as the Electronic Privacy Information Center ("EPIC") is there is little transparency about profiling practices.[233] From that perspective, the obligation of controllers to inform consumers about the logic involved with profiling, as well as the envisaged consequences of profiling, should be the focus of enforcement.

231 Article 29 Working Party 8/2014, p. 16.
232 Recital 72 GDPR.
233 EPIC 2016.

5. CONCLUSION

This research purported to solve the following research question:

> How will the General Data Protection Regulation apply to profiling based on data collected in the Internet of Things, and *how should the Regulation apply in this context*, based on an assessment what should be the object of data protection law?

To answer this question, it was first established that the Internet of Things is about connected and smart objects that operate in the background of people's lives, where the things learn about consumers' behaviours and preferences in order to deliver personalised services.

Then the research analysed how the General Data Protection Regulation will apply to the profiling of European consumers in the Internet of Things. The scope of application of the Regulation is wide, and it will cover about all profiling of European consumers in the Internet of Things, regardless of whether this is done by EU or non-EU based data controllers and processors. Naturally, the general principles of the Regulation governing processing of personal data will apply to profiling in the Internet of Things. These principles branch off in a range of obligations for the controllers and rights for the data subjects; those are not repeated here, but the general impression is that data protection is indeed becoming "the locus of regulation of very concrete things" with the Regulation.[234] In addition to the general principles, the Regulation will also address profiling in the Internet of Things via dedicated provisions that award certain rights to data subjects. None of these rules are new, and they all relate back to the more general principles and rights in the Regulation. Therefore, the rules on profiling are subject to the same critique that the research formulated in the second part of the research.

In that second part, the research determined how the General Data Protection Regulation should apply to profiling in the Internet of Things. The work of the Article 29 Working Party is strongly influenced by the presumption that individuals should be in control over their personal data in the Internet of Things. However, this research

234 De Hert 2015, p. 2.

showed there are other ways to conceive of data protection, most importantly general obligations of fair and transparent processing. The finding that individual control over personal data is hard to implement with regard to profiling in the Internet of Things, implies that application of the Regulation should be geared towards these general principles of fair and transparent processing. In that regard, the final section of this research highlights how enhanced transparency and information obligations for the controllers may shift the focus of control from individual data subjects, to civil society organisations. The Regulation provides ground to involve these organisations in data protection impact assessments. Via this route, EU data protection may be guided towards a more "principle-driven human rights system."[235]

This conclusion brings a new dimension to the discussion about profiling in the Internet of Things. There is more research needed to explore the full potential of the new General Data Protection Regulation in putting civil society "in control" over profiling in the Internet of Things. The European Commission could take the initiative, and promote such exploration with its expected policy action on the Internet of Things.

235 De Hert 2015, p. 2.

LITERATURE

(VERSIONS OF PROPOSED) LEGISLATION AND OTHER EU MATERIAL

Charter of Fundamental Rights of the European Union (*OJ* 2000, C 364/1).

Consolidated version of the **Treaty on the Functioning of the European Union** (*OJ* 2012, C 326/49).

Directive 95/46/EC of the European Parliament and of the Council of 24 October on the protection of individuals with regard to the processing of personal data and on the free movement of such data (*OJ* 1995, L 281/31) ("**Data Protection Directive**").

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (*OJ* 2002, L 201/37) ("**Directive on privacy and electronic communications**").

Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (*OJ* 2009, L 337/11).

Albrecht 2013

Jan-Phillip Albrecht, *Inofficial consolidated version after LIBE Committee vote provided by the rapporteur - Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)* , 22 October 2013, available at <https://www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf> (last accessed: 29 February 2016).

Council of the European Union 2016

Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [first reading] - Political agreement, 28 January 2016, available at <http://data.consilium.europa.eu/doc/document/ST-5455-2016-INIT/en/pdf> (last accessed: 29 February 2016).

Council of the European Union 2015

Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Preparation of a general approach, 15 June 2015, available at <http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf> (last accessed: 29 February 2016).

European Commission 2009
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), 18 June 2009.

European Commission 2012a
Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21st Century (COM(2012) 9 final), 25 January 2012.

European Commission 2012b
Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (**General Data Protection Regulation**) (COM(20212) 11 final), 25 January 2012.

European Commission 2015a
'Press release - Commission proposal on new data protection rules to boost EU Digital Single Market supported by Justice Ministers', 15 June 2015, available at <http://europa.eu/rapid/press-release_IP-15-5176_en.htm> (last accessed: 29 February 2016).

European Commission 2015b
'Press release - Agreement on Commission's EU data protection reform will boost Digital Single Market (IP/15/6321)', 15 December 2015, available at <http://europa.eu/rapid/press-release_IP-15-6321_en.htm> (last accessed: 29 February 2016).

European Parliament 2014
European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), 12 March 2014.

European Parliament 2010
European Parliament resolution of 15 June 2010 on the Internet of Things (2009/2224(INI)).

European Parliament, the Council and the Commission 2013
Joint Practical Guide of the European Parliament, the Council and the Commission for persons involved in the drafting of European Union legislation, Brussels: 11 July 2013.

European Union Agency for Fundamental Rights and Council of Europe 2014
European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European Data Protection Law*, Luxembourg: Publications Office of the European Union, 2014.

COUNCIL OF EUROPE MATERIAL

Council of Europe 2010

Recommendation of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling, Adopted by the Committee of Ministers on 23 November 2010 at the 1099th meeting of the Ministers' Deputies (CM/Rec(2010)13), 23 November 2010.

Council of Europe 2015

Council of Europe, 'What is the Committee of Ministers (CM)?', 2015, available at <http://www.coe.int/fr/web/tbilisi/committeeofministers> (last accessed: 29 February 2016).

ARTICLE 29 WORKING PARTY MATERIAL

Article 29 Working Party 2005

Working document on data protection issues related to RFID technology, (WP 105), 19 January 2005.

Article 29 Working Party 4/2007

Opinion 4/2007 on the concept of personal data, (WP 136), 20 June 2007.

Article 29 Working Party 1/2010

Opinion 1/2010 on the concepts of "controller" and "processor", (WP 169), 16 February 2010.

Article 29 Working Party 08/2012

Opinion 08/2012 providing further input on the data protection reform discussions, (WP 199), 5 October 2012.

Article 29 Working Party 03/2013

Opinion 03/2013 on purpose limitation, (WP 203) 03/2013.

Article 29 Working Party 05/2014

Opinion 05/2014 on Anonymisation Techniques, (WP 216) 10 April 2014.

Article 29 Working Party 8/2014

Opinion 8/2014 on Recent Developments on the Internet of Things, (WP 223), 16 September 2014.

Article 29 Working Party 9/2014

Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting, (WP 224), 25 November 2014.

CASE LAW

CJEU 19 November 1998, C-162/97 (*Nilsson, Hagelgren and Arrborn*).

CJEU 20 May 2003, in joined cases C-465/00, C-138/01 and C-139/01 (*Österreichischer Rundfunk*).

CJEU 29 January 2008, C-275/06 (*Promusicae*).

CJEU 9 November 2010, in joined cases C-92/09 and C-93/09 (*Volker und Markus Schecke*).

CJEU 13 May 2014, C-131/12 (*Google Spain v. Costeja González*).

CJEU 1 October 2015, C-230/14 (*Weltimmo*).

CJEU Request for a preliminary ruling from the Bundesgerichtshof (Germany) lodged on 17 December 2014, C-582/14 (*Patrick Breyer v. Bundesrepublik Deutschland*).

BOOKS AND ARTICLES

Accenture 2014

Accenture, *The Internet of Things: The Future of Consumer Adoption*, 2014.

Acquisti and Grossklags 2005

Alessandro Acquisti and Jens Grossklags, 'Privacy and Rationality in Individual Decision Making', *IEEE Security & Privacy*, 2005 (1), p. 26-33.

Al-Fuqaha et al. 2015

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.

Andrews and Przyware 2015

Gerard Andrews and Larry Przyware, *Keeping Always-On Systems On for Low-Energy Internet-of-Things Applications*, Cadence Design Systems, Inc., 2015.

Arnold, Hillebrand and Waldburger 2015

René Arnold, Annette Hillebrand and Martin Waldburger, *Personal Data and Privacy*, Bad Honnef: WIK-Consult GmbH, 26 May 2015.

Atzori, Iera and Morabito 2010

Luigi Atzori, Antonio Iera and Giacomo Morabito, 'The Internet of Things: A Survey', *Computer Networks*, 2010 (15), p. 2787–2805.

Barkin 2015

Samuel Barkin, 'Translatable? On Mixed Methods and Methodology', *Millennium Journal of International Studies*, 2015 (3), p. 1003-1006.

Bennett and Raab 2006

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

Van den Berg 2016

Bibi van den Berg, 'Mind the Air Gap', in: Serge Gutwirth, Ronald Leenes and Paul De Hert (eds.), *Data*

Protection on the Move: Current Developments in ICT and Privacy/Data Protection, Dordrecht: Springer, 2016, p. 1-24.

Bloustein 1964

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.

Blume 2012

Peter Blume, 'The inherent contradictions in data protection law', *International Data Privacy Law*, 2012 (1), p. 26-34.

Borgia 2014

Eleonora Borgia, 'The Internet of Things vision: Key features, applications and open issues', *Computer Communications*, December 2014, p. 1–31.

Brill 2014

Julie Brill, 'The Internet of Things: Building Trust and Maximizing Benefits Through Consumer Control', *Fordham Law Review*, 2014 (1), p. 205-217.

Burton et al. 2016

Cedric Burton, Laura De Boel, Christopher Kuner, Anna Pateraki, Sarah Cadiot and Sára G. Hoffman, *The Final European Union General Data Protection Regulation (Privacy & Security Law Report)*, Bloomberg BNA, 25 January 2016.

Bygrave 2002

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

Calo 2014

Ryan Calo, 'Digital Market Manipulation', *The George Washington Law Review*, 2014 (4), p. 995-1051.

Čas 2005

Johann Čas, 'Privacy in Pervasive Computing Environments - A Contradiction in Terms?', *IEEE Technology and Society Magazine*, 2005 (1), p. 24-33.

Čas 2011

Johann Čas, 'Ubiquitous Computing, Privacy and Data Protection: Options and Limitations to Reconcile the Unprecedented Contradictions', in: Serge Gutwirth, Yves Poullet, Paul De Hert and Ronald Leenes (eds.), *Computers, Privacy and Data Protection: an Element of Choice*, Dordrecht: Springer, 2011, p. 139-169.

Costa and Poullet 2012

Luiz Costa and Yves Poullet, 'Privacy and the regulation of 2012', *Computer Law & Security Review*, 2012 (3), p. 254-262.

Cryer et al., 2011

Robert Cryer, Tamara Hervey, Bal Sokhi-Bulley and Alexandra Bohm, *Research Methodologies in EU and International Law*, Oxford: Hart Publishing, 2011.

Cuijpers, Purtova and Kosta 2014

Colette Cuijpers, Nadezhda Purtova and Eleni Kosta, 'Data Protection Reform and the Internet: The Draft Data Protection Regulation', *Tilburg Law School Legal Studies Research Paper Series*, No. 03/2014.

Deloitte 2015

Deloitte, *Tech Trends 2015: The fusion of business and IT*, Deloitte University Press, 2015.

Eberlein and Newman 2008

Burkard Eberlein and Abraham L. Newman, 'Escaping the International Governance Dilemma? Incorporated Transgovernmental Networks in the European Union', *Governance*, 2008 (1), p. 25-52.

Eckes 2013

Christina Eckes, 'European Union Legal Methods - Moving Away From Integration', in: Ulla Neergaard and Ruth Nielsen (eds.), *European Legal Method - Towards a New European Legal Realism?*, DJOF Publishing, 2013, p. 163-188.

Edwards 2015

Lilian Edwards, 'Privacy, Security and Data Protection in Smart Cities: a Critical EU Law Perspective', *CREATe Working Paper 2015/11*, December 2015.

Evans 2011

Dave Evans, *The Internet of Things: How the Next Evolution of the Internet Is Changing Everything*, Cisco Internet Business Solutions Group (IBSG), April 2011.

Friedewald and Raabe 2011

Michael Friedewald and Oliver Raabe, 'Ubiquitous computing: An overview of technology impacts', *Telematics and Informatics*, 2011 (2), p. 55-56.

Gandy 1993

Oscar H. Gandy, *The Panoptic Sort: A Political Economy of Personal Information*, Boulder, CO: Westview Press, 1993.

Gandy 2010

Oscar H. Gandy, 'Engaging rational discrimination: exploring reasons for placing regulatory constraints on decision support systems', *Ethics and Information Technology*, 2010 (1), p. 29-42.

Gartner 2015

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

Gellert 2015

Raphaël Gellert, 'Understanding Data Protection as Risk Regulation', *Journal of Internet Law*, May 2015, p. 3-16.

Gellert and Gutwirth 2013

Raphaël Gellert and Serge Gutwirth, 'The Legal Construction of Privacy and Data Protection', *Computer Law & Security Review*, 2013 (5), p. 522–530.

Gellman 2015

Bob Gellman, *Fair Information Practices: A Basic History (Version 2.13)*, www.bobgellman.com, 11 February 2015.

Gershenfeld 1999

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

Gershenfeld, Krikorian and Cohen 2004

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

Van Gestel, Micklitz and Poiares Maduro 2013

Rob van Gestel, Hans-W Micklitz and Miguel Poiares Maduro, *Methodology in the New Legal World*, European University Institute, (EUI Working Paper LAW) 2012/13.

González Fuster 2014

Gloria González Fuster, *The Emergence of Personal Data Protetion as a Fundamental Right of the EU*, Cham: Springer, 2014.

González Fuster and Gellert 2012

Gloria González Fuster and Raphaël Gellert, 'The fundamental right of data protection in the European Union: in search of an uncharted right', *International Review of Law, Computers & Technology*, 2012 (1), p. 73-82.

Gubbi et al. 2013

Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic and Marimuthu Palaniswami, 'Internet of Things (IoT): A vision, architectural elements, and future directions', *Future Generation Computer Systems*, 2013 (7), p. 1645-1660.

Gumzej 2012

Nina Gumzej, 'Data protection for the digital age: comprehensive effects of the evolving law of accountability', *Juridical Tribune*, (2), p. 84-110.

Gutwirth et al. (eds.) 2011

Serge Gutwirth, Yves Poullet, Paul De Hert and Ronald Leenes (eds.), *Computers, Privacy and Data Protection: an Element of Choice*, Dordrecht: Springer, 2011.

Gutwirth and De Hert 2008

Serge Gutwirth and Paul De Hert, 'Regulating Profiling in a Democratic Constitutional State', in: Mireille Hildebrandt and Serge Gutwirth (eds.), *Profiling the European Citizens: Cross-Disciplinary Perspectives*, Springer, 2008, p. 271-302.

Gutwirth, Poullet and De Hert (eds.) 2009

Serge Gutwirth, Yves Poullet and Paul De Hert (eds.), *Data Protection in a Profiled World*, Dordrecht: Springer, 2009.

De Hert 2015

Paul De Hert, 'The Right to Protection of Personal Data. Incapable of Autonomous Standing in the Basic EU Constituting Documents?', *Utrecht Journal of International and European Law*, 2015 (80), p. 1-4.

De Hert and Papakonstantinou 2012

Paul De Hert and Vagelis Papakonstantinou, 'The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals', *Computer Law & Security Review*, 2012 (2), p. 130-142.

Hesselink 2009

Martijn Hesselink, 'A European Legal Method? On European Private Law and Scientific Method', January 2009 (1), p. 20-45.

Hijmans 2016

Hielke Hijmans, *The European Union as a Constitutional Guardian of Internet Privacy and Data Protection: the Story of Article 16 TFEU*, (diss. Amsterdam UvA), Amsterdam, 2016.

Hildebrandt 2008

Mireille Hildebrandt, 'Profiling and the Identity of the European Citizen', in: Mireille Hildebrandt and Serge Gutwirth (eds.), *Profiling the European Citizen: Cross-Disciplinary Perspectives*, Dordrecht: Springer, 2008, p. 303-343.

Hildebrandt 2012

Mireille Hildebrandt, 'The Dawn of a Critical Transparency Right for the Profiling Era', in: Jacques Bus, Malcolm Crompton, Mireille Hildebrandt and George Metakides (eds.), *Digital Enlightenment Yearbook 2012*, Amsterdam: IOS Press, 2012, p. 41-56.

Hildebrandt and Gutwirth (eds.) 2008

Mireille Hildebrandt and Serge Gutwirth (eds.), *Profiling the European Citizen: Cross-Disciplinary Perspectives*, Dordrecht: Springer, 2008.

Hildebrandt and Vries (eds.) 2013

Mireille Hildebrandt and Katja d. Vries (eds.), *Privacy, Due Process and the Computational Turn: The philosophy of law meets the philosophy of technology*, Abingdon, Oxon: Routledge, 2013.

Hornung 2012

Gerrit Hornung, 'A General Data Protection Regulation for Europe? Light and Shade in the Commission's Draft of 25 January 2012', *Scripted*, 2012 (1), p. 64-81.

Hustinx 2014

Peter Hustinx, *EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*, EDPS, 15 September 2014, available at <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2014/14-09-15_Article_EUI_EN.pdf> (last accessed: 29 February 2016).

Hutchinson 2013

Terry Hutchinson, 'Doctrinal research: Researching the jury', in: Dawn Watkins and Mandy Burton (eds.), *Research Methods in Law*, London: Routledge, 2013, p. 7-33.

Hutchinson and Duncan 2012

Terry Hutchinson and Nigel Duncan, 'Defining and Describing What We Do: Doctrinal Legal Research', *Deakin Law Review*, 2012 (1), p. 83-199.

Jones 2015

Meg L. Jones, 'Privacy Without Screens & the Internet of Other People's Things', *Idaho Law Review*, 2015, p. 639-660.

Kang and Cuff 2005

Jerry Kang and Dana Cuff, 'Pervasive Computing: Embedding the Public Sphere', *Washington and Lee Law Review*, 2005, p. 93-146.

Kirby 2010

Michael Kirby, 'The History, Achievement and Future of the 1980 OECD Guidelines on Privacy', *Journal of Law, Information and Science*, 2009/2010 (2), p. 1-14.

Klimas and Vaičiukaitė 2008

Tadas Klimas and Jūratė Vaičiukaitė, 'The Law of Recitals in European Community Legislation', *ILSA Journal of International & Comparative Law*, 2008 (1), p. 61-93.

Kokott and Sobotta 2013

Juliane Kokott and Christoph Sobotta, 'The Distinction Between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR', *International Data Privacy Law*, 2013 (4), p. 222-228.

Koops 2014

Bert-Jaap Koops, 'The trouble with European data protection law', *International Data Privacy Law*, 2014 (4), p. 250-261.

Korff 2012

Douwe Korff, *Comments on selected topics in the draft EU Data Protection Regulation*, London: 17 September 2012, available at <http://ssrn.com/abstract=2150145> (last accessed: 29 February 2016).

Kosta and Cuijpers 2015

Eleni Kosta and Colette Cuijpers, 'The Draft Data Protection Regulationand the Development of Data Processing Applications', in: Marie Hansen, Jaap-Henk Hoepman, Ronald Leenes and Diance Whitehouse (eds.), *Privacy and Identity Management for Emerging Services and Technologies, IFIP AICT 421*, Berlin: Springer-Verlag, 2015, p. 12-32.

Kuner 2012

Christopher Kuner, *The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law (Privacy and Security Law Report)*, Bloomberg BNA, 6 February 2012.

Kuner and Burton 2014

Christopher Kuner and Cedric Burton, 'EU Data Protection Regulators Issue Several Opinions on Key EU Data Protection Issues', 15 July 2014, available at <http://www.wsgrdataadvisor.com/2014/07/eu-data-protection-regulators-issue-several-opinions-on-key-eu-data-protection-issues/> (last accessed: 29 February 2016).

Larouche 2012

Pierre Larouche, *A Vision of Global Legal Scholarship*, Tilburg Law School Research Paper No. 09/2012, 2012.

Lyon (ed.) 2003

David Lyon (ed.), *Surveillance as Social Sorting: Privacy, risk, and digital discrimination*, London: Routledge, 2003.

Mäkinen 2015

Jenna Mäkinen, 'Data quality, sensitive data and joint controllership as examples of grey areas in the existing data protection framework for the Internet of Things', *Information & Communications Technology Law*, 2015 (3), p. 262–277.

Malgieri 2016

Gianclaudio Malgieri, 'Trade Secrets v Personal Data: a possible solution for balancing rights', *International Data Privacy Law*, forthcoming 2016.

Manwaring and Clarke 2015

Kayleen Manwaring and Roger Clarke, 'Surfing the third wave of computing: A framework for research into eObjects', *Computer Law & Security Review*, 2015 (5), p. 586–603.

Maras 2015

Marie-Helen Maras, 'Internet of Things: Security and Privacy Implications', *International Data Privacy Law*, (2), p. 99-104.

Mauritius Declaration 2014

Mauritius Declaration on the Internet of Things, adopted on the 36th International Conference of Data Protection and Privacy Commissioners, Balaclava: 14 October 2014, available at <http://www.privacyconference2014.org/media/16596/Mauritius-Declaration.pdf>.

Mayer-Schönberger and Cukier 2013

Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think*, Boston: Houghton Mifflin Harcourt, 2013.

McKinsey Global Institute 2015

McKinsey Global Institute, *The Internet of Things: Mapping the Value Beyond the Hype*, June 2015.

Miorandi et al. 2012

Daniele Miorandi, Sabrina Sicari, Francesco De Pelligrini and Imrich Chlamtac, 'Internet of things: Vision, applications and research challenges', *Ad Hoc Networks*, 2012 (7), p. 1497–1516.

Newman 2010

Abraham L. Newman, 'IO under dual obligation', in: Deborah D. Avant, Martha Finnemore and Susan K. Sell (eds.), *Who Governs the Globe?*, Cambridge: Cambridge University Press, 2010, p. 131-152.

OECD 2012

OECD, 'Machine-to-Machine Communications: Connecting Billions of Devices', *OECD Digital Economy Papers*, No. 192, OECD Publishing, 2012.

OECD 2013

OECD, *Building Blocks for Smart Networks*, Paris: OECD Publishing, 2013.

Ohm 2010

Paul Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization', *UCLA Law Review*, 2010, p. 1701-1777.

Olson, Nolin and Nelhans 2015

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.

Peppet 2014

Scott R. Peppet, 'Regulating the Internet of Things: First Steps Towards Managing Discrimination, Privacy, Security, and Consent', *Texas Law Review*, 2014 (1), p. 85-178.

Poullet 2009

Yves Poullet, 'About the E-Privacy Directive: Towards a Third Generation of Data Protection Legislation?', in: Serge Gutwirth, Yves Poullet and Paul De Hert (eds.), *Data Protection in a Profiled World*, Dordrecht: Springer, 2009, p. 3-30.

Regalado 2014

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

Roessler 2005

Beate Roessler, *The Value of Privacy*, Cambridge: Polity Press, 2005.

Rose, Eldrigde and Chapin 2015

Karen Rose, Scott Eldrigde and Lyman Chapin, *The Internet of Things: An Overview*, Geneva and Reston, VA: Internet Society (ISOC), October 2015.

Sarma, Brock and Ashton 2000

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, October 2000.

Savin 2015

Andrej Savin, 'Profiling in the Present and New EU Data Protection Frameworks', in: Peter A. Nielsen, Peter K. Schmidt and Katja D. Weber (eds.), *Erhvervsretlige emne*, Copenhagen: Juridisk Institut, Copenhagen Business School (CBS), 2015, p. 249-270.

Schaub et al. 2015

Florian Schaub, Rebecca Balebake, Adam L. Durity and Lorrie F. Cranor, 'A Design Space for Effective Privacy Notices', *Proceedings of the Eleventh Symposium On Usable Privacy and Security (SOUPS 2015),* USENIX Association, 22-24 July 2015.

Scherer and Heinickel 2014

Joachim Scherer and Caroline Heinickel, 'Regulating Machine-to-Machine Applications and Services in the Internet of Things', *European Networks Law & Regulation Quarterly*, 2014 (2), p. 141-155.

Schindler et al. 2013

Helen R. Schindler, Jonathan Cave, Neil Robinson, Veronika Horvath, Petal Hackett, Salil Gunashekar, Maarten Botterman, Simon Forge and Hans Graux, *Europe's policy options for a dynamic and trustworthy development of the Internet of Things, report prepared for the DG CONNECT*, 31 May 2013.

Schwartz 1989

Paul Schwartz, 'The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination', *The American Journal of Comparative Law*, 1989, p. 675-701.

Schwartz 1999

Paul Schwartz, 'Privacy and Democracy in Cyberspace', *Vanderbilt Law Review*, 1999 (6), p. 1609-1701.

Schwartz 2013

Paul Schwartz, 'Information Privacy in the Cloud', *University of Pennsylvania Law Review*, 2013 (6), p. 1624-1662.

Van der Sloot 2014

Bart van der Sloot, 'Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation', *International Data Privacy Law*, 2014 (4), p. 307-325.

Solove 2002

Daniel J. Solove, 'Conceptualizing Privacy', *California Law Review*, 2002 (4), p. 1087-1156.

Sykes 1999

Charles J. Sykes, *The End of Privacy: The Attack on Personal Rights - at Home, at Work, Online, and in Court*, New York, NY: St. Martin's Press.

Thierer 2014

Adam D. Thierer, 'The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation', *Richmond Journal of Law & Technology*, 2014 (2), p. 1-118.

U.S. Department of Health Education & Welfare 1973

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

Van Hoecke (ed.) 2011

Mark Van Hoecke (ed.), *Methodologies of Legal Research*, Oxford: Hart Publishing, 2011.

Vermesan and Friess (eds.) 2015

Ovidiu Vermesan and Peter Friess (eds.), *Building the Hyperconnected Society: IoT Research and Innovation Value Chains, Ecosystems and Markets*, Aalborg: River Publishers, 2015.

Vermeulen 2013

Mathias Vermeulen, 'Regulating profiling in the European Data Protection Regulation: An interim insight into the drafting of Article 20', *EMSOC Working Paper*, 1 September 2013.

Vranken 2012

Jan Vranken, 'Exciting Times for Legal Scholarship', *Law and Method (Recht En Methode in Onderzoek En Onderwijs)*, 2012 (2), p. 42-62.

Watkins and Burton (eds.) 2013

Dawn Watkins and Mandy Burton (eds.), *Research Methods in Law*, London: Routledge, 2013.

Weber 2015

Rolf H. Weber, 'Internet of Things: Privacy issues revisited', *Computer Law & Security Review*, 2015 (5), p. 618-627.

Weiser 1991

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

Westin 1967

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

Wolf and Polonetsky 2013

Christopher Wolf and Jules Polonetsky, *An Updated Privacy Paradigm for the "Internet of Things"*, Future of Privacy Forum, 19 November 2013.

Wright et al. (eds.) 2008

David Wright, Serge Gutwirth, Michael Friedewald, Elena Vildjiounaite and Yves Punie (eds.), *Safeguards in a World of Ambient Intelligence*, Dordrecht: Springer, 2008.

Zarsky 2013

Tall Zarsky, 'Transparency in Data Mining: From Theory to Practice', in: Bart Custers, Toon Calders, Bart Schermer and Tall Zarksy (eds.), *Discrimination and Privacy in the Information Society: Data Mining and Profiling in Large Databases*, Heidelberg: Springer, 2013, p. 301-324.

Ziegeldorf, Morchon and Wehrle 2004

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.

Zott, Amit and Massa 2011

Christoph Zott, Raphael Amit and Lorenzo Massa, 'The Business Model: Recent Developments and Future Research', *Journal of Management*, 2011 (4), p. 1019-1042.

Zuiderveen Borgesius 2016

Frederik J. Zuiderveen Borgesius, 'Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation', *Computer Law & Security Review*, forthcoming 2016.

INTERNET SOURCES

Business Insider 2015

John Greenough, 'The corporate 'Internet of Things' will encompass more devices than the smartphone and tablet markets combined', 9 July 2015, available at <http://uk.businessinsider.com/the-enterprise-internet-of-things-market-2015-7?r=US&IR=T> (last accessed: 29 February 2016).

EPIC 2016

EPIC, 'Algorithmic Transparency: End Secret Profiling', 2016, available at <https://epic.org/algorithmic-transparency/> (last accessed: 29 February 2016).

EurActiv 2015

Jorge Valero, 'Commission to unveil Internet of Things plan by mid-2016', 1 December 2015, available at <http://www.euractiv.com/sections/innovation-industry/commission-unveil-internet-things-plan-mid-2016-319886> (last accessed: 29 February 2016).

Gartner 2015

Rob van den Meulen, '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> (last accessed: 29 February 2016).

The Guardian 2015

Elisabeth Braw, 'Communal living projects moving from hippie to mainstream', 11 May 2015, available at <http://www.theguardian.com/sustainable-business/2015/may/11/communal-living-projects-moving-from-hippie-to-mainstream> (last accessed: 29 February 2016).

Harvard Business Review 2014

Simona Jankowski, 'The Sectors Where the Internet of Things Really Matters', 22 October 2014, available at <https://hbr.org/2014/10/the-sectors-where-the-internet-of-things-really-matters/> (last accessed: 29 February 2016).

Meloan 2003

Steve Meloan, *Toward a Global Internet of Things*, Sun Microsystems, 11 November 2003, available at <http://wenku.baidu.com/view/16859b26ccbff121dd368320.html> (last accessed: 29 February 2016).

Nest Labs 2015a

Inc Nest Labs, 'Privacy Statement for Nest Products and Services', 17 June 2015, available at <https://nest.com/legal/privacy-statement-for-nest-products-and-services/> (last accessed: 29 February 2016).

Nest Labs 2015b

Inc Nest Labs, '3rd Generation Nest Learning Thermostat Now Available in Europe', 17 November 2015, available at <https://nest.com/press/3rd-generation-nest-learning-thermostat-now-available-in-europe/> (last accessed: 29 February 2016).

Nest Labs 2016a

Inc Nest Labs, 'Meet the Nest Learning Thermostat', 2016, available at <https://nest.com/thermostat/meet-nest-thermostat/> (last accessed: 29 February 2016).

Nest Labs 2016b

Inc Nest Labs, 'Privacy Statement - archived', 2016, available at <https://nest.com/legal/privacy-statement/archive/> (last accessed: 29 February 2016).

Tado GmbH 2016

'Tado°, The Smart Thermostat for your Heating System', 2016, available at <https://www.tado.com> (last accessed: 29 February 2016).

Out-law.com 2014

''Internet of things' data should be 'treated as personal data', say privacy watchdogs', 21 October 2014, available at <http://www.out-law.com/en/articles/2014/october/internet-of-things-data-should-be-treated-as-personal-data-say-privacy-watchdogs/> (last accessed: 29 February 2016).