Consent as a basis of processing personal data in the Internet of Things

Master's thesis
University of Helsinki
Faculty of Law
November 2021
Ina Elevant
014700888

Abstract

Faculty: Faculty of Law

Degree programme: Master's degree programme in International Business Law

Study track: International Business Law

Author: Ina Elevant

Title: Consent as a basis of processing personal data in the Internet of Things

Level: Master's thesis

Month and year: November 2021

Number of pages: 62

Keywords: consent, IoT, GDPR, ePrivacy Directive, data protection

Supervisor or supervisors: Ville Pönkä

Where deposited:

Additional information:

Abstract:

The rise of the Internet of Things (IoT) has brought with itself an unimaginable ease to large-scale collection and sharing of personal data. Such large-scale collection and sharing are often done on the basis of data subject's consent. Consent enjoys a prominent role in the European data protection framework. Consent has, however, been criticised for not providing individuals with adequate protection in online environments. This problem will only be exacerbated with the rise of IoT as IoT extends the data collection practices of the online environments also to offline environments.

The purpose of this thesis is to explore the use of consent in the processing of personal data in the IoT. There are two research questions this thesis aims to answer: i) what are the problems and challenges related to the traditional consent based model in relation to IoT, and ii) is there an alternative way forward to user consent? This will be done through legal doctrinal methodology. However, this thesis will also take an interdisciplinary approach as it also draws from different disciplines than law such as technology, behavioural sciences and economics.

This thesis shows that, in digitalized world, consent is neither freely given nor informed; thus, challenging the notion of valid consent. These problems arise from information and power asymmetries that are present between data subjects and controllers. However, IoT also brings with itself a unique set of problems as most IoT devices lack screens and input methods making it hard for individuals to access information and provide consent. Moreover, the unobtrusive and ubiquitous nature of IoT makes data collection activities invisible making it hard to apply transparency principle. It is also predicted that the presence of IoT in public spaces leads to the diminishment of private spaces. In light of this, this thesis discusses some alternative ways forward to user consent. The first approach focuses on improving consent, while the second approach aims to shift the focus away from consent by placing accountability on controllers. While both of these alternatives have appeal, they do not come without challenges. Therefore, more research is needed in the field of IoT and data protection.

Table of Contents

List of abbreviations

Charter	Charter of Fundamental Rights of the European Union
CIPL	Centre for Information Policy Leadership
Citizen's Rights Directive	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
CJEU	Court of Justice of the European Union
Data Protection Directive	Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
EDPB	European Data Protection Board
ePrivacy 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 (Directive on privacy and electronic communications)
ePrivacy Regulation	Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) (2021) 6087/21

EU	European Union
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
IoT	Internet of Things
OECD	Organization for Economic Co-operation and Development
Planet49	Case C-673/17 *Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v Planet49 GmbH*
Tele2	Joined Cases C-203/15 and C- 698/15 Tele 2 *Sverige AB v Post- och telestyrelsen,* and *Secretary of State for the Home Department v Watson*
TFEU	Treaty on the Functioning of the European Union
WP29	Article 29 Data Protection Working Party

1. Introduction

Privacy has come under fire in the last decade due to rapid technological developments and the rise of the Internet. These developments have brought with them an unimaginable ease to a large-scale collection and sharing of personal data. While in the past privacy was seen as something to be protected from the unrestrained power of the state, nowadays technology allows both state authorities and private companies to "make use of personal data on an unprecedented scale in order to pursue their activities".[1] This kind of "multiveillance", where individuals are tracked not just by the state but also by companies, is enabled by millions of smart devices connected to the Internet also known as the Internet of Things (IoT).[2]

In the European Union (EU) the rights to privacy and protection of personal data are recognized as fundamental rights.[3] The Treaty on the Functioning of the European Union (TFEU), which is one of the two treaties forming the constitutional basis of the EU, also provides that everyone has the right to protection of personal data concerning them.[4] Although the right to privacy and data protection are two distinct fundamental rights, it is clear that privacy is a value that the right to protection of personal data aims to protect.[5] In the EU the fundamental right to data protection is being governed by the GDPR. The regulation aims to give natural persons "control of their own personal data".[6] According to Solove this kind of "privacy self-management" aims to provide people with rights that in turn provide them "with control over their personal data, and through this control people can decide for themselves how to weigh the costs and benefits of the collection, use, or disclosure of their information".[7]

At the heart of privacy self-management is the concept of consent. According to the Article 29 Data Protection Working Party (WP29), now replaced by the European Data Protection Board (EDPB), "the notion of consent is traditionally linked with the idea that the data subject should

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119, ("GDPR"), Recital 6.
[2] Jenna Lindqvist, 'Personal Data Protection on the Internet of Things an EU Perspective' (Doctoral dissertation, University of Helsinki, 2018) 1 < https://helda.helsinki.fi/handle/10138/263707> accessed 1 August 2021.
[3] Article 7 and 8(1) of the Charter of Fundamental Rights of the European Union [2012] OJ C 326 ("the Charter")
[4] Article 16 (1) of the Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C 326/47.
[5] Yvonne McDermott, 'Conceptualising the right to data protection in an era of Big Data' (2017) 4(1) Big Data & Society, 2 < https://journals.sagepub.com/doi/pdf/10.1177/2053951716686994> accessed 1 August 2021.
[6] Recital 7 of the GDPR
[7] Daniel J. Solove, 'Introduction: Privacy Self-Management and the Consent Dilemma' (2013) 126 Harvard Law Review 1879, 1880.

be in control of the use that is being made of his data".[8] Consent has been emphasized, for instance, in the Charter according to which personal data must be processed "on the basis of consent or some other legitimate basis laid down by law".[9] In other words, the Charter sees consent as a key aspect of the fundamental right of protection of natural persons in relation to the processing of personal data.[10] That prominent position of consent is also evident in the GDPR.[11] Significantly, consent is one of six legal bases under Article 6(1) of the GDPR that make processing of personal data lawful. Consent is also present in the ePrivacy Directive[12], which complements the current EU data protection regime by setting specific privacy rights on electronic communications. According to the ePrivacy directive consent is a prerequisite before information can be stored and accessed in devices.[13]

According to WP29 individual's consent has "always been a key notion in data protection".[14] Although consent is only one of six lawful basis of processing personal data in the GDPR, the others being performance of a contract[15], legal obligation[16], vital interest[17], public task[18] and legitimate interest[19], its widespread use seems to imply that it is the most commonly used basis for processing personal data. This seems to be the case especially in the online world, where notice and consent has become the dominant model for lawfully processing personal data.[20] However, consent should be only a lawful basis of processing when "data subject is offered control and is offered a genuine choice with regard to accepting or declining the terms offered or declining them without detriment".[21] In light of this, the use of consent as a basis for processing personal data has faced a lot of criticism. One of the main critiques being that

[8] WP29, 'Opinion 15/2011 on the definition of consent' (WP187, 13 July 2011) 8.
[9] Article 8(2) of the Charter
[10] WP29, 'Opinion 15/2011 on the definition of consent' (n 8) 5.
[11] See for example Recitals 7 and 75 of the GDPR that emphasize the need for control of personal data.
[12] 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 (Directive on privacy and electronic communications) [2002] OJ L 201/37 ("ePrivacy Directive").
[13] Article 5(3) of the ePrivacy Directive
[14] WP29, 'Opinion 15/2011 on the definition of consent' (n 8) 3.
[15] Art. 6(1)(b) of the GDPR
[16] Art. 6(1)(c) of the GDPR
[17] Art. 6(1)(d) of the GDPR
[18] Art. 6(1)(e) of the GDPR
[19] Art. 6(1)(f) of the GDPR
[20] Midas Nouwens et al., 'Dark Partterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence' (2020) Conference on Human Factors in Computing Systems, 2. < https://arxiv.org/pdf/2001.02479.pdf> accessed 8 August 2021.
[21] EDPB, 'Guidelines 05/2020 on consent under Regulation 2016/679' (4 May 2020) 5.

consent does not provide an adequate protection for personal data in online environments.[22] IoT will extend the data collection practices of the online environments to the offline environments.[23] Therefore, it is likely that any existing problems will only exacerbate with the rise of IoT as more and more devices will become connected to the Internet. This increase in Internet connected devices means that more personal data is being collected thus complicating privacy self-management.

1.1 Research questions and structure

The purpose of this thesis is to explore the use of consent in the processing of personal data in IoT. This thesis seeks to answer the following questions:

i) *What are the problems and challenges related to the traditional consent based model in relation to IoT?*

ii) Is *there an alternative way forward to user consent?*

The focus of this thesis will be EU law, specifically the GDPR and ePrivacy Directive. This thesis will also take a brief look of the proposed regulation concerning respect for private life and the protection of personal data in electronic communications[24] that is set to replace the ePrivacy Directive, as the proposed ePrivacy Regulation will cover IoT and alike technologies. Furthermore, as this thesis focuses on processing of personal data, it is logical to choose consumer IoT as the scope of the evaluation. Consumer IoT such as wearable technology, smart vehicles and home automation devices are directly interfaced to individuals. Moreover, consumer IoT devices are intended to monitor individuals' activities, behavior and even health.[25] This thesis will also briefly touch upon IoT in public spaces as IoT extends beyond the classic notion of private spaces.[26]

[22] See for example Bert-Jaap Koops, 'The Trouble with European Data Protection Law' (2014) 4(4) International Data Privacy Law 250, 251.
[23] Gilad Rosner and Erin Kenneally, 'Clearly Opaque: Privacy Risks of the Internet of Things' (2018) IoT Privacy Forum, 2 < https://www.iotprivacyforum.org/wp-content/uploads/2018/06/Clearly-Opaque-Privacy-Risks-of-the-Internet-of-Things.pdf?d8bd54&d8bd54 > accessed 15 October 2021.
[24] Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) (2021) 6087/21 ("ePrivacy Regulation").
[25] Gilad Rosner and Erin Kenneally, 'Privacy and the Internet of Things. Emerging Frameworks for Policy and Design' (2018) Center for Long-Term Cybersecurity, 7 <https://ssrn.com/abstract=3320670> accessed 30 September 2021.
[26] Ibid, 6-8.

The structure of this thesis will be as follows. Following this introductory chapter, the second chapter aims to provide an overview of IoT. Chapter 2 will also describe EU's data protection framework applicable to consumer IoT that is the GDPR and ePrivacy Directive. In addition, the chapter will briefly describe the proposed ePrivacy Regulation.

Chapter 3 introduces the concept of consent as defined in the GDPR. The chapter will also look of the notion of consent in the ePrivacy Directive. The chapter will then move on to discuss the elements of valid consent. In order for consent to be valid it should be freely given, specific, informed and unambiguous. These elements will be analyzed in detail in subchapter 3.3. Moreover, the chapter will explore the requirement of explicit consent. The remaining part will introduce additional conditions for obtaining valid consent.

The fourth chapter explores the problems and challenges related to consent in the processing of personal data in relation to IoT. Chapter 4 will start by introducing the rationale behind the use of consent in the European data protection framework. Then the chapter will move on to discuss the problems of consent and the unique set of challenges IoT brings to the consent-based model.

As chapter four aims to show that the consent-based model is failing to provide adequate protection to data subjects in digital environments, chapter 5 logically asks is there an alternative to user consent. Two alternative ways forward are discussed: improving consent or shifting the focus away from consent.

Lastly, chapter 6 will summarize what has been concluded in the previous chapters and provides an overall conclusion to this thesis.

1.2 Methodology

Before moving forward to the analysis, this section will describe the methodology used in this thesis. As the main aim of this thesis is to analyze and evaluate the use of consent in the processing of personal data in relation to IoT, a close look will be taken at the GDPR and the ePrivacy Directive. Thus, the legal doctrinal methodology will be employed.

Legal doctrinal methodology or "black letter" methodology "aims to give a systematic exposition of the principles, rules and concepts governing a particular legal field or institution and analyses the relationship between these principles, rules and concepts with a view to solving

unclarities and gaps in the existing law".[27] The legal doctrinal methodology thus focuses on primary sources of law, namely legislation and case law, and to some extent authoritative materials such as secondary sources of law e.g. legal literature and commentaries.[28] In other words, the legal doctrinal methodology mandates the author to locate the relevant statutory provisions and other authoritative materials that are relevant to the field of enquiry.[29]

This thesis places much weight on the opinions and reports of the WP29 and EDPB. The EDPB has been established by Article 68 of the GDPR. It is an independent advisory board on data protection consisting of the representatives of national supervisory authorities and the European Data Protection Supervisor. Although EDPB's (and its predecessors WP29's) opinions are not legally binding, they are considered authoritative in the field of data protection law.[30] Due to this particular nature of the EDPB (and its predecessor), and the fact that as of yet there is not much case law available on data protection[31], this thesis considers their opinions and reports to hold persuasive authority. Moreover, this thesis makes use of legal literature and academic debate surrounding the use of consent and IoT.

In order to answer the research questions, the doctrinal research undertaken in this thesis also takes a reformist approach. While pure doctrinal research analyses existing rules and the relationship between these rules, a reformist approach evaluates the adequacy of these existing rules and recommends changes to any rules found wanting.[32] Although reform-oriented research has been described by many as a separate methodology, "most 'good' quality doctrinal research goes well beyond description, analysis, and critique, and invariably suggests ways the law could be amended or the philosophy, processes or administration of the law could be improved".[33] Thus, this thesis considers the reformist approach undertaken as a support tool of the doctrinal legal research.

---

[27] Jan M. Smits, 'What is legal doctrine? On the aims and methods of legal-dogmatic research' (2015) Maastricht European Private Law Institute Working Paper No. 2015/06, 5 < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2644088 > accessed 8 August 2021.
[28] Ibid, 14-15.
[29] See Ibid (n 27) 12-16; Marnix Vincent Roderick Snel, 'Source-usage within doctrinal legal inquiry: choices, problems, and challenges' (2014) Law and Method < http://www.lawandmethod.nl/tijdschrift/lawandmethod/2014/06/RENM-D-13-00003/fullscreen> accessed 8 August 2021.
[30] Manon Oostveen, *Protecting Individuals Against the Negative Impact of Big Data. Potential and Limitations of the Privacy and Data Protection Law* (Kluwer Law International, 2018) ch. 4.
[31] Ibid.
[32] Terry Hutchinson, 'The Doctrinal Method: Incorporating Interdisciplinary Methods in Reforming the Law' (2015) 8(3) Erasmus Law Review 130, 132.
[33] Ibid.

IoT is very technical in nature. Moreover, law does not operate in a vacuum. Therefore, this thesis will also draw from different disciplines than law such as technology, behavioral sciences and economics. By doing this the analysis takes steps away from doctrinal legal methodology towards interdisciplinary one. This kind of interdisciplinary approach allows this thesis to get a wider and more informed understanding of the social context and technology to which the field of enquiry relates.[34] Interdisciplinary research, however, requires a balancing act as it is important that the focus of this thesis will not be shifted too much away from law. That is to say, it is important that this thesis provides a general description of IoT, without, however, going into too much technical details and specifications.

[34] See Paul Chynoweth, 'Legal research' in Andrew Knight and Les Ruddock (eds.), *Advanced research Methods in the Built Environment* (Blackwell Publishing, 2008) 30.

2. IoT

2.1 Defining IoT

IoT is a complex subject as it is based on several different technologies and disciplines. Consequently, IoT has been defined in a number of different ways. According to WP29 IoT refers to:

> "an infrastructure in which billions of sensors embedded in common, everyday devices – "things" as such, or things linked to other objects or individuals – are designed to record, process, store and transfer data and, as they are associated with unique identifiers, interact with other devices or systems using networking capabilities".[35]

The European Parliament, in turn, has defined IoT as:

> "a distributed network connecting physical objects that are capable of sensing or acting on their environment and able to communicate with each other, other machines and computers".[36]

And lastly, the European Commission describes IoT as follows:

> "The IoT is the next step towards digitalization where all objects and people can be interconnected through communication networks, in and across private, public and industrial spaces, and report about their status and/or about the status of the surrounding environment".[37]

What is common with these descriptions is the existence of objects that communicate with each other and are connected to the Internet. Such smart devices or sensors come in all shapes and sizes. Over the last years we have seen a rise of smart mobile devices, smart fridges, cars and TVs, as well as smart meters measuring the domestic consumption of water and energy and wearable devices such as smart watches. In other words, the Internet has moved away from just our computer screens to everyday objects in the domestic and consumer world.[38] However, IoT

[35] WP29, 'Opinion 8/2014 on the Recent Developments on the Internet of Things' (WP 223, 16 September 2014) 4.
[36] European Parliament, 'The Internet of Things: Opportunities and challenges', (Briefing) (May 2015), 1 <https://www.europarl.europa.eu/RegData/etudes/BRIE/2015/557012/EPRS_BRI(2015)557012_EN.pdf> accessed 9 August 2021.
[37] European Commission, 'Advancing the Internet of Things in Europe' SWD(2016) 110 final, 5.
[38] Lilian Edwards, 'Data Protection and e-Privacy: From Spam and Cookies to Big Data, Machine Learning and Profiling' in Lilian Edwards (ed.) *Law, Policy and the Internet* (Hart Publishing, 2019) 148.

should not be seen as an extension of Internet, but rather "a number of independent systems that operate with their own infrastructures (and partly rely on existing Internet infrastructures)".[39] The spread of IoT into domestic and human environments has also given a rise to specific terms such as "smart homes" referring to IoT being applied to the management of houses and "smart cities" where IoT is used to optimize and improve the efficiency of city infrastructure and resources.[40]

2.2 IoT and data

The network of Internet connected "things" has long surpassed the number or people.[41] It has been estimated that by 2025 there would be 30.9 billion IoT connected devices.[42] In the consumer sector it is expected that the smart home revenue in Europe will grow from 17 billion to 38.1 billion euros between 2020 and 2025, while the worldwide consumer IoT products and services revenue is expected to grow from 105.7 billion in 2019 to 404.6 billion euros in 2030.[43]

As the number of these smart "things" grow, so will the volume of data generated by them as these devices are "characterized by a high degree of autonomous data capture, event transfer, network connectivity and interoperability".[44] This exponential growth in the availability of data as well as its automated use is often referred as Big Data.[45] These large amounts of data are then collected, further combined and processed enabling, for example, businesses and governments to gain an insight on "how individuals live, work, travel, study, eat, or sleep, and how and what they consume".[46] Moreover, it has been shown that IoT devices such as smart phone sensors can show "user's mood; stress levels; personality type; bipolar disorder;

[39] European Commission, 'Internet of Things – An action plan for Europe' COM(2009) 278 final, 2.
[40] European Parliament (n 36).
[41] Lilian Edwards, 'Data Protection and e-Privacy: From Spam and Cookies to Big Data, Machine Learning and Profiling' (n 38) 148.
[42] Statista, Internet of Things (IoT) and non-IoT active device connections worldwide from 2010 to 2025 < https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/> accessed 9 August 2021.
[43] European Commission, 'Preliminary report – Sector Inquiry into Consumer Internet of Things' SWD(2021) 144 final, 6.
[44] CASAGRAS, 'RFID and the Inclusive Model for the Internet of Things' (2009) CASAGRAS EU Framework Project, Final Report, 10 <www.rfidglobal.eu%20CASAGRAS%20IoT%20Final%20Report%20low%20resolution.pdf> accessed 2 April 2020.
[45] Gloria Gonzalez Fuster and Amandine Scherrer, 'Big Data and Smart Devices and Their Impact on Privacy' (2015) Study for the LIBE Committee (European Parliament), 7 <https://op.europa.eu/en/publication-detail/-/publication/65d436ef-7273-11e5-9317-01aa75ed71a1> accessed 9 August 2021.
[46] Ibid, 8.

demographic (e.g. gender, marital status, job status, age); smoking habits; overall well-being, progression of Parkinson's disease, sleep patterns, happiness, levels of exercise; and types of physical exercise and movement".[47] Such information is expected to bring many benefits to businesses, consumer and governments alike.[48] These benefits may materialize for example through better healthcare, improved products, increased efficiency, cost savings, reduced consumption of resources and energy and through other solutions addressing societal challenges.[49] However, the collection, transmission, analyses, storage and sharing of data also raises a significant number of privacy and personal data concerns.[50]

2.3 Regulating processing of data in the IoT

2.3.1 The GDPR

The GDPR regulates the processing of personal data. Unless operating in an industrial environment, the data collected by IoT devices will most likely qualify as personal data in the sense of the GDPR.[51] According to Article 4(1) of the GDPR personal data means:

> "any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural 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, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

Furthermore, information about a device can qualify as personal data if it relates to an individual. The GDPR makes it clear that natural persons may be identified with online identifiers, such as IP addresses and RFIG tags, which are provided by smart devices and

[47] Scott R. Peppet, 'Regulating the Internet of Things: First Steps Towards Managing Discrimination, Privacy, Security & Consent' (2014) 93 Texas Law Review 85, 116.
[48] See European Parliament (n 36) 3-4.
[49] European Commission, 'Digitising European Industry Reaping the full benefits of a Digital Single Market SWD(2016) 110 final, 8.
[50] See Federal Trade Commission Staff Report, 'Privacy & Security in a Connected World (January 2015), ii <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf> accessed 28 August 2021.
[51] Article 29 Data Protection Working Party, 'Opinion 8/2014 on the Recent Developments on the Internet of Things' (n 35) 4.

applications.[52] These online identifiers enable identification when leaving traces; especially when combined with other information received by servers or other devices.[53]

In other words, "personal data" may include data, which has no or very little direct connection to a particular person.[54] However, when that data is combined with other data, that data can become "personal". This idea of personal data being formed from multiple pieces of data is especially relevant in terms of IoT. Data collected by IoT devices can easily fall within "personal data" as it is the business idea of IoT stakeholders to collect, analyze and combine large volumes of data to get the insight or result they want.[55] The more data there is available the better or more accurate the end result will be.[56] In addition, the large scale collection maximizes the utility of the data for the IoT stakeholders as "part of the benefit can only be realized by combining one set of data with others or through analyzing very large quantities of data to establish patterns or trends".[57]

The GDPR also makes a distinction between "personal data" and "sensitive personal data". Sensitive personal data is a set of special categories of personal data, which are considered sensitive in relation to fundamental rights and freedoms, and thus merit a special protection.[58] Such data includes information about racial and ethnic origin, political opinions, religious and philosophical beliefs, trade union membership, genetic data and biometric data where processed to uniquely identify someone as well as data concerning individuals' health, sex life and sexual orientation.[59] According to the GDPR the principle rule is that the processing of such data is prohibited, however there are exceptions to this general prohibition.[60] Many IoT devices and applications collect such sensitive data. A good example of such sensitive personal data is health data collected by wearable fitness trackers and watches. Moreover, personal data can become sensitive as time goes on.[61] For instance, location data can become sensitive, when

[52] Recital 30 of the GDPR
[53] Ibid.
[54] Lindqvist (n 2) 38.
[55] European Parliament (n 36) 6; Article 29 Data Protection Working Party, 'Opinion 8/2014 on the Recent Developments on the Internet of Things' (n 35) 4.
[56] Daniel Bastos et al., 'GDPR Privacy Implications for the Internet of Things' (4th Annual IoT Security Foundation Conference, London, 2018), 2 <https://www.researchgate.net/publication/331991225_GDPR_Privacy_Implications_for_the_Internet_of_Things > accessed 16 August 2021.
[57] European Parliament (n 36) 9.
[58] Recital 51 of the GDPR
[59] Article 9(1) of the GDPR
[60] Article 9(2) of the GDPR gives exceptions to this rule one of which is that data subject has given explicit consent to the processing.
[61] Lindqvist (n 2) 60.

individual's location is tracked over time. Frequent visits to a particular church or hospital can reveal information about individual's religion and health. In other words, although an IoT stakeholder would not directly collect sensitive personal data, they might be able to infer it from the data collected. The fact that location data can disclose sensitive information has also been acknowledged by the Court of Justice of the European Union (CJEU), which found in its ruling in *Tele2* case that traffic and location data allow "very precise conclusions" to be drawn about the private lives of the persons whose data has been retained, including their everyday habits, their places of residence, daily movements, the activities carried out, their social relationships and social environments, which in part, can provide the means to establish a profile of the person concerned.[62]

2.3.2 ePrivacy Directive and the draft ePrivacy Regulation

The ePrivacy Directive is focused on protecting privacy and confidentiality of personal data in electronic communication sector.[63] The ePrivacy Directive is a *lex specialis* to the GDPR, meaning that if both regimes apply, the special rules of ePrivacy Directive will prevail over general provisions of the GDPR.[64] While the GDPR is grounded on Article 8 of the Charter (protection of personal data), the ePrivacy Directive also details a right to respect for private and family life, as enshrined in Article 7 of the Charter.[65] The ePrivacy Directive will likely apply to IoT devices as the Directive is applicable to data collection from terminal equipment, in other words from a device connected to a public communication network.

According to Article 5(3) of the Directive where information is stored or to accessed on a user's or subscriber's device, the user must give consent to such storage or access. As the article refers to any type of information, the information also includes personal data. This is confirmed by Recital 24 of the Directive which states that user's device and any information stored in it are part of the user's private sphere requiring protection. The ePrivacy Directive also details rules for the processing of location and traffic data for the providers of public communication

[62] Joined Cases C-203/15 and C- 698/15 *Tele 2 Sverige AB v Post- och telestyrelsen, and Secretary of State for the Home Department v Watson* [2016] ECLI:EU:C:2016:970, para 99.
[63] Article 1 of the ePrivacy Directive.
[64] See Article 95 and Recital 173 of the GDPR that confirm the *lex generalis* and *lex specialis* relationship between the GDPR and the ePrivacy Directive, with Article 95 stating that it shall not impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC that is the ePrivacy Directive.
[65] Recital 2 of the ePrivacy Directive

networks and service providers.[66] This kind of metadata is a key piece of data collected by IoT devices.[67] The Directive provides different rules for these two types of data, however, through modern communication technologies and services the line between these has become blurred.[68]

While the rules for processing location and traffic data only apply to providers of publicly available electronic communication services and providers of public communication networks, the rules detailed in Article 5(3) set out standards for all actors that wish to store, or access information stored in user's device. In other words, article 5(3) is a general provision that applies to every entity regardless of the sector they operate in or the nature of the data being stored or accessed. It should, however, be noted that data such as traffic and location data are not collected only by traditional service providers such as telecoms and internet service providers, but also by many different organizations via different routes. These organizations can thus gain access to a very detailed overview of user's movements and communication patterns, while the ePrivacy Directive's scope does not apply to them as long as they do not access the information stored in user's device.[69] Most of ePrivacy Directive's provisions apply only to these traditional providers, thus making its scope narrower than the GDPR as the latter applies regardless of the sector.

The ePrivacy Directive does not explicitly mention IoT devices, and as seen above it is clear that the Directive has been designed to fit more traditional electronic communication providers as well as traditional devices such as computers and mobile phones. Thus, it is unclear to what extent does Article 5(3) of the ePrivacy Directive apply to IoT. For example, can an IoT sensor be seen as a terminal equipment of a user? Moreover, who can be considered to be the user or subscriber of the device? As Lilian Edwards puts it "is the owner of the connected car (who may not be the usual occupier) – or everyone who rides in it? Since the data of *all* riders is likely to be collected, one would hope the latter".[70] These questions are left unanswered by the Directive. However, the ePrivacy Directive was amended in 2009 by the Citizen's Rights

[66] Article 6 and 9 of the ePrivacy Directive
[67] Lilian Edwards, 'Data Protection and e-Privacy: From Spam and Cookies to Big Data, Machine Learning and Profiling (n 38) 149.
[68] Article 29 Working Party, 'Opinion 03/2016 on the evaluation and review of the ePrivacy Directive' (WP 240, 19 July 2016), 13.
[69] Ibid.
[70] Lilian Edwards, 'Data Protection and e-Privacy: From Spam and Cookies to Big Data, Machine Learning and Profiling' (n 38) 152.

Directive to clarify the role of IoT devices.[71] Recital 56 of the Citizen's Rights Directive reads as follows:

> "technological progress allows the development of new applications based on devices for data collection and identification…When such devices are connected to publicly available electronic communications networks or make use of electronic communications services as a basic infrastructure, the relevant provisions of Directive 2002/58/EC (Directive on privacy and electronic communications)…should apply".

It is, however, the intention of EU to repeal the ePrivacy Directive, as a new ePrivacy Regulation is under discussions. The proposal of the ePrivacy Regulation specifically mentions IoT stating:

> "The use of machine-to-machine and Internet of Things services, that is to say services involving an automated transfer of data and information between devices or software-based applications with limited or no human interaction, is emerging. In order to ensure full protection of the rights to privacy and confidentiality of communications, and to promote a trusted and secure Internet of Things in the digital single market, this Regulation, in particular the requirements relating to the confidentiality of communications, should apply to the transmission of such services. The transmission of machine-to-machine or Internet of Things services regularly involves the conveyance of signals via an electronic communications network and, hence, constitutes an electronic communications service. This Regulation should apply to the provider of the transmission service if that transmission is carried out via a publicly available electronic communications service or network".[72]

In other words, it is clear that the proposed ePrivacy Regulation is intended to govern IoT. Further, it appears from the proposal that the ePrivacy Regulation may have, in some ways, a broader material scope than the GDPR. For example, the proposal provides that machine-to-machine communications will be covered by the Regulation. In practice, this would mean that non-personal data communicated between machines will be covered by the ePrivacy Regulation as the GDPR only applies to processing of personal data. Interestingly, however, the proposal

[71] 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 [2009] OJ L 337.
[72] Recital 12 of the ePrivacy Regulation.

Regulation has limited the material scope of the Regulation to transmission services and excluded the application layer, in other words, mobile applications.[73] Therefore, mobile applications would fall within the GDPR insofar as they process personal data. Although this thesis is mainly interested in IoT devices, this is of interest as mobile applications work as the primary interface through which individuals interact with their IoT devices.[74] For example, most smart home devices such as security, lighting, heating etc. will be controllable through a mobile application.

Moreover, the proposal Regulation extends the protection of "information stored in the terminal equipment"[75] to information "emitted by terminal equipment" as well as to any interference with the terminal equipment including using its processing capabilities.[76] However, as in the ePrivacy Directive, such interferences shall be allowed in case the end-user has given his or her consent. In addition, the proposal Regulation covers metadata related to terminal equipment of an end-user.[77] Such metadata could include for example "the numbers called, the websites visited, geographical location, the time, date and duration when an individual made a call etc.,".[78] This clearly applies to a lot of data collected by IoT devices. What's more, the Regulation recognizes that metadata may reveal very sensitive data such as habits and social relationships etc.[79] To conclude, the ePrivacy Regulation may apply to all metadata related to and all data going through an IoT device.

[73] Recital 12 of the ePrivacy Regulation.
[74] Ihor Feokristov, 'Mobile IoT Apps and All You need to Know About Them' (Relevant) < https://relevant.software/blog/mobile-iot-apps/ > accessed 1 September 2021; WP29, 'Opinion 8/2014 on the Recent Developments on the Internet of Things' (n 35) 12.
[75] Article 5(3) of the ePrivacy Directive
[76] Article 8(2) of the ePrivacy Regulation
[77] See Recital 2 and 20 of the ePrivacy Regulation
[78] Recital 2 of the ePrivacy Regulation
[79] Recital 2 of the ePrivacy Regulation

3. Consent

3.1 Consent and other legal grounds for processing personal data

Under the EU data protection framework, processing of personal data has to be lawful, fair and transparent.[80] The GDPR sets out several grounds for the lawful processing of personal data. According to Recital 40 of the GDPR "in order for processing to be lawful, personal data should be processed on the basis of the consent of the data subject concerned or some other legitimate basis". Section 1 of Article 6 lays down the grounds for lawful processing. These grounds are as follows:

a) a consent has been given by the data subject for a specific purpose
b) processing is necessary for the performance of a contract
c) there is a legal obligation
d) protecting the vital interest of the data subject or another person
e) public interest or exercising official authority
f) to carry out a legitimate interest of a data controller or a third party, where these interests do not override the fundamental rights and freedoms of the data subject

According to Article 6, at least one of these grounds must apply for the processing of personal data to be lawful.

The relationship between the lawful grounds leaves some questions open. Although the GDPR does not suggest a hierarchy between the lawful grounds for processing personal data, it is evident that consent is put in a prominent position.[81] Not only is consent listed first, but it is also referred to in the Recitals; consent is clearly presented as a lawful ground while a reference is only made to "the other" grounds.[82] In addition, consent is used in the GDPR both as a general ground for lawfulness and as specific ground for processing sensitive personal data. The prominence of consent is also advocated by its widespread use as well as its history in the EU data protection framework. The important role of consent has been emphasized in Articles 7 and 8 of the Charter. Therefore, consent has also been seen in some Member States as a

[80] See Recital 39 of the GDPR
[81] See also Shaira Thobani, 'Processing Personal Data and the Role of Consent' (2020) 2020 European Journal of Privacy Law & Technology 93; Benjamin Bergemann, 'The Consent Paradox: Accounting for the Prominent Role of Consent in Data Protection' in Marit Hansen et al. (eds.), *Privacy and Identity Management. The Smart Revolution* (Springer International Publishing, 2018); Koops (n 22).
[82] See Recitals 40 and 51 of the GDPR

preferred ground for processing personal data as the role of consent has been explicitly recognized in the Charter.[83] Further, consent has been considered a lawful ground for processing personal data since the Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data.[84] The Data Protection Directive presented the modern definition of consent, [85] which has not changed much since the introduction of the GDPR.

Article 4(11) of the GDPR defines consent as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her". In other words, a valid consent consists of all of these elements.

3.2 Consent in the ePrivacy Directive

As we saw in section 2.3.2, consent is also very much present in the ePrivacy Directive as some of the provisions of the Directive require consent. This is the case, for example, regarding storing of information or accessing information already stored in user's or subscriber's terminal equipment detailed in Article 5(3). In relation to IoT, this consent requirement is the primary concern of device manufacturers as well as other stakeholders who want to access data stored in the IoT device.[86] In such circumstances, the stakeholders must ensure that the user or subscriber has been provided with clear and comprehensive information about the purposes of the processing.[87]

There are also exceptions to the Article 5(3) consent requirement. These exceptions include i) "technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communication network", or ii) "as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user".[88] However, it has been noted that the data transmitted by IoT devices "by default" for technical reasons, is increasingly used for intrusive purposes such as marketing and market analyses that

[83] WP29, 'Opinion 15/2011 on the definition of consent' (n 8) 7.
[84] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31 ("Data Protection Directive").
[85] WP29, 'Opinion 15/2011 on the definition of consent' (n 8) 5.
[86] WP29, 'Opinion 8/2014 on the Recent Developments on the Internet of Things' (n 35) 14.
[87] Article 5(3) of the ePrivacy Directive
[88] Ibid.

is not related to the original purpose of broadcasting.[89] It is not clear from the Directive whether such marketing purposes could be considered strictly necessary to deliver a service requested by a user.

Consent is also required where location data other than traffic data is processed by the public communications networks or publicly available electronic communications services: "where location data other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, can be processed, such data may only be processed when they are made anonymous, or with the consent of the users or subscribers".[90] As the ePrivacy Directive differentiates between location data and traffic data, consent is required in regard to traffic data when a provider of a publicly available electronic communication service processes traffic data for marketing purposes, or to provide a value added service.[91] Value added service is defined as "any service which requires the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof".[92]

Keeping in mind the *lex specialis – lex generalis* relationship between the ePrivacy Directive and the GDPR, it should be noted that the processing of personal data with the complete range of possible lawful grounds provided by Article 6 of the GDPR cannot be applied when the ePrivacy Regulation explicitly states that a consent of the user or subscriber is required and the information constitutes personal data.[93] For example, Article 5(3) of the ePrivacy Directive shall take precedence over Article 6 of the GDPR with regards to the storing or accessing information in a device insofar as the information constitutes personal data.[94] However, any processing of personal data after the abovementioned processing operations, including processing personal data obtained by accessing information in the user's device, must be based on one of the grounds in Article 6 of the GDPR in order to be lawful. To put it another way, once the data accessed on a user's device has been uploaded on a server and there is a desire to further process such information, the processing is not subject to the ePrivacy Directive anymore but to the provisions of the GDPR.

[89] Article 29 Working Party, 'Opinion 03/2016 on the evaluation and review of the ePrivacy Directive' (n 68) 11.
[90] Article 9(1) of the ePrivacy Directive
[91] Article 6(3) of the ePrivacy Directive
[92] Article 2(g) of the ePrivacy Directive
[93] EDPB, 'Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities' (12 March 2019), 13-14.
[94] Ibid.

The concept of consent in the ePrivacy Directive is defined in Article 2(f) according to which consent "corresponds to the data subject's consent in Directive 95/46/EC". As the Data Protection Directive has been replaced by the GDPR, consent shall have the same meaning as defined in the GDPR. This has been confirmed by the EDPB according to which the references to the repealed Data Protection Directive shall be understood as references to the GDPR.[95] In other words, this means that when the ePrivacy Directive requires user's or subscriber's consent, the criteria to determine whether consent is valid is the same as in the GDPR.

3.3 Elements of valid consent

As described above, the requirements for valid consent under the EU data protection framework are freely given, specific, informed and unambiguous indication of data subject's wishes. These requirements apply whenever consent is sought. The meaning of these elements of consent, will be discussed in detail below.

3.3.1 Freely given

For a consent to be considered freely given the first element is that the data subject is able to exercise real choice.[96] That means that there is no risk of "deception, intimidation, coercion or significant negative consequences" if the data subject does not consent.[97] If any of these elements are present, the data subject's consent cannot be considered freely given. This is also clarified by Recital 42 of the GDPR according to which "consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment".

Consent is not considered to be freely given where there is a clear imbalance of power between the data subject and controller. According to Recital 43: "in order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority, and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation". In other words, Recital 43 makes

[95] See EDPB, 'Statement of the EDPB on the revision of the ePrivacy Regulation and its impact on the protection of individuals with regard to the privacy and confidentiality of their communications' (25 May 2018) < https://edpb.europa.eu/sites/default/files/files/file1/edpb_statement_on_eprivacy_en.pdf> accessed 18 September 2021.
[96] WP29, 'Opinion 15/2011 on the definition of consent' (n 8) 12.
[97] Ibid.

it clear that it is unlikely that public authorities can rely on consent for processing personal data. Imbalance of power also occurs in employment relationships.[98] Due to the nature of employee-employer relationship, it is not likely that the employee is able to deny his or her employer consent to data processing as the consequence might be a loss of a job.

Freely given consent also implies that the data subject has control of the processing of his or her personal data.[99] If consent is bundled with the acceptance of terms and conditions, or there is an inability to refuse of withdraw consent without detriment, it is presumed that consent is not freely given.[100] Article 7(4) of the GDPR highlights that the performance of a contract, including a delivery of service, should not be conditional on consent, where such processing of personal data is not necessary for the performance of that contract. According to Recital 43 of the GDPR in such a case consent shall not be considered freely given. The purpose behind article 7(4) is that consent does not become the counter-performance of a contract.[101] As consent is a distinct legal ground from the performance of a contract, these two legal grounds "cannot be merged and blurred".[102]

Furthermore, Recital 43 also clarifies that consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations respectively. In other words, consent mechanisms should be executed in way that offers granularity. Consent should cover "all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them".[103] If the process does not allow the data subject to give separate consent for each separate purpose, there is considered to be a lack of freedom.

3.3.2 Specific

The second element of valid consent requires that consent must be given in relation to "one or more specific purposes".[104] In other words, the data subject should know the exact purpose of the processing of his or her data. A blanket consent is thus not acceptable. Further, if data is processed for multiple purposes, the data subject should consent to all of them.[105] In other

[98] EDPB, 'Guidelines 05/2020 on consent under Regulation 2016/679' (n 21) 9.
[99] Ibid, 7.
[100] See for further discussion section 3.5.2.
[101] EDPB, 'Guidelines 05/2020 on consent under Regulation 2016/679' (n 21) 10.
[102] Ibid.
[103] Recital 32 of the GDPR
[104] Article 6(1)(a) of the GDPR
[105] Recital 43 of the GDPR

words, there must be granularity in consent requests as discussed in section 3.3 above. For example, if a consent is asked for the data subject to receive behavioral advertising that same consent would not cover transfer of personal data to third parties. Instead, a separate consent should be received for that particular purpose. Moreover, the GDPR does not contain a specific time limit for consent. When data is processed for a particular purpose and later on that purpose changes or evolves considerably, the original consent is no longer valid.[106] In such an instance the data subject must be informed of these changes and a new consent must be sought to such new specific purpose.[107]

In addition, pursuant to Article 5(1)(b) of the GDPR personal data shall be collected for specified, explicit and legitimate purposes. In other words, prior to obtaining consent, the data controlled must consider what specific purpose or purposes the data will be used for.[108] This purpose limitation functions as a safeguard so that the purpose of the data processing is not gradually widened and blurred.[109] The danger with this "function creep" is that personal data is used beyond the original purpose resulting to unanticipated use of the personal data and the loss of data subjects control.[110] The purpose limitation thus limits for which purposes the data collected can be used for, and also helps to establish safeguards on data protection.[111]

The requirement that consent must be specific is also closely linked to the requirement of informed consent. In order for the data subject to be able to give specific consent, he or she needs to be made aware of the different aspects of the processing: the purposes of the processing and what data is being processed. Being clear and specific about the purposes of the processing is necessary also to comply with the principle of transparency.[112] According to WP29 "a purpose that is vague or general, such for instance 'improving users' experience', 'marketing purposes', 'IT-security purposes' or 'future research' will – without more detail – usually not meet the criteria of being 'specific'".[113]

[106] EDPB, 'Guidelines 05/2020 on consent under Regulation 2016/679' (n 21) 23.
[107] WP29, 'Opinion 15/2011 on the definition of consent' (n 8) 19.
[108] WP29, 'Opinion 03/2013 on purpose limitation' (WP 203, 2 April 2013), 15.
[109] EDPB, 'Guidelines 05/2020 on consent under Regulation 2016/679' (n 21) 14.
[110] Ibid.
[111] WP29, 'Opinion 03/2013 on purpose limitation' (n 108) 15.
[112] See Article 5(1)(a) of the GDPR
[113] WP29, 'Opinion 03/2013 on purpose limitation' (n 108) 16.

3.3.3 Informed

The third element of valid consent is that the consent is informed. As seen above, the concepts of specific and informed consent are linked. In order for the data subject to be able to provide informed consent, they must have received specific information prior to consenting. In other words, the data subject must be able to understand to what he or she is consenting to. This also applies to being able to withdraw his or her consent.[114] Informed consent is thus integrally linked to the principal of transparency. If the data subject is not provided with appropriate information, the consent will not be valid.[115]

According to WP29 guidelines on transparency data subjects should be able to determine prior to processing what the scope and consequences of the processing entail.[116] In addition, it should not come as a surprise to them later on how their personal data has been used.[117] This has also been highlighted in Recital 39 of the GDPR according to which "natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing". As per WP29, these are also important aspects with the principle of fairness, a principle that is closely related with the principle of transparency.[118]

According to Recital 42 of the GDPR "for consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended". Further, according to the GDPR when requesting consent, such request should be presented in a clear and plain language and in a manner, which is clearly distinguishable from the other manners and provided in an intelligible and easily accessible form.[119] In other words, the way the information is presented is crucial to whether consent can be considered to be valid. According to the EDPB that means, for example, that the information provided by the controllers should be understandable to an average person and not only to a lawyer.[120] Moreover, the accessibility and visibility of information is important. For instance, the data subject should not have to seek out the appropriate information. For example, the information should be clearly different from non-privacy related information such as general

[114] EDPB, 'Guidelines 05/2020 on consent under Regulation 2016/679' (n 21) 15.
[115] Ibid.
[116] WP29, 'Guidelines on transparency under Regulation 2016/679' (WP260, 11 April 2018), 7.
[117] Ibid.
[118] See Article 5(1)(a) of the GDPR
[119] Article 7(2) of the GDPR
[120] EDPB, 'Guidelines 05/2020 on consent under Regulation 2016/679' (n 21) 16.

terms and conditions.[121] Recital 32 of the GDPR also provides that consent requests cannot be unnecessarily disruptive to users.

3.3.4 Unambiguous indication of wishes

The last element of valid consent is unambiguous indication of wishes. In other words, there should be no doubt whether the data subject has given his or her consent to the processing.[122] According to Article 4(11) of the GDPR consent requires "a statement or clear affirmative action". According to the EDPB this means that consent must always be given through an active and deliberate motion or declaration.[123] This could be done, for example, by written statement or oral statement, ticking a box when visiting an website, choosing technical settings for information society services or another statement or conduct.[124] However, the EDPB has emphasized that consent cannot be obtained through blanket acceptance of general terms and conditions which include consent provisions.[125] Such acceptance cannot be seen as clear affirmative action to consent to the processing of personal data.

The GDPR is also clear that silence or inactivity does not constitute consent.[126] In addition, according to the GDPR the same goes with pre-ticked boxes.[127] This has been confirmed by the CJEU in *Planet49* case.[128] In this case the CJEU held that the requirement of "indication" clearly means that there must be active rather than passive behavior from the data subject.[129] Thus, a pre-ticked box does not constitute active behavior and cannot be regarded as valid consent.[130] The CJEU reasoned that it is impossible in these kind of situations to know whether the user has given his or her consent to the processing by not removing the tick from the pre-selected box and whether such consent is informed.[131] It could be that the user has not read the information regarding the pre-ticked box or has not even seen the checkbox.[132] In other words, consent must be opt-in consent; opt-out consent is not valid under the GDPR.

---

[121] WP29, 'Guidelines on transparency under Regulation 2016/679' (n 113) 7.
[122] EDPB, 'Guidelines 05/2020 on consent under Regulation 2016/679' (n 21) 18.
[123] Ibid.
[124] Recital 32 of the GDPR
[125] EDPB, 'Guidelines 05/2020 on consent under Regulation 2016/679' (n 21) 18.
[126] Recital 32 of the GDPR
[127] Recital 32 of the GDPR
[128] Case C-673/17 *Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v Planet49 GmbH* [2019] ECLI:EU:C:2019:801.
[129] Ibid. para 52.
[130] Ibid.
[131] Ibid. para 55.
[132] Ibid.

The EDPB has also emphasized that consent mechanisms should be designed and presented in a way that it is clear to the data subject which action they are consenting to.[133] The action must be based on clear information and that information should be presented in a way that it is not mistaken for other material such as for an advertisement.[134] Further, the indication of wishes must be an action that can be told apart from other actions.[135] For instance, scrolling or swiping through a webpage does not constitute an unambiguous indication of wishes according to the EDPB as such action cannot be distinguished from other action by user.[136]

Recital 66 of the Citizens' Rights Directive reads that consent can be expressed through "using the appropriate settings of a browser or other application" where it is technically possible and effective. As the rule seems to apply to more traditional devices such as computers and smart phones, it is unclear whether under this rule users could choose when starting to use their new IoT device their privacy settings and such settings would constitute consent. Moreover, according to WP29 such settings "only deliver consent in very limited circumstances".[137] For example, by simply using a browser or other application which by default enables collection and processing of personal data, does not constitute an unambiguous indication of the data subject's wishes and thus a valid consent.[138] Furthermore, an average person is not aware how to access and use their device settings; not even when the instructions are included in the privacy policy.[139] Therefore, it could be hard for a controller to be confident that the data subject has been fully informed and actively made changes to their device settings.[140]

3.4 Explicit consent

There is a stricter regime for special categories of personal data. The processing of such sensitive personal data is prohibited, unless an exception has been provided for in the GDPR, or specifically in Union law or national legislation.[141] According to Recital 51 of the GDPR "derogations from the general prohibition for processing such special categories of personal data should be explicitly provided, inter alia, where the data subject gives his or her explicit

[133] EDPB, 'Guidelines 05/2020 on consent under Regulation 2016/679' (n 21) 19.
[134] WP29, 'Working Document 02/2013 Providing Guidance on Obtaining Consent for Cookies' (WP 208, 2 October 2013) 4.
[135] EDPB, 'Guidelines 05/2020 on consent under Regulation 2016/679' (n 21) 19.
[136] Ibid.
[137] WP29, 'Opinion 2/2010 on Online Behavioral Advertising' (WP 171, 22 June 2010), 3.
[138] Ibid 13-14.
[139] Ibid, 14.
[140] See WP29, 'Working Document 02/2013 Providing Guidance on Obtaining Consent for Cookies' (n 134) 4.
[141] See Article 9 of the GDPR

consent or in respect of specific needs in particular where the processing is carried out in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms".

Sensitive personal data may thus be processed by virtue of GDPR if the data subject has given his or her explicit consent,[142] the processing is necessary to protect the vital interests of the data subject,[143] the processing is done in the course of legitimate activities of a foundation, association or any other not-for-profit body,[144] the processing relates to data manifestly made public by the data subject,[145] or processing is necessary to defend a legal claim[146]. Moreover, processing sensitive data is allowed if the processing is necessary for legal reasons (such as obligations under employment, social security and social protection law),[147] processing is necessary for the reasons of substantial public interest[148] or public interest in the area of public health[149], processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems,[150] or processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.[151]

Although explicit consent remains one of many exceptions for processing sensitive personal data, it seems most likely that explicit consent will be the main exception used for processing sensitive data in commercial context. Although there is a linguistic indicator between "regular consent" and "explicit consent", the difference between these two standards is unlikely to be very large since there is already a "statement of clear affirmative action" -standard in place. According to the EDPB the term explicit refers to the way consent must be expressed.[152] Hence, the term explicit has been seen as a synonym to express consent.[153] An obvious way to make such an express statement of consent would be through a hand-written statement or a signature.

[142] Article 9.2(a) of the GDPR.
[143] Article 9.2(c) of the GDPR
[144] Article 9.2(d) of the GDPR
[145] Article 9.2(e) of the GDPR
[146] Article 9.2(f) of the GDPR
[147] Article 9.2(b) of the GDPR
[148] Article 9.2(g) of the GDPR
[149] Article 9.2(i) of the GDPR
[150] Article 9.2(h) of the GDPR
[151] Article 9.2(j) of the GDPR
[152] EDPB, 'Guidelines 05/2020 on consent under Regulation 2016/679' (n 21) 20.
[153] WP29, 'Opinion 15/2011 on the definition of consent' (n 8) 25.

However, in an online environment such explicit consent could be given by filling in an electronic form, sending an email, uploading a scanned document carrying the signature of the data subject or using an electronic signature.[154]

The WP29 has describes explicit consent as encompassing "all situations where individuals are presented with a proposal to agree or disagree to a particular use or disclosure of their personal information and they respond actively to the question".[155] It is thus clear that explicit consent requires an active motion from the data subject. This in turn means that a consent that is inferred from someone's actions cannot be considered explicit consent.[156] However, such active motion or declaration is also required in case of a "regular consent".

The EDPB also suggest a two-stage verification process as a way to make sure that explicit consent is valid.[157] According to the EDPB such process could go as follows: information is sent to the data subject explaining the intent to process sensitive personal data and the purposes for such processing. In order to consent, the data subject would be required to reply, "I agree". After that a verification link or code would be send to the data subject through an email or SMS to confirm the agreement. This suggestion of the EDPB thus seems to imply that explicit consent would require a statement of words rather than just an active motion.

It appears that there is only a subtle difference between "regular consent" and "explicit consent". In other words, it seems that these two concepts are somewhat blurred. Other than the two-stage verification process, the methods for obtaining each of them seem very similar. In addition, each of them requires a clear indication of the data subject's wishes.

3.5 Other conditions for obtaining valid consent

3.5.1 Prior consent

Consent must be obtained prior to processing of data. The timing of consent has not been explicitly mentioned in the GDPR. However, such timing can be inferred from the language of the Regulation. According to Article 6(1)(1) of the GDPR processing of personal data shall be

[154] EDPB, 'Guidelines 05/2020 on consent under Regulation 2016/679' (n 21) 21.
[155] WP29, 'Opinion 15/2011 on the definition of consent' (n 8) 25.
[156] Ibid.
[157] See EDPB, 'Guidelines 05/2020 on consent under Regulation 2016/679' (n 21) 21.

lawful if subject "has given" his or her consent to the processing. The language used here implies that consent must be obtained before processing commences.

Further, the ePrivacy Directive explicitly includes requirements of prior consent. For example, according to Article 6 of the Directive in order for the publicly available electronic communication service provider to process traffic data for the purpose of marketing electronic communication services or value-added services, such provider must provide the user or subscriber with information and to obtain the user's or subscriber's prior consent.[158]

As WP29 points out, obtaining consent before the processing of data is crucial in order to make the processing legitimate.[159] Without such prior consent, the processing would lack a legal ground.[160] If such consent is refused and the processing has started, the processing is unlawful.[161]

3.5.2 Withdrawal of consent

According to Article 7(3) of the GDPR data subject shall have the right to withdraw his or her consent at any time. By being able to withdraw his or her consent, the data subject is able to exercise some form of control of his or her data.[162] Although withdrawal does not retroactively render processing based on consent unlawful, it prevents any further processing of personal data.[163] Once consent is withdrawn, the controllers also have an obligation to erase such data, unless there is another purpose that justifies the processing.[164]

Furthermore, the data subject should not suffer any detriment from the withdrawal as highlighted by Recital 42 of the GDPR. For example, withdrawing consent should not lead to any costs for the data subject or to a clear disadvantage. In addition, withdrawal of consent should be as easy as to give consent. According to the EDPB if consent for processing is obtained through a certain electronic user interface, consent should be able to be withdrawn through that same interface.[165]

[158] See Articles 6(3) & 6(4) of the ePrivacy Directive
[159] WP29, 'Opinion 15/2011 on the definition of consent' (n 8) 9.
[160] Ibid, 30-31.
[161] Ibid, 30.
[162] Ibid, 9.
[163] Ibid.
[164] See Article 17 of the GDPR. EDPB, 'Guidelines 05/2020 on consent under Regulation 2016/679' (n 21) 24-25.
[165] EDPB, 'Guidelines 05/2020 on consent under Regulation 2016/679' (n 21) 23-24.

3.5.3 Demonstrating consent

According to Article 7(1) of the GDPR the controller needs to be able to demonstrate data subject's consent. This is further clarified in Recital 42, which states that "where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation." According to EDPB such an obligation also includes that the controller can show that the data subject was informed, and that the controller met all the criteria of valid consent.[166] This obligation to demonstrate valid consent is in place as long as the processing activity in questions lasts.[167] The purpose behind this obligation is to place accountability on the data controller.[168]

[166] Ibid, 22-23.
[167] Ibid.
[168] Ibid, 23.

4. Limitations of consent in the processing of personal data in IoT

4.1 Rationale behind consent

As we have seen, consent has been accorded great value in the European data protection framework. The current consent-based model is closely tied with the concept of information self-determination.[169] The concept was made known by the German Constitutional Court in 1983, which ruled in its famous decision on the constitutionality of the Census Act that the right of information self-determination is a constitutional fundamental right: "the fundamental right guarantees the authority conferred on the individual to, in principle, decide themselves on the disclosure and use of their personal data. Limitations of this right to "informational self-determination" are only permissible if there is an overriding public interest".[170] The principle of information self-determination, as expressed by the German Constitutional Court, reflects the value of individual's autonomy, ability to make choices and exercise control on his or her personal data.[171] At the heart of this principle is consent, which is used as a means of the "participatory right of information self-determination".[172]

It is clear that the EU data protection framework has been influenced by information self-determination. As we have seen, consent of the data subject has been given a prominent role in the GDPR and ePrivacy Directive. Consent is seen as an expression of free choice and is thus closely connected to the principle of autonomy.[173] Moreover, the GDPR emphasizes the

[169] WP29, 'Opinion 15/2011 on the definition of consent' (n 8) 9.
[170] BVerfGE 65, 1 – Volkszahlung Urteil des Ersten Senats vom 15. Dezember 1983 auf die ¨ mundliche Verhandlung vom 18. und 19. Oktober 1983 -1 BvR 209, 269, 362, 420, 440, 484/83 in den Verfahren uber die Verfassungsbeschwerden. English Abstract of the German Federal Constitutional Court's Judgment of 15 December 1983 <https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html> accessed 24 September 2021.
[171] Michelle De Mooy, 'Rethinking Privacy Self-Management and Data Sovereignty in the Age of Big Data. Considerations for Future Policy Regimes in the United States and the European Union' (2017) Center for Democracy and Technology, 15 < https://cdt.org/wp-content/uploads/2017/04/Rethinking-Privacy_2017_final.pdf> accessed 25 September 2021; Cécile de Terwangne, 'The Right to be Forgotten and the Information Autonomy in the Digital Environment' (2013) Publications Office of the European Union, 4 < https://publications.jrc.ec.europa.eu/repository/handle/JRC86750> accessed 25 September 2021.
[172] Eleni Kosta, *Consent in European Data Protection Law* (Martinus Nijhoff Publishers, 2013), 109.
[173] Bart W. Schermer, Bart Custers and Simone van der Hof, 'The Crisis of Consent. How Stronger Legal Protection may lead to Weaker Consent in Data Protection' [2014] Ethics and Information Technology, 5 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412418> accessed 27 September 2021.

importance of individuals' control over their personal data.[174] Such control is deemed to foster autonomy and empower individuals to manage their personal data.[175]

Soleve has referred to the current approach to privacy regulation as privacy self-management.[176] According to him under this current approach a set of rights is given to individuals such as rights of i) notice of the upcoming collection and use of personal data and ii) choice whether to consent to such processing of their personal data.[177] The purpose behind this set of rights is to give control to individuals over their personal data, and through this control individuals are expected to make privacy decisions based on costs-benefit analysis of the collection, disclosure and use of their data.[178] However, the emphasis on control and consent has not turned out to have the desired effects.

4.2 Problems with consent

Despite the prominence of consent in European data protection, consent has faced a lot of criticism. The problems with consent are especially obvious in the digitalized world. It has even been argued that, in online context, consent is not a suitable approach to data processing.[179] This section will explore the academic critique towards consent and discuss the problems related to IoT.

4.2.1 Problems with informed consent

The emphasis on consent is premised on the fact that individuals are rational actors who are able to make the best decisions for themselves and to navigate the obscure digital and technological environment. However, this approach has been criticized by many. The most common line of criticism seems to center the notion of informed consent. Consent must be based on appropriate information; this is essential for the data subject "in order to enable them to make informed decisions, understand what they are agreeing to, and for example exercise

[174] Recital 7 of the GDPR
[175] Christophe Lazaro and Daniel Le Métayer, 'The control over personal data: True remedy or fairy tale?' (2015) 12 SCRIPT-ed, 4 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2689223> accessed 27 September 2021.
[176] See Solove (n 7).
[177] Ibid, 1880.
[178] Ibid.
[179] See for example Koops (n 22) 251.

their right to withdraw their consent".[180] This transparency requirement is often implemented in the form of privacy notices.

i) People do not read privacy notices

The first critique addresses the fact that people do not tend to read privacy notices.[181] Although an important part of privacy self-management are notices, they are often many pages long, legalistic and difficult for a regular person to understand.[182] According to 2019 Eurobarometer, 37% of respondents do not read privacy statements at all, citing the length and difficulty of understanding being the main reasons for not reading them.[183]

Schermer, Custers and van der Hof have criticized the overemphasis on consent.[184] According to them such overemphasis has led to an information overload.[185] It has been estimated that it would take an average person 244 hours annually to read all the privacy notices he or she is being presented with.[186] That would mean an average of 40 minutes per day. In addition, companies regularly modify their privacy policies, so one would also have to keep up with these changes in order to stay informed. This overload of information will overwhelm the recipient "causing her to skim, freeze, or pick out information arbitrary".[187] According to Schermer, Custers and van der Hof the issue with information overload is further aggravated when consent is asked in situations where individuals are making completely different decisions, such as online shopping or booking a holiday".[188] Because privacy notices are so common, people will become tired of these procedures that take them away from the fun and functionality of the service. In similar fashion, those eager to use a new IoT device may bypass privacy information and become bound to terms and conditions they have no knowledge of. Privacy protection then

[180] EDPB, 'Guidelines 05/2020 on consent under Regulation 2016/679' (n 21) 15.
[181] Solove (n 7) 1885.
[182] Ibid.
[183] See European Commission, Special Eurobarometer 487a: The General Data Protection Regulation (2019) 48, 51.
[184] See Schermer, Custers and van der Hof (n 173).
[185] Ibid, 10-11.
[186] Aleecia M. McDonald and Lorrie Faith Cranor, 'The Cost of Reading Privacy Policies' [2008] I/S Journal of Law and Policy for the Information Society, 17-18 <https://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf> accessed 27 September 2021.
[187] M. Ryan Calo, 'Against Notice Skepticism in Privacy (and Elsewhere) (2012) 87 Notre Dame Law Review 1027, 1054.
[188] Schermer, Custers & van der Hof (n 173) 11.

becomes a tradeoff between "instant gratification… versus the abstract risks associated with the misuse or abuse of personal data".[189]

Moreover, according to Schermer, Custers and van der Hof there is an overload of consent transactions.[190] In other words, there are simply too many consent requests and privacy notices presented to individuals. According to them this will negatively affect the psychological function of being presented with a consent transaction".[191] The need to avoid this kind of "user fatigue" has also been warned by the EDPB. According to the EDPB "in the digital context, many services need personal data to function, hence, data subjects receive multiple consent requests that need answers through clicks and swipes every day. This may result in a certain degree of click fatigue: when encountered too many times, the actual warning effect of consent mechanisms is diminishing".[192]

The result of these overloads is that consent questions and privacy notices are no longer read.[193] Further, Schermer, Custers and van der Hof argue that information and consent transaction overload will lead to "consent decentralization".[194] This means that individuals will no longer make active and informed choices when asked for a consent, but rather give consent every time consent is asked.[195] This notion is supported by behavioral economics according to which when consent requests are encountered too many times, the act of making an informed decision becomes costly.[196] Thus, consenting becomes an automatic action where people rely on automatic impulses such as rules of thumb and heuristics rather than on conscious thinking.[197] This is a problem to the validity of informed consent.

ii) People do not understand privacy notices

Another argument that has been presented by scholars is that it is questionable whether people understand privacy notices. Privacy notices have been criticized of being inefficient as they are

[189] Ibid.
[190] Ibid, 10.
[191] Ibid.
[192] EDPB, 'Guidelines 05/2020 on consent under Regulation 2016/679' (n 21) 19.
[193] Ibid.
[194] Schermer, Custers & van der Hof (n 173) 12.
[195] Ibid.
[196] Santiago Ramirez Lopez, 'Informing Consent: Giving Control Back to the Data Subject from a Behavioral Economics Pespective' (2018) 9 Journal of Intellectual Property, Information Technology and E-Commerce Law 35, 42 <JIPITEC_9_1_2018_35-50_Ramirez_Lopez> accessed 27 September 2021.
[197] Ramirez Lopez (n 196) 42. See also Solove (n 7) 1887; Frederik Zuiderveen Borgesius, 'Informed Consent: We Can Do Better to Defend Privacy' (2015) 13 Security & Privacy, 7 < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2793769> accessed 27 September 2021.

not being read and are difficult for users to understand.[198] According to Solove people have several cognitive problems that cause issues to privacy self-management.[199] These cognitive problems negatively affect people's ability to make informed and rational choices when it comes to consenting to different forms of collection, use and disclosure of their personal data.[200] Data protection activities can be hard to understand for an average person; however, Soleve points out that individuals are also uninformed about the data collected about them as they do not engage in privacy self-management.[201] As highlighted above this could be due to multiple factors, the length of the notices and their difficulty being one of the commonly cited ones.[202] However, making the privacy policies shorter and easier to understand conflicts with fully informing people about the types of data being collected and the purposes of the processing.[203] According to Barocas and Nissenbaum this "transparency paradox" means that loss of complexity inevitably results to loss of specificity.[204] People need to be provided with specific information to be able to make informed choices and simplified, plain-language notices cannot do this.[205]

iii) Skewed decision making

Second cognitive problem pointed out by Solove is that people lack the "expertise to adequately assess the consequences of agreeing to certain present uses or disclosures of their data", even if they would read privacy notices.[206] Although people regularly express in surveys how much they value and care about their privacy, people constantly disclose their data for very small benefits.[207] This skewed decision making has also been called "privacy paradox", where behavioral intentions are not reflected in the actual behavior.[208] Soleve sees the skewed decision making as a result of individual's cognitive capabilities and bounded rationality.[209] According

[198] Calo (n 187) 1029.
[199] Solove (n 7) 1883.
[200] Ibid.
[201] Ibid, 1885.
[202] Ibid.
[203] Ibid.
[204] Solon Barocas and Helen Nissenbaum, 'Big Data's End Run around Anonymity and Consent' in Julia Lane et al. (eds.) *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (Cambridge University Press, 2014), 58; Soleve (n 6) 1886.
[205] Barocas and Nissenbaum (n 204) 59.
[206] Solove (n 7) 1886.
[207] Ibid.
[208] Tuukka Lehtiniemi and Yki Kortesniemi, 'Can the obstacles to privacy self-management be overcome? Exploring the consent intermediary approach' [2017] Big Data & Society, 2 < https://doi.org/10.1177/2053951717721935> accessed 27 September 2021.
[209] Solove (n 7) 1887. See also Calo (n 187) 1053.

to Calo privacy notices rely on false conception of rational consumer with limitless attention.[210] Behavioral economics have shown that human rationality is bounded. In other words, people struggle to apply their knowledge, solve problems and make informed choices in complex situations.[211] Instead people often rely on simplified rules of thumb, mental models and heuristics.[212] Such mental shortcuts can lead to behavior that goes against people's self-interest.[213] For example, those possessing mental models on how a traditional computer operates, might completely misjudge how an IoT device functions.[214] In addition, the complexity of IoT can make it difficult for users to develop new and accurate mental models on how their devices function, what kind of information is being collected by their devices, and how their devices use and disclose information.[215]

Further, according to Soleve people are more willing to disclose their personal data when they feel that they are in control, even if the control is illusory.[216] People are often unaware of the nudging methods and manipulation pertaining to the design and layout of the user interfaces, and thus made believe they are in control, leaving the stakeholders free to engage in collection and other processing activities.[217] This appears to be also true in terms of IoT. As Williams, Nurse and Creese state the novelty and functionality of IoT devices can divert user's attention away from the large amounts of data they are disclosing.[218] Moreover, as Rosner and Kenneally state, IoT devices are not neutral; they are manufactured by companies who benefit from the processing of data and thus are built with a commercial logic that encourages sharing of data.[219]

iv) Problems with scale

[210] Calo (n 187) 1054.
[211] Solove (n 7) 1887; Calo (n 187) 1054.
[212] Solove (n 7) 1887.
[213] Borgesius (n 197) 7.
[214] Meredydd Williams, Jason R. C. Nurse and Sadie Creese, 'The Perfect Storm: The Privacy Paradox and the Internet-of-Things' (2016) 11th International Conference on Availability, Reliability and Security, 3 < https://doi.org/10.1109/ARES.2016.25> accessed 18 September 2021.
[215] Office of the Victorian Information Commissioner, 'Internet of Things and Privacy – Issues and Challenges' < https://ovic.vic.gov.au/privacy/internet-of-things-and-privacy-issues-and-challenges/> accessed 2 October 2021.
[216] Solove (n 7) 1887.
[217] Eletta Bietti, 'The Discourse of Control and Consent over Data in EU Data protection Law and Beyond' (2020) A Hoover Institution Essay, 1 <https://www.hoover.org/research/discourse-control-and-consent-over-data-eu-data-protection-law-and-beyond> accessed 16 September 2021; Lilian Edwards & Michael Vale, 'Slave to the Algorithm' (2017) 16 Duke Law & Technology Review 18, 33.
[218] Williams, Nurse and Creese (n 214) 3.
[219] Rosner and Kenneally, 'Clearly Opaque: Privacy Risks of the Internet of Things' (n 23) 3..

In addition to the cognitive problems, Soleve points out that privacy self-management also faces structural problems.[220] The first structural problem is the problem with scale.[221] In other words, there are too many information actors processing personal data, making it impossible for a person to control and monitor these entities. Even if all these entities would provide individuals with notice and appropriate choice whether to consent to such processing, a regular person does not have enough time or resources to manage such entities.[222] As we saw above, it would take an around 40 minutes per day to read all the relevant privacy policies an average individual faces. However, that 40 minutes does not take into account how long it would take to actually truly understand the policies. Moreover, managing the entities is difficult as the landscape of information actors working behind the scenes is constantly changing.[223] For example, the entity that collects individual's data might sell it to another entity or store it to servers managed by others.[224]

v) Aggregation effect

The second structural issue raised by Soleve is that even if people make rational choices with how they use their data, that data may be aggregated in the future in ways the person did not anticipate and reveal new information about the person in question.[225] By analyzing existing information, the new information that can be deduced is so complex and evolving so quickly that people cannot assess the harms and benefits involved.[226] This aggregation problem means that "it makes it nearly impossible to manage data".[227] Consenting to data collection, use and disclosure is something that can have future detriments and thus is something that should be assessed and decided far in advance. However, as Solove point out it is difficult to assess the harm as individuals are unable to predict what the harm could be down the road.[228] In addition, this kind of cost-benefits analysis is difficult as people prefer immediate benefits.[229] According to Borgesius people are influenced by biases such as the present bias, which suggests that

[220] See Solove (n 7) 1888.
[221] Ibid.
[222] Ibid, 1889.
[223] Daniel Susser, 'Notice After Notice-and-Consent. Why Privacy Disclosures Are Valuable Even If Consent Frameworks Aren't' (2019) 9 Journal of Information Policy 37, 45.
[224] Ibid.
[225] Solove (n 7) 1889.
[226] Ibid, 1890.
[227] Ibid.
[228] Ibid, 1891.
[229] Ibid.

"people often choose for immediate gratification and disregard future costs and disadvantages".[230]

The aggregation effect is very much applicable to IoT. As IoT continues to grow and spread into human environments, more and more information will be collected. It has been estimated by the Organization for Economic Co-operation and Development (OECD) that in 2022 an average household of four, in an OECD member country, will have around 50 connected devices.[231] When data is combined from just one IoT device or from various different IoT enabled sensors and devices, new inferences can be derived.[232] Further, data that may seem simple or insignificant at the moment of disclosure to the data subject, may reveal complex and unexpected results when combined with other sources of data. It has been described by Peppet that this kind of sensor fusion leads to a world where "everything reveals everything on the Internet of Things".[233] This "everything" may also be sensitive personal data.

In addition, aggregation can alter the identifiability of data. The WP29 has recognized that pseudonymized or even anonymized data risks being identified in IoT. [234] The large amounts of data collected by several different sensors and the fact that data is being processed automatically means that there is a limited possibility to remain anonymous in IoT. According to Peppet the reason why sensor data is particularly vulnerable to re-identification is because "sensor data capture such a rich picture of an individual, with so many related activities, that each individual in a sensor-based dataset is reasonably unique".[235]

4.2.2 Information asymmetries

The problems presented above in section 4.2.1 are all examples of information asymmetries. Information asymmetry means that there are several knowledge gaps between data subjects and controllers; in other words, individuals do not know what the companies do with their data, thus undermining the basic notion of informed consent.[236] It should be noted that the companies

[230] Borgesius (n 197) 7.
[231] OECD, 'Building Blocks for Smart Networks' (2013) 215 OECD Digital Economy Papers, 10 < https://read.oecd-ilibrary.org/science-and-technology/building-blocks-for-smart-networks_5k4dkhvnzv35-en#page1> accessed 27 September 2021.
[232] WP29, 'Opinion 8/2014 on the Recent Developments on the Internet of Things' (n 35) 7-8.
[233] Peppet (n 47) 116.
[234] Article 29 Data Protection Working Party, 'Opinion 8/2014 on the Recent Developments on the Internet of Things' (n 35) 11.
[235] Peppet (n 47) 129.
[236] Borgesius (n 197) 5.

processing the data do not face the same problems. As stated by Hoofnagle and Whittington "despite lengthy and growing terms of service and privacy, consumers enter into trade with online firms with practically no information meaningful enough to provide the consumer with either ex ante or ex post bargaining power. In contrast, the firm is aware of its cost structure, technically savvy, often motivated by high-powered incentives of stock values, and adept at structuring the deal so that more financially valuable assets are produced from consumers than consumers would prefer".[237]

The GDPR has tried to mitigate this problem by imposing transparency requirements to data controllers.[238] However, according to Borgesius the information asymmetry is very hard to solve as transaction costs arise for individuals.[239] As we saw reading privacy policies takes a lot of time. Furthermore, it is questionable can the data subjects understand the privacy policies as they are often long, ambiguous and difficult to read. Because data subjects do not read the privacy policies, or even access them, their understanding of the significance of the disclosure will most likely be very low.[240]

Van de Waerdt has categorized the instances where information asymmetries arise into two categories: those which arise from personal data collection, and those arising from personal data analysis.[241] The first instance where information asymmetries typically arise is when companies collect personal data through methods and quantities that an average person cannot simply comprehend, manage and monitor.[242] As the WP29 states in regard to IoT "interaction between objects, between objects and individuals' devices, between individuals and other objects, and between objects and back-end systems will result in the generation of data flows that can hardly be managed with the classical tools used to ensure the adequate protection of the data subjects' interests and rights".[243] Furthermore, communication between devices and

[237] Chris Hoofnagle and Jan Whittington, 'Free: Accounting for the Costs of the Internet's Most Popular Price' (2014) 61 UCLA Law Review 606, 640.
[238] See Peter van de Waerdt, 'Information asymmetries: recognizing the limits of the GDPR on the data-driven market' [2020] Computer Law & Security Review <https://pure.rug.nl/ws/portalfiles/portal/128134033/1_s2.0_S0267364920300418_main.pdf> accessed 27 September 2021.
[239] Borgesius (n 197) 6.
[240] Masooda Bashir et al., 'Online privacy and Informed Consent: The Dilemma of Information Asymmetry' (2016) 52 Proceedings of the Association for Information Science and Technology, 2-3 < https://asistdl.onlinelibrary.wiley.com/doi/epdf/10.1002/pra2.2015.145052010043> accessed 27 September 2021.
[241] See van de Waerdt (n 238).
[242] Ibid, 3.
[243] WP29, 'Opinion 8/2014 on the Recent Developments on the Internet of Things' (n 35) 6.

transmission of data can be triggered automatically and by default, without human involvement, and without the user of the IoT device knowing about it.[244] If the user is not aware of such automatic communication, it is very difficult for him or her to control the data flows.[245] In addition, it will be even harder to control the subsequent use of that data, and thereby prevent function creep.[246] Moreover, IoT is very fragmented. There are multiple stakeholders involved in IoT. These include for example device manufacturers, social platforms, application developers and other third parties.[247] Taken into account all the IoT stakeholders and the complicated tangle of contracts and subcontracts between them, it is no wonder the flows of personal data are almost impossible for an average person to manage.

The second instance where information asymmetries can arise is personal data analysis: "having previously collected a set of personal data from the consumer, data analysis is used to expand and enrich the dataset without requiring further involvement or knowledge of the data subject".[248] As discussed above, seemingly meaningless information generated by IoT devices and sensors can be combined and analyzed resulting in information that has value to the data controller. This is especially the case when data streams are combined into profiles.[249] Such profiles can reveal information about the device user's living patterns, habits and preferences and can thus constitute sensitive personal data. Although it is unclear to what extent and to what level of detail individuals are being profiled for example for targeted advertising, the fact that its extent is unknown functions as an indication of the information asymmetries present on the data-driven market.[250]

4.2.3 Problems with freely given consent

Another line of criticism has questioned whether consent can be considered freely given. Freely given consent implies that the data subject is able to exercise real choice and control regarding

[244] Ibid.
[245] Ibid.
[246] Ibid.
[247] See Ibid, 12.
[248] van de Waerdt (n 238) 6.
[249] Bibi van den Berg, 'Mind the Air Gap. Preventing Privacy Issues in Robotics' in Serge Gutwirth, Ronald Leenes and Paul De Hert (eds.) *Data Protection on the Move. Current Developments in ICT and Privacy/Data Protection* (Springer, 2016), 9.
[250] van de Waerdt (n 238) 6.

the processing of his or her data.[251] However, many scholars have shown that whenever data subjects are confronted with consent request, they often lack a real choice.

vi) No room for negotiations

First of all, according to Schermer, Custers and van der Hof people lack meaningful choice in online environments as many services function with a principle of take-it-or-leave-it.[252] The same appears also to be true with IoT devices, which according to Rosner and Kenneally operate on "fire and forget it" basis.[253] When confronted with a consent request people often have a choice to accept the terms of the privacy notice or not to use the product or service.[254] The controllers do not offer any room for negotiation.[255] According to Schermer, Custers and van der Hof the controllers lack an incentive to offer such room as their business model is based on personal data collection.[256] However, if accepting the terms of a privacy notice is a precondition for using an IoT device, it is questionable can such consent be considered as freely given as the data subject was not able to exercise real choice. As Susser point out opting out is not often a realistic option as the cost of opting out is too high for the data subject.[257]

As more and more "regular" devices such as watches and TVs become smart, it can become problematic if the device cannot be used without consenting to also personal data processing. As time goes on, people might be unable to buy products that are not smart.[258] This can lead to an "erosion of choice".[259] Furthermore, according to WP29 "the possibility to renounce certain services or features of an IoT device is more a theoretical concept than a real alternative".[260] In other words, it might not be possible to disable the "connected" features of an IoT device and use it as a "regular" device where no personal data is collected. In addition, as smart devices in people's homes become more common, so will smart devices in shared spaces such as cities

[251] EDPB, 'Guidelines 05/2020 on consent under Regulation 2016/679' (n 21) 7.
[252] Schermer, Custers & van der Hof (n 173) 11-12.
[253] Rosner and Kenneally, 'Privacy and the Internet of Things. Emerging Frameworks for Policy and Design' (n 25) 10.
[254] Susser (n 223) 43.
[255] Schermer, Custers & van der Hof (n 173) 11-12.
[256] Ibid, 12.
[257] Susser (n 223) 43.
[258] Rosner and Kenneally, 'Privacy and the Internet of Things. Emerging Frameworks for Policy and Design' (n 25) 10.
[259] Office of the Privacy Commissioner of Canada, 'The Internet of Things. An Introduction to privacy issues with a focus on the retail and home environments' (February 2016) < https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/iot_201602/> accessed 30 September 2021.
[260] WP29, 'Opinion 8/2014 on the Recent Developments on the Internet of Things' (n 35) 7.

and retail stores.[261] For example retail stores may place sensors inside and outside their stores to track the location of their customers to derive information about consumer behavior and travel.[262] Thus, people may have to choose between entering a physical area and consenting to a processing of their personal data or not entering at all.

Moreover, in order for an IoT device holder to access their data or to even use the functionalities of their device, they will often have to install a third-party application.[263] Installing the application also means providing the app developer access to the data collected by the device.[264] Although such an application is usually installed on an opt-in basis[265], not installing the application (and thus not providing access to data to the app developer) will most likely mean that the device owner will not be able to use the device as the app works as a primary interface through which the device can be managed.

vii) No alternatives

Koops has pointed out that not consenting to data processing is not an option as there are no privacy respecting alternatives on the market.[266] The market has been taken over by tech giants such as Apple, Google and Amazon, and their partners. This means that if the device manufacturer's privacy policy does not satisfy the device owner, there is a possibility that there is no alternative device yet on the market he or she could switch to.

Article 20 of the GDPR provides a right to data portability. This means that the data subject has the right to receive their data from the controller and transmit that data to another controller making switching services easier. However, due to lack of standardization and interoperability in IoT, it could be that such option to switch services does not exist in practice. As WP29 states "the Internet of Things is sometimes seen as an "Internet of Things" in which every manufacturer has defined its own set of interferences and data format".[267] In other words, data is hosted in isolated silos making transferring of data from one device to another almost

[261] See for example Lilian Edwards, 'Privacy, security and data protection in smart cities: a critical EU law perspective' (2016) 2 European Data Protection Law Review <http://dx.doi.org/10.2139/ssrn.2711290> accessed 30 September 2021.
[262] Office of the Privacy Commissioner of Canada (n 259).
[263] WP29, 'Opinion 8/2014 on the Recent Developments on the Internet of Things' (n 35) 12.
[264] Ibid.
[265] Ibid.
[266] Koops (n 22) 251.
[267] WP29, 'Opinion 8/2014 on the Recent Developments on the Internet of Things' (n 35) 13.

impossible.[268] WP29 has noted that device users do not often have an access to the raw data that are registered by their device.[269] Getting access to such raw data would mean that the user would be able to transfer their data to another data controller.[270] It thus seems that if device owners do not accept data controllers' privacy policies, "these persons have in practice no other possibility than to stop using their devices as most data controllers do not provide such functionality [access to raw data] and provide access only to a degraded version of the stored raw data".[271]

viii) Dependency

Related to the above points, it has been noted that people are becoming increasingly dependent on the usage of digital platforms and smart devices.[272] For example Matzner et al. points out that smartphones have become so common that people who refuse to use them might face social costs such as "less contacts with friends, missing carrier opportunities, more complicated dating, being considered inefficient as a colleague, being considered suspicious at border controls, and many more".[273]

Moreover, Martzner et al. argue that through the use of online services, the users are able to obtain social gratifications.[274] It has been noted by the WP29 that individuals are even more likely to use smart devices when they can share the data collected by their device with others on social platforms.[275] According Martzner et al. sharing information online functions as relationship-building and leads to social acceptance.[276] Thus, protecting one's privacy becomes a balancing act between data protection and social gratification. However, as Martzner et al. note this balancing act assumes that users always have a choice whether to use the service or not.[277] This is not always the case as in today's world people will have to engage with certain services and products to achieve certain things e.g. keeping in touch with people, managing

[268] Ibid. See also European Commission, 'A Digital Agenda for Europe' COM(2010)245 final, 5 according to which the lack of interoperability is one of the significant obstacles to a thriving digital economy.
[269] WP29, 'Opinion 8/2014 on the Recent Developments on the Internet of Things' (n 35) 19.
[270] Ibid, 20.
[271] Ibid [emphasis added].
[272] Bergemann (n 81) 6; Tobias Matzner et al., 'Do-It-Yourself Data protection- Empowerment or Burden? in Serge Gutwirth, Ronald Leenes and Paul De Hert (eds.), *Data Protection on the Move* (Springer, 2016), 297.
[273] Matzner et al. (n 272) 297.
[274] Ibid, 287-288.
[275] WP29, 'Opinion 8/2014 on the Recent Developments on the Internet of Things' (n 35) 12.
[276] Matzner et al. (n 272) 288
[277] Ibid.

their finances etc.[278] As Nissenbaum states: "while it may seem that individuals freely choose to pay the informational price, the price of not engaging socially, commercially, and financially may in fact be exacting enough to call into question how freely these choices are made."[279]

4.2.4 Power asymmetries

As we have seen above in section 4.2.3, it seems that there are some significant problems with freely given consent due to power asymmetries between data subjects and controllers. One of the cited reasons for this imbalance is that the digital market is characterized by the presence of tech "monopolies".[280] In practice, this means that dominant companies are able to exercise their power by imposing one-sidedly their practices on individuals.[281] This calls into question the validity of freely given consent as the data subjects seldom are able to exercise real choice. For example, as Schrems argued in his complaint to the Irish Data Protection Commissioner "facebook.com has become a standard form of communication and that consent to a monopoly is hardly "free"".[282] For dominant companies consent thus seems to be just a formality; something that is asked to ensure legal compliance.[283]

According to Clifford, Graef and Valcke this imbalance of power has been enabled by the existence of economic characteristics such as network effects.[284] Network effect mean that the more people use a product or a service the more valuable it will become often resulting to a winner-takes-it-all situation.[285] Network effect thus leads to market concentration, where users have no choice or a very limited choice which product or service to use. Such network effect is

[278] Ibid.
[279] Helen Nissenbaum, 'A Contextual Approach to Privacy Online' (2011) 140(4) Daedalus 32, 35.
[280] Damian Clifford, Inge Graef & Peggy Valcke, 'Pre-formulated Declarations of Data Subject Consent- Citizen-Consumer Empowerment and the Alignment of Data, Consumer and Competition Law protection' (2019) 20 German Law Journal 679, 713 <doi:10.1017/glj.2019.56> accessed 3 October 2021; Bergemann (n 81) 6.
[281] Clifford, Graef & Valcke (n 280) 713.
[282] Europe-v-facabook.org, 'Response to "audit" by the Irish Office of the Data Protection Commissioner on "Facebook Ireland Ltd.' (4 December 2012), 42 <http://www.europe-v-facebook.org/report.pdf> accessed 3 October 2021.
[283] Marco Botta & Klaus Wiedemann, 'The Interaction of EU Competition, Consumer, and Data Protection Kaw in the Digital Economy: The Regulatory Dilemma in the Facebook Odyssey' (2019) 64 The Untitrust Bulletin 428, 433 <https://doi.org/10.1177/0003603X19863590> accessed 3 October 2021.
[284] Clifford, Graef & Valcke (n 280) 713.
[285] Olga Batura, Nicolai van Gorp and Pierre Larouche, 'Online Platforms and the EU Digital Single Market' (2015) A Response to the Call for Evidence by the House of Lord's Internal Market Sub-Committee, 4-5 < https://ec.europa.eu/information_society/newsroom/image/document/2016-7/nikolai_van_gorp_-_response_e-conomics_to_the_uk_house_of_lords_call_for_evidence_14020.pdf > accessed 30 September 2021.

especially common with platforms.[286] As consumer IoT platforms are characterized by interoperability, the effect of competing platforms is diminished.[287] For example, FitBit, which is a wearable fitness tracker, is only usable in the FitBit platform. Market concentration and dominance leads to a situation where there is no incentive for the platforms to negotiate with their users. According to Botta and Wiedemann if the market would be competitive and "well-functioning", platforms would have to negotiate with users and offer options for different privacy preferences.[288] However, it is very difficult for competitors to enter the market due to the network effects. Further, as the dominant platforms already hold very large pools of data, it functions as "the single biggest barrier to entry in the digital economy".[289]

4.2.5 Notice and choice ill-fitting for IoT

The notice and choice model has also been criticized as completely ill-fitting for IoT. The critique mainly addresses the design of IoT devices. First of all, IoT devices are often small and lack screens and input mechanisms such as keyboards or touch screen.[290] This poses practical challenges for the notice and consent model as the devices do not facilitate consent. For example, a smart watch has a tiny screen, but a smart water meter does not have any input or output capabilities. This means that most IoT devices do not have any means to display privacy notices to their users.[291] As a result, users will have to be informed through other channels such as through an associated mobile application, manufacturer's website or a paper version in the device's box.[292] According to Peppet in most cases manufacturers prefer to display privacy related information in their website.[293] In other words, this model assumes that once an individual buys an IoT device and brings it home, he or she will also go online through his or her smart phone or computer to read the privacy policy. However, according to a study conducted by Peppet privacy policies are hard to find as most IoT devices he studied did not

[286] See Ibid.
[287] Arturo Basaure, Alexandr Vesselkov and Juuso Töyli, ' Internet of things (IoT) platform competition: Consumer switching versus provider multihoming' (2020) 90-91 Technovation, 3 < https://doi.org/10.1016/j.technovation.2019.102101> accessed 30 September 2021.
[288] Botta & Wiedemann (n 283) 432.
[289] Jason Furman et al., 'Unlocking digital competition' (2019) Report of the Digital Competition Expert Panel, 33 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf> accessed 30 September 2021.
[290] Peppet (n 47) 139-140; Rosner & Kenneally, 'Privacy and the Internet of Things. Emerging Frameworks for Policy and Design' (n 25) 8.
[291] Peppet (n 47) 140.
[292] Ibid.
[293] Ibid.

include even a mention of the existence of a privacy policy nor directed the user to manufacturer's website.[294] Moreover, if the user would be able to find the privacy policy of his or her device, research has shown that IoT privacy policies fail to provide appropriate information to consumers. According to a report by 2016 GPEN Sweep, a study by 25 data protection regulators around the world, 59% of IoT devices involved in the study failed to adequately explain to the customers how their personal information was collected, used and disclosed.[295] Furthermore, 72% failed to explain to consumers how they could delete their information off the device.[296] Consent will not be valid, if it is not specific and informed.

The lack of screens also means that IoT devices do not provide a mechanism to obtain individual's consent.[297] Furthermore, in practice most devices are plug and play, meaning that users will be able to start using the device as soon as taken out of its box.[298] This certainly raises questions about whether just a mere use of a device constitutes a clear affirmative action and thus a valid consent. Because of this plug and play model, users are not required to manually configure settings before use.[299] However, the default settings tend not to provide optimal privacy and rely on the unawareness of individuals to support data collection.[300] Although some devices provide an option to evaluate and customize their settings, most people do not deviate from the default settings.[301]

Obtaining consent through classical mechanisms can also be hard due to the fact that IoT devices may process data that does not belong to the user or subscriber of the IoT device.[302] For example, a smart car may collect data from its passengers.[303] Such passengers will most likely have no idea that their data is being processed, as information may only be provided to the

[294] Ibid, 140-142.
[295] Information Commissioner's Office (ICO), '2016 GPEN Sweep – Internet of Things' (2016) < https://ico.org.uk/media/about-the-ico/disclosure-log/1625142/irq0648379-attachment.pdf> accessed 30.9.2021. See also Wiredgov, 'Privacy regulators study finds Internet of Things shortfalls' (23 September 2016) <https://www.wired-gov.net/wg/news.nsf/articles/Privacy+regulators+study+finds+Internet+of+Things+shortfalls+23092016092000 > accessed 30 September 2021.
[296] 2016 GPEN Sweep (n 295).
[297] WP29, 'Opinion 8/2014 on the Recent Developments on the Internet of Things' (n 35) 7.
[298] Office of the Victorian Information Commissioner (n 215).
[299] Ibid.
[300] Williams, Nurse and Creese (n 214) 4.
[301] Wendy E. Mackay, 'Triggers and Barriers to Customizing Software' (1991) Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 153 < https://www.lri.fr/~mackay/pdffiles/CHI91.Triggers.pdf> accessed 2 October 2021.
[302] WP29, 'Opinion 8/2014 on the Recent Developments on the Internet of Things' (n 35) 13.
[303] See EDPB, 'Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications' (9 March 2021).

owner of the car.[304] Smart devices are also becoming increasingly common in shared spaces. For example, cities are installing information infrastructures such as traffic control sensors, smart lighting, smart transportation etc.[305] This raises questions how people will be informed about the purposes of the processing of their personal data in such public spaces? Further, in such a situation how can an individual give a valid consent? It is clear that IoT in public places moves individuals beyond the "realm of control".[306]

A second issue with IoT is that it has been explicitly designed to be ubiquitous, unobtrusive and invisible.[307] As Weiser stated already in 1991, technologies "weave themselves into the fabric of everyday life until they are indistinguishable from it".[308] In practice, this means that individuals may not even be aware that they are surrounded by sensors that are processing their data. Such lack of information constitutes a significant problem to valid consent. WP29 has raised the issue with wearable devices such as smart watches. As it notes "most observers may not distinguish a normal watch from a connected one, when the latter may yet embed cameras, microphones and motion sensors that can record and transfer data without the individuals being aware of, and even less consenting to such processing".[309] This same problem applies also to shared spaces. While an individual may be able to decide what smart devices they place in their home, this control does not extend to shared places where smart devices are used by others.[310] That is to say, in shared spaces individuals will be exposed to IoT devices of other people such as smart watches, smart glasses and smart phones. As Leta Jones argues the notice and choice model is not available in the "internet of other people's things".[311]

4.2.6 Summary of the problems

As can be seen from the discussion above, the consent-based model has come under sustained criticism. It has been argued that in digitalized world consent does not offer individuals real

[304] Ibid, 13-14.
[305] Meg Leta Jones, 'Privacy Without Screens & the Internet of Other People's Things' [2015] Idaho Law Review 639, 644-645, 647. See also Edwards, 'Privacy, security and data protection in smart cities: a critical EU law perspective' (n 261).
[306] Leta Jones (n 305) 647.
[307] Edwards, 'Privacy, security and data protection in smart cities: a critical EU law perspective' (n 261) 17.
[308] Mark Weiser, 'The Computer for the 21st Century' (1991) Scientific American, [no pagination] < https://www.ics.uci.edu/~corps/phaseii/Weiser-Computer21stCentury-SciAm.pdf> accessed 1 October 2021.
[309] WP29, 'Opinion 8/2014 on the Recent Developments on the Internet of Things' (n 35) 7.
[310] Leta Jones (n 305) 647.
[311] Ibid.

control, but rather an "illusion" of it.[312] The critics have pointed out that in practice consent is neither freely given nor informed. The problems are summarized below.

i) *People do not read privacy notices*: most people do not read privacy notices due to information overload and consent transaction overload.

ii) *People do not understand privacy notices*: privacy notices are too long and difficult to understand.

iii) *Skewed decision making:* human rationality is bounded, and individuals' decision making is influenced by mental models and heuristics. Mental models can be inaccurate due to being based on false information or misplaced assumptions.

iv) *Problems with scale*: There are too many entities providing privacy notices and consent requests, which makes privacy management difficult due to lack of time and resources.

v) *Aggregation effect*: data that might have seemed insignificant may be combined with other data in the future revealing new and possibly sensitive information.

vi) *No room for negotiations*: When confronted with a consent request people often have a choice to accept the terms of the privacy notice or not to engage with the device.

vii) *No alternatives*: There are no privacy respecting alternatives on the market as the market is dominated by tech giants. The lack of standardization and interoperability in IoT makes it hard to switch service provider and/or device.

viii) *Dependency*: Smart devices are becoming increasingly common, and users are becoming more and more dependent on such devices.

The above-mentioned problems are examples of information and power asymmetries between data subjects and controllers. Such asymmetries invalidate consent; the value of user consent diminishes if users are not adequately informed, or they perceive to have no other choice but to accept the terms and conditions of a given product.

[312] Edwards & Vale (n 217) 33. See also Iskander Sanches-Rola et al, 'Can I Opt Out Yet?: GDPR and the Global Illusion of Cookie Control' (2019) The 2019 ACM Asia Conference on Computer and Communication <https://doi.org/10.1145/3321705.3329806 > accessed 3 October 2021; Lilian Edwards, 'Privacy, Law, Code and Social Networking Sites' in Ian Brown (ed.) *Research Handbook on Governance of the Internet* (Edward Elgar Publishing, 2013) 332. In addition, the EDPB has stated that "If obtained in full compliance with the GDPR, consent is a tool that gives data subjects control over whether or not personal data concerning them will be processed. If not, the data subject's control becomes illusory and consent will be an invalid basis for processing, rendering the processing activity unlawful" in 'Guidelines 05/2020 on consent under Regulation 2016/679' (n 21) 5.

Moreover, the rise of IoT brings with itself a unique set of problems to the consent-based model. The design of IoT devices ads to the challenges presented above. IoT devices often lack screens and input mechanisms, and so users cannot easily access privacy notices, change default settings or provide consent. Most devices do not include privacy policies in their packaging, but rather privacy policies are displayed in manufacturer's website or related mobile application. These practical challenges with notice and consent get even worse in shared spaces such as smart cities. The ubiquitous and invisible nature of IoT also brings with itself issues as individuals may be completely unaware that they are surrounded by sensors collecting data about them. Data processing does not always require human intervention as communication between objects can be triggered automatically and by default. Moreover, the data collected might not always belong to the user or subscriber of the device. In other words, it is hard to control whose data is being collected by IoT devices and to provide transparency. It might also not be possible to use IoT devices in a mode where data collection is disabled. The combination of lack of screens, the fact that people do not read or understand privacy notices and the ubiquitous nature of IoT means that individuals are often not aware what kind of data is collected about them and how that data will be used by the IoT stakeholders in the future. Furthermore, sensor data permits unexpected interferences to be drawn about individuals' habits and preferences making it hard for individuals to manage data.

5. Alternative ways forward to consent based model

This thesis has shown that the consent-based model is failing to provide adequate protection to data subjects in digital environments. As IoT continues to evolve and become more and more common, intertwining itself to our everyday lives, the problems with consent will arguably exacerbate. Those factors which are contributing to the current "privacy paradox", such as skewed decision making, aggregation effect and scale, will only be aggravated with IoT.[313] However, if privacy self-management is not the answer, then what is?

The most obvious alternative would be to disregard consent in digital environments. However, such approach appears too radical as consent, despite its problems, seems to function as a last line of defense against the loss of control of personal data. As Solove states "for all its flaws, privacy self-management should not be abandoned. Providing people with notice, access, and the ability to control their data is key to facilitating some autonomy in a world where decisions are increasingly being made about them with the use of personal data, automated processes, and clandestine rationales, and where people have minimal abilities to do anything about such decisions".[314] This thesis agrees. Furthermore, it is hard to see that consent could be completely set aside considering its "fundamental" role given by the Charter. The same applies to the notice and consent paradigm as Article 8 of the Charter expressly states that personal data "must be processed fairly for specified purposes and on the basis of consent of the person concerned or some other legitimate basis laid down by law". Moreover, it has been argued that the absence of consent would make privacy framework too rigid and paternalistic.[315] In light of this, the following two alternatives are discussed as the best ways forward.

5.1 Improving consent

What is clear is that most of the very critics of consent are not ready to revoke consent entirely, but rather to improve and complement it. Some scholars argue that there should be more substantive controls in place to what kind of processing individuals can consent to. For example, Solove proposes that the law should take a stronger stance about substance: "more substantive rules about data collection, use, and disclosure could consist of hard boundaries that block

[313] See Williams, Nurse and Creese (n 214).
[314] Solove (n 7) 1899.
[315] Omer Tene and Jules Polonetsky, 'To Track or "Do Not Track": Advancing Transparency and individual Control in Online Behaviorak Advertising' (2012) 13(1) Minnesota Journal of Law, Science & Technology, 42 < http://dx.doi.org/10.2139/ssrn.1920505> accessed 4 October 2021.

particularly troublesome practices as well as softer default rules that can be bargained around".[316] However, one could argue that the European data protection framework already contains such substantive rules making Solove's argument more relevant for the United States. For example, the GDPR has a stricter regime for special categories of data. Because of the sensitive nature of special categories of data and the privacy risks involved with using such data, Borgesius has proposed that the use of health related data should be completely prohibited in behavioral targeting regardless whether the data subject has given explicit consent.[317] Moreover, Borgesius sees that privacy self-management should learn from consumer law, which contains not only rules which empower individuals but also protection rules.[318] For example, food labeling rules require companies to disclose comprehensive information to consumers about the content of food products empowering them to make decisions, while other consumer law rules protect consumers by banning for example certain food additives and placing minimum safety standards for products.[319]

These kinds of rules that protect people by limiting their autonomy are examples of paternalism. Paternalism is seen by some as the preferred solution to the problems with consent. As acknowledges by Solove "consent performs an enormous amount of work. Activities that would otherwise be illegitimate are made legitimate by consent".[320] As seen above, this means in most instances that individuals do not engage in privacy self-management and end-up up giving over their personal data for very small benefits and agreeing to processing operations that might cause them harm in the long run. In light of this, some scholars have considered that law should regulate privacy in a more paternalistic manner. According to Allen privacy is a "foundational human good" that must in certain instances be mandated.[321] Because of this foundational nature of privacy, "privacy cannot be left solely to the realm of waiver-eligible free choice".[322] In other words, law must override individual's choice on some occasions. Arguably the GDPR already includes some paternalistic provisions such as principles of fairness and purpose limitation as individuals cannot give away the protection offered by those principles.[323] Moreover, the GDPR's stringent conditions for valid consent could be seen as a form of paternalism. However,

[316] Solove (n 7) 1903.
[317] Borgesius (n 197) 9.
[318] Ibid.
[319] Ibid.
[320] Solove (n 7) 1894.
[321] Anita Allen, *Unpopular Privacy: What Must We Hide?* (Oxford Scholarship, 2011) 4.
[322] Ibid.
[323] See for more discussion Claudia Quelle, 'Not just User Control in the General Data protection Regulation' in A. Lehmann et al. (eds.), *Privacy and Identity Management – Facing up to Next Steps* (Springer, 2017) 140-163.

as we have seen even the "stringent" requirements do not necessary lead to people making better decisions regarding their data. Although Solove proposes more substantive rules about data collection, he also (somewhat contradictory) believes that paternalistic regulation should be avoided as it takes away individuals' autonomy and denies freedom to make choices.[324] Convincedly he argues that the correct choices about privacy are not always clear.[325] As an example Solove uses a person suffering from an eating disorder who would like to share her experience online as a way of empowering herself. He argues that "if the law were to put restrictions on her disclosure, then it would be limiting her freedom and autonomy — ironically in the name of preserving her freedom and autonomy".[326]

Other scholars are focused on improving informedness of consent. According to van Alsenoy et al. despite the problems related to privacy notices, notices should not be abandoned as notices hold the "potential to fulfill an array of other functions, including the promotion of fairness, the reduction of knowledge asymmetries and the increase of accountability of data controller".[327] Thus, many scholars seek to improve privacy notices. In order to achieve this, scholars are proposing innovative new ways to present privacy notices. These include shortening the notices or otherwise making the notices easier to understand, layering notices and visualizing notices with images and icons.[328] However, as Calo states it does not matter how short or visual notices are, if no one reads them.[329] Therefore, Calo proposes the use of visceral notices.[330] Rather than using traditional long text formats, visceral notices attempt to convey awareness of data collection through design, without conveying information with text or symbols.[331] An example of visceral notices is an interactive avatar that speaks or moves while the user moves on the screen.[332] By building the notice as part of the experience, would mean that users are not required to leave the fun and functionality of the service or required to click anything.[333]

[324] Solove (n 7) 1894
[325] Ibid, 1895.
[326] Ibid, 1896.
[327] Brendan Van Alsenoy, Eleni Kosta & Jos Dumortier, 'Privacy notices versus informational self-determination: Minding the gap' (2014) 28 International Review of Law, Computers &Technology 185, 192.
[328] Bergemann (n 81) 8.
[329] Calo (n 187) 1056.
[330] See Ibid.
[331] Ibid, 1044.
[332] Shara Monteleone, 'Addressing the 'Failure' or Informed Consent in Online Data Protection: Learning the Lessons from Behavior-aware Regulation' (2015) 43(1) Syracuse Journal of International Law and Commerce 69, 111.
[333] Calo (n 187) 1057-1058.

Visceral notices could be seen as a form of nudges. A nudge is "any aspect of the choice architecture that alters people's behavior in a predictable way without forbidding any options or significantly changing their economic incentives".[334] In the last years the idea of "nudging" people into better privacy decisions has gained popularity.[335] The idea is to design systems so that they guide and influence individuals' choices encouraging privacy protective behavior.[336] Although meant to empower individuals, nudges are also a form of soft paternalism.[337] However, according to Acquisti such system would not take away individuals' freedom, but rather offer them option of more informed choices.[338]

With nudges comes also some ethical concerns. Is it right that individuals' behavior is directed in such a way? However, as Acquisti et al. argue every design choice, whether intentional or not, will affect users' behavior.[339] Moreover, design choices are already influencing the way we interact with systems. Most of the time individuals are completely unaware of the nudging methods pertaining to the design and layout of the user interfaces, leaving the companies free to engage in collection and other processing activities. However, taken into account how nudges may affect user's choice, it would be important that nudges are subject to an oversight mechanism. Furthermore, Calo acknowledges that one possible drawback about visceral notices is that when compared to written text they contain "less actionable information".[340] Thus, the problem with these proposed models of notices, whether simplified or visceral, is that the transparency paradox remains. Making the notices "simpler" conflicts with the notion of informed consent where people are fully aware about the consequences of giving up data.

According to Susser the bar of informed consent is extremely high.[341] To resolve the transparency paradox presented above, Susser proposes that notice and consent should be decoupled.[342] This would allow to take the burden off notice. Susser persuasively states that

---

[334] Richard H. Thaler and Cass R. Sunstein, *Nudge: Improving Decisions about Health, Wealth and Happiness* (Yale University Press, 2008) 6.
[335] Bergemann (n 81) 8.
[336] See Alessandro Acquisti, 'Nudging privacy: The behavioral economics of personal information' [2009] IEEE Security & Privacy 72, 74.
[337] Ibid.
[338] Ibid.
[339] Alessandro Acquisti, 'Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online' (2017) 50(3) ACM Computing Surveys 1, 27 < https://www.ftc.gov/system/files/documents/public_comments/2017/11/00031-141888.pdf> accessed 4 October 2021.
[340] Calo (n 187) 1062.
[341] Susser (n 223) 48.
[342] Ibid, 47-51.

"while it's true, then, that privacy disclosures can't facilitate the level of understanding required for informed consent, the level of understanding they *can* facilitate is still valuable".[343] In some instances a lesser degree of understanding could be enough as the exhaustive privacy policies are not helping to achieve truly informed consent.[344] Thus, if informed consent is no longer a requirement, new designs could be developed such as visceral forms of notice. Another rather compelling design option proposed by Ciocchetti is a privacy label on the model of food nutrition labels.[345]

By seeking new and better ways to convey information to individuals, this approach aims to find a way to solve the information asymmetries present between data subjects and controllers. This thesis believes that improving the informedness of consent could be done by lowering the bar for informed consent as suggested by Susser. This thesis especially believes that nutrition labels for privacy would be a good idea. To begin, Europeans are accustomed to information being presented in such a way, as EU requires majority of packaged food to bear nutrition labels.[346] Secondly, such notices would allow companies to focus on the content of their privacy notices as well as to the design. It also seems that privacy labels could become a new standard as Apple has required apps to add privacy nutrition labels since the end of 2020.[347] Such labels will present the user with information about what data the app can access and what data the app will collect such as location data, browsing history, contact info etc.[348] Finally, as has been discussed in this thesis, there are some unique problems when it comes to smart devices and privacy notices. As Peppet states "sensor-device firms seem stuck in a notice paradigm designed for websites rather than connected consumer goods".[349] Instead of presenting privacy policies

[343] Ibid, 57 [emphasis included in the original text].
[344] Ibid, 49.
[345] See Corey A. Ciocchetti, 'The Future of Privacy Policies: A Privacy Nutrition Label Filled with Fair Information Practices' (2008) 26(1) The John Marshall Journal of Information Technology & Privacy Law 1.
[346] See Regulation (EU) No 1169/2011 of the European Parliament and of the Council of 25 October 2011 on the provision of food information to consumers, amending Regulations (EC) No 1924/2006 and (EC) No 1925/2006 of the European Parliament and of the Council, and repealing Commission Directive 87/250/EEC, Council Directive 90/496/EEC, Commission Directive 1999/10/EC, Directive 2000/13/EC of the European Parliament and of the Council, Commission Directives 2002/67/EC and 2008/5/EC and Commission Regulation (EC) No 608/2004 [2011] OJ L 304.
[347] Ian Carlos Campbell, 'Apple will require apps to add privacy 'nutrition labels' starting December 8th' (The Verge, 5 November 2020) <https://www.theverge.com/2020/11/5/21551926/apple-privacy-developers-nutrition-labels-app-store-ios-14> accessed 4 October 2021; Melanie Weir, 'What are Apple's Privacy Nutrition Labels? Here's what you need to know about the new App Store feature that prioritizes user privacy' (Business Insider, 20 January 2021) <https://www.businessinsider.com/what-are-apple-privacy-nutrition-labels?r=US&IR=T> accessed 4 October 2021.
[348] Campbell (n 347)
[349] Peppet (n 47) 147.

in their websites, device manufacturers could include a privacy nutrition label in the box of the IoT device.

However, improving the informedness of consent fails to account for the reality of screenless technologies. Nudges and visceral notices, for example, are designed for traditional screens. Although such nudges could be provided through a device application, it is questionable can an app be downloaded for everything (and more importantly is it meaningful). If we consider that an average household soon has 50 IoT devices, managing such a scale of apps could prove to be difficult. Furthermore, improving informedness of consent does not solve the issue with "internet of other people's things". Moreover, the discussion centering the informedness of consent only tries to solve the issue with informed consent. It does not explain how to reconcile the problems with freely given consent.

5.2 Shifting the focus away from consent

The emphasis on control and consent puts the responsibility on individuals as the ultimate decision makers. However, this places a significant burden on data subjects.[350] Therefore, some scholars have proposed that in the age of big data the emphasis placed on consent should be reduced.[351] This could be done by shifting the burden on companies.[352] According to Mayer-Schönberger & Cukier most of data's value lies in its secondary uses; therefore more emphasis should be placed on holding data controllers accountable for what they do with the data.[353] In this model, companies would have to assess the secondary use of data based on the impact it would cause to the data subject.[354] Due to the information asymmetries companies know much more about the purposes of the processing of a particular set of data and how they intend to use it. As Mayer-Schönberger & Cukier argue it makes sense that companies bear the burden of responsibility as they are also the ones to benefit from the secondary uses of individuals' data.[355] Moreover, Tene & Polonetsky see that by shifting the burden from individuals to companies, online privacy will become part of their corporate governance.[356] According to them this would

[350] Van Alsenoy, Kosta & Dumortier (n 327) 190.
[351] Bergemann (n 81) 6.
[352] See Tene and Polonetsky (n 315) 48; Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data. A Revolution That Will Transform How We Live, Work and Think* (Houghton Mifflin Harcourt, 2013) 173-175.
[353] Mayer-Schönberger & Cukier (n 52) 173.
[354] Ibid.
[355] Ibid, 174..
[356] Tene & Polonetsky (n 315) 49.

make companies integrate privacy into products and business processes rather than focusing on writing extensive privacy notices.[357]

However, it should be noted that the GDPR already places responsibility on controllers. Controllers' responsibilities are laid down in Article 24 of the GDPR, which is complemented by Article 25. Moreover, the GDPR includes an accountability principle which provides that controllers shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with the Regulation.[358] The Regulation requires that personal data is i) processed lawfully, fairly and transparently, ii) collected for specific purposes (purpose limitation), iii) adequate, relevant and limited to what is necessary (data minimization), iv) accurate and, where necessary, kept up to date (accuracy), v) kept in a form which permits identification of data subjects for no longer than is necessary (storage limitation), and vi) processed in a manner that ensures appropriate security of personal data (integrity and confidentiality).[359]

Shifting the burden of on companies has also been considered in relation to the ePrivacy Regulation. In 2020 the Croatian Presidency of the European Council proposed changes to the proposed ePrivacy Regulation. One of the key changes was the introduction of legitimate interest as a legal basis, in addition to consent, to process metadata and collect information from a terminal equipment.[360] Although legitimate interest as a ground for processing electronic communications data has been removed during the German Presidency[361], the Croatian Presidency's proposal is a notable step away from consent.

According to Article 6(1)(f) of the GDPR processing of personal data is lawful if "processing is necessary for the purposes of 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, in particular where the data subject is a child". Legitimate interest thus places responsibility on the controller to justify the

[357] Ibid.
[358] Article 5(2) and Article 24 of the GDPR.
[359] Article 5(1) of the GDPR.
[360] Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), 5979/20, 21 February 2020.
[361] Jonathan McDonald, 'ePrivacy Update' (*Lexology,* 5 February 2021) < https://www.lexology.com/library/detail.aspx?g=77a4c80a-b718-4543-8baf-aa7b580d1485> accessed 15 October 2021.

processing and the impact of the processing on individuals. The legitimate interest ground contains a three-stage test for the ground to be applicable. First of all, the purpose test requires that there is an existence of a legitimate interest.[362] Secondly, the necessity test requires that the processing of personal data is necessary for those legitimate interest to be achieved.[363] Lastly, the balancing test dictates that the interest of the controller or a third party must be balanced against the impact of the fundamental rights and freedoms of the individual whose data is being processed.[364]

Some have seen the Croatian Presidency's proposal as a welcomed step due to the shortcomings of consent.[365] The Centre for Information Policy Leadership (CIPL) has for example criticized the overemphasis of consent in the proposed ePrivacy Regulation and the exclusion of other grounds for processing.[366] According to them "the over-reliance on consent will have the unintended consequence of undermining the GDPR, as well as legitimate, necessary and beneficial processing of data and business practices within the Digital Single Market".[367] In their view consent should be used only in situations where there is a high risk for individual's privacy that cannot be alleviated and in situations where the end user can be provided with meaningful information and choices.[368] In other instances, the ePrivacy Regulation should recognize legitimate interest as an available ground for processing according to CIPL.[369] However, the EDPB has not supported the idea. For example, the Croatian Presidency's proposal contradicts with the EDPB's statement delivered in 2018 according to which "there should be no possibility under the ePrivacy Regulation to process electronic communications

[362] ICO, 'How do we apply legitimate interest in practice?' < https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/> accessed 15 October 2021.
[363] Ibid.
[364] Ibid.
[365] For example, Eduardo Ustaran, Hogan Lovells Privacy and Cybersecurity Practice Global Co-Head, believes that "after so many years of flawed cookie consent, it is a productive thing to do to introduce another approach into the legislative debate. My view is that 'legitimate interests' is misunderstood and underrated as a regulatory mechanism to protect our privacy" in Jennifer Baker, 'Critics on Croatia's ePrivacy proposal: Legitimate interest provisions not legitimate' (*IAPP,* 25 February 2020) <https://iapp.org/news/a/critics-on-croatias-eprivacy-proposal-legitimate-interest-provisions-not-legitimate/> accessed 15 October 2021.
[366] CIPL, 'Recommendation for Implementing Transparency, Consent and Legitimate Interest under the GDPR' (19 May 2017) 15 < https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_recommendations_on_transparency_consent_and_legitimate_interest_under_the_gdpr_-19_may_2017-c.pdf> accessed 15 October 2021.
[367] CIPL, 'Comments on the Proposal for an ePrivacy Regulation' (11 September 2017) 3 < https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_the_proposal_for_an_eprivacy_regulation_final_draft_11_september_2017.pdf> accessed 15 October 2021.
[368] Ibid.
[369] Ibid.

content and metadata based on open-ended grounds, such as 'legitimate interests', that go beyond what is necessary for the provision of an electronic communications service".[370]

According to the Croatian Presidency's proposal the end-user's interests shall be deemed to override the interests of the service or network provider when the service provider processes, stores or collects data to build an individual profile of the end-user and when the information or metadata contains special categories of personal data.[371] Although it is good that the sensitive nature of special categories of data has been considered, the proposal does not acknowledge the sensitive nature of metadata. Although a piece of metadata would not contain special categories of personal data at the moment of collection, that does not mean that it would not reveal sensitive information about an individual over time.

It is difficult to see how shifting burden from individuals to companies would work taken into account how much commercial value data holds to them. Data has been said to be the oil of the 21st century – a raw material on which companies and even economies are being built on.[372] Further, as Joergensen notes, trusting companies' accountability seems "overly optimistic" as in the modern age harvesting personal data functions as the core of many companies' business model.[373] In today's world, a lot of data collection happens in a position of power and information asymmetry. Although this thesis agrees that companies may be better placed to assess the impact of the processing and to implement appropriate mitigations and safeguards, this would tip the scale almost completely to companies' side. For example, introducing a legitimate interest ground to the ePrivacy regulation would lead to even lesser degree of control by the user than they currently have under ePrivacy Directive. Furthermore, according to Koops the current system already places too much faith in controller action.[374] He argues that even though controllers would want to follow data protection law, the current system is so complex that controllers will blindly follow the rules without actually understanding much of data

[370] EDPB, 'Statement of the EDPB on the revision of the ePrivacy Regulation and its impact on the protection of individuals with regard to the privacy and confidentiality of their communications' (n 95).
[371] Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), 5979/20, 21 February 2020 (n 360).
[372] See Shannon Tellis, 'Data is the 21st century's oil, says Siemens CEO Joe Kaeser' (May 24 2018) *The Economic Times* < https://economictimes.indiatimes.com/magazines/panache/data-is-the-21st-centurys-oil-says-siemens-ceo-joe-kaeser/articleshow/64298125.cms> accessed 15 October 2021.
[373] Rikke Frank Joergensen, 'The unbearable lightness of user consent' (2014) 3(4) Internet Policy Review, 9 < http://policyreview.info/articles/analysis/unbearable-lightness-user-consent> accessed 4 October 2021.
[374] Koops (n 22) 253-256.

protection.[375] As he describes, this will "not lead to data protection law being a dead letter, as the letters are (at best) obediently followed, but it will result in the law being a zombie: it seems to live, but lacks vital spirit".[376]

In order to accommodate the challenges of IoT, many scholars are turning to privacy by design, which has been praised "as the best way forward for the failure of 'traditional' consent".[377] The WP29 has for example stated that "every stakeholder in the IoT should apply the principles of Privacy by Design and Privacy by Default".[378] The core idea here is to embed privacy into the design and engineering processes of smart devices as well as to business practices of the stakeholders. This would free individuals from bearing the burden of data protection as personal data would be automatically protected for example in any device and application. According to Cavoukian privacy by design should include seven principles: i) proactive rather than reactive, ii) the default settings of a device or a service should be set to a level that provide maximum privacy iii) embed privacy into the solution design and architecture of a device or a service, iv) full functionality – positive-sum, not zero-sum meaning that there should be no unnecessary trade-offs where individuals have to choose between seemingly contradicting options such as privacy and security, but rather all legitimate interests should be accommodated, v) provide full lifecycle protection, vi) establish visibility and transparency, and vii) respect user privacy and keep it user-centric.[379]

Privacy by design and default are already put into law in Article 25 of the GDPR. According to Article 25(1) controller shall implement appropriate technical and organizational measures which are designed to implement the data protection principles and to integrate the necessary safeguards into the processing in order to meet the requirements and protect the rights and freedoms of data subjects. Moreover, Article 25(2) stipulates that controller shall implement

[375] Ibid, 255.
[376] Ibid, 255-256.
[377] Edwards, 'Data Protection and e-Privacy: From Spam and Cookies to Big Data, Machine Learning and Profiling' (n 38) 161.
[378] WP29, 'Opinion 8/2014 on the Recent Developments on the Internet of Things' (n 35) 21.
[379] Ann Cavoukian, 'Privacy by Design. The 7 Foundational Principles Implementation and Mapping of Fair Information Practices' (2010) Information and Privacy Commissioner of Ontario < https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf > accessed 11 October 2021; see also Ann Cavoukian and Claudia Popa, 'Embedding Privacy into What's Next: Privacy by Design for the Internet of Things' (2016) Ryerson University, Privacy & Big Data Institute < https://www.ryerson.ca/content/dam/pbdce/papers/Privacy-by-Design-for-the-Internet-of-Things.pdf > accessed 11 October 2021. Moreover, these principals established by Cavoukian are echoed in the Spanish data protection authority's (AEPD) guide to privacy by design, thus implying that these principles are also recognized in the EU; see AEPD, 'A Guide to Privacy by Design' (2019) < https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf > accessed 11 October 2021.

appropriate technical and organizational measures, by default, to ensure that only necessary personal data is processed. Privacy by design thus reflects an accountability requirement for controllers.[380] The introduction of accountability represents a paradigm shift in data protection: "something which has traditionally been construed of in engineering terms as a 'non-functional' requirement—a matter of providing information to people (e.g., via terms and conditions or privacy notices)—is shifting under GDPR into a 'functional' requirement and something that must, therefore, be built into the IoT".[381]

Such privacy by design solutions could include for example restricting the amount of data collected by sensors to minimum, anonymizing personal data (as we saw there are, however, some difficulties to this when it comes to IoT), implementing better ways to provide privacy notices and designing user-friendly privacy settings.[382] Although privacy by design solutions seem especially attractive in terms of IoT considering the lack of screens, opacity of data flows and "internet of other people's things", the GDPR does not specify or provide clear guidance on how such solutions should be implemented in practice or what such solutions should look like. As Urquhart et al. puts it "GDPR is 'technologically neutral', it offers no insight to 'systems designers' as to how to build accountability into the technological ecosystem generally or into the IoT specifically".[383] Due to this vagueness of privacy by design and default, it comes as no surprise that there have been some troubles putting the policy into practice.[384]

First of all, engineers do not have a detailed understanding of data protection requirements and lack the tools to make privacy by design a reality. As Birnhack et al. argue "whereas for lawyers PbD [privacy by design] seems an intuitive and sensible policy tool, for information systems developers and engineers it is anything but intuitive as it goes against the grain of several well-established principles of information systems engineering".[385] Raising the engineers' and designers' awareness of law is therefore important. However, it may not be enough. It has been

[380] AEPD (n 379) 6.
[381] Andy Crabtree et al., 'Building accountability into the Internet of Things: the IoT Databox model' (2018) 4 Journal of Reliable Intelligent Environment 39, 41.
[382] Edwards, 'Privacy, security and data protection in smart cities: a critical EU law perspective' (n 261) 27.
[383] Lachlan Urquhart et al., 'Demonstrably doing accountability in the Internet of Things' (2019) 27 International Journal of Law and Information Technology 1, 15.
[384] See for example Enisa, 'Privacy and data protection in mobile applications. A study on the app development ecosystem and the technical implementation of GDPR' (2017) < https://www.enisa.europa.eu/publications/privacy-and-data-protection-in-mobile-applications> accessed 11 October 2021.
[385] Michael Birnhack et al, 'Privacy Mindset, Technological Mindset' (2014) 55 Jurimetrics: Journal of Law, Science & Technology, 3 <http://dx.doi.org/10.2139/ssrn.2471415> accessed 11 October 2021.

pointed out by Urquhart that the whole concept of privacy is contested.[386] Engineers and developers are required to implement rather abstractive concept into practice, while users of IoT devices are providing them with limited guidance due to the privacy paradox and the law does not specify what is required from them in practice.[387] Lastly, Edwards has argued that privacy by design does not work well with fact that data holds such value to companies.[388] In other words, although there is a regulatory incentive to adopt privacy protecting features to IoT devices, there may not be enough economic incentive to do so. This thesis agrees. However, this argument could be contested as the national data protection authorities are starting to fine companies for non-compliance of the principle. For example, in 2019 a German real estate company was fined 14,5 million euros for not implementing privacy by design.[389] However, considering all the arguments above it seems rightful to state that "encoding data protection requirements in software or hardware shows that this is much easier said than done".[390]

5.3. Summary of the alternative ways forward

The above discussion shows that the very critics of consent are not ready to entirely abandon consent. However, it is clear that the current consent model in failing in digital environments. An alternative way forward is thus needed. From the discussion above, two alternative ways can be distinguished:

i) Improving consent
ii) Shifting the focus away from consent

The first alternatives presented focus on improving consent. While some scholars and authors have focused on putting in place more substantive rules that prohibit certain troublesome practices, most have focused on improving the informedness of consent. These ideas have centered around new ways to present privacy notices. These include making the notices shorter or otherwise easier to understand, layering notices and presenting notices in more visual ways

[386] Lachlan Urquhart, "White Noise from the White Goods? Privacy by Design for Ambient Domestic Computing" in Lilian Edwards (ed.), *Future Law: Emerging Technology, Regulation and Ethics* (Edinburgh University Press, 2020) ch. 3.
[387] Ibid.
[388] Edwards, 'Privacy, security and data protection in smart cities: a critical EU law perspective' (n 261) 28.
[389] Avishai Ostrin, 'Privacy by design – GDPR's sleeping gian' (IAPP, 15 June 2020) < https://iapp.org/news/a/privacy-by-design-gdprs-sleeping-giant/> accessed 16 October 2021.
[390] Bert-Jaap Koops and Ronald Leenes, 'Privacy Regulation Cannot Be Hardcoded. A critical comment on the 'privacy by design' provision in data-protection law' (2014) 28 International Review of Law, Computers & Technology, 8 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2564791> accessed 11 October 2021.

such as with images and icons. With the rise of behavioral research, scholars have also explored the use of nudges and visceral notices. Although this thesis sees improving informedness of consent as an important goal, it also recognizes that this approach fails to take into account the realities of screenless technologies. Most of the alternatives proposed here thus seem more suitable for improving website user's consent, rather than smart device users. It is also important to recognize that improving the informedness of consent only attempts to solve issues relating to informed consent. However, it does not present a solution for the problems of freely given consent. In other words, improving the informedness of consent attempts to solve information asymmetries between data subjects and controllers, but fails to take into account the power asymmetries also present.

The second line of alternatives take a step away from consent. The consent model places much responsibility on individuals. However, as we have seen individuals are not always apt to take on such responsibility. Thus, some critics of consent have proposed that the burden of data protection should be shifted on companies. This thesis argues that companies may be better placed to assess the impact of the processing and to implement appropriate mitigations and safeguards, however, it also questions whether shifting the responsibility to companies would work in practice taken into account the huge commercial value data holds.

One way of shifting the burden of data protection to companies is privacy by design and default. Privacy by design and default aims to embed privacy into the design and engineering process of the smart device as well as to business practices of the stakeholders. Privacy by design places an accountability requirement for controllers. The introduction of accountability represents a paradigm shift in data protection. Companies are not only required to provide privacy information to people but are also required design devices and processes with privacy in mind.

6. Conclusion

IoT has become part of individuals' everyday lives. As sensor embedded devices become more and more common, so will privacy concerns, as these devices have a capacity to collect data in an unprecedented scale. This thesis has shown that the data collected by these smart devices will most likely qualify as personal data as defined in the GDPR. Moreover, it has been established that large amounts of data collected by IoT devices can, in many instances, constitute sensitive personal data that reveal information such as racial or ethnic origin, political opinions, health and religion of the individual concerned.

The protection of individuals in relation to the processing of personal data is a fundamental right. Therefore, in accordance with the GDPR processing of personal data is allowed only under a number of legal bases one of which is consent. In order for consent to be valid it must be freely given, specific, informed and unambiguous indication of the data subject's wishes. Consent also plays a central role in the ePrivacy Directive, where the processing of electronic communications content and metadata as well as storing or accessing information already stored in user's or subscriber's device is only possible with consent.[391] In the European data protection framework consent thus functions as a key element of data protection. Its widespread use implies that it is the most common standard of legitimacy for the processing of personal data. Consent is closely tied with the notions of information self-determination and privacy self-management, where individuals are granted the control of their personal data and through this control, they are expected to make privacy decisions based on costs-benefit analysis of the use of their personal data. However, this thesis has shown that this kind of privacy-self management is not working.

This thesis has examined the problems related to consent in IoT. This thesis has shown that in practice consent is neither freely given nor informed. The problems with informed consent stem from the information asymmetries between individuals and companies. These asymmetries arise from personal data collection and analysis as individuals are not aware of what data is collected from them, how that data is being used and what inferences can be derived from that data, consequently calling into question the validity of informed consent. IoT only worsens this asymmetry as smart devices are designed to be ubiquitous and function unobtrusively.

[391] ePrivacy Directive excludes the other grounds for processing. However, these operations are possible with consent or if they meet one of the exceptions offered by the ePrivacy Directive such as transmission of a communication over an electronic communication network.

Furthermore, communication between IoT devices may be triggered automatically, making it almost impossible for individuals to manage their personal data. The GDPR tries to mitigate the information asymmetry through transparency requirement, which often manifests itself through privacy notices and policies. However, this thesis has shown that privacy notices are often too long and legalistic making them difficult to understand; resulting to a situation where notices are not read.

The problems with freely given consent arise from power asymmetries between individuals and companies. In practice, this means that dominant companies are able to exercise their power by one-sidedly imposing their practices on individuals. This undermines the basic notion of freely given consent as data subjects are not able to exercise real choice. As IoT devices become increasingly common, users will become increasingly dependent on smart devices. It is thus problematic, if individuals are forced to engage with challenging practices, where there is no room for negotiation. Moreover, in many cases switching devices or service provider may not be a viable option as IoT is characterized by lack of standardization and interoperability.

IoT also brings with itself a unique set of problems as most IoT devices lack screens and input methods making it hard for individuals to access privacy notices and provide consent. The unobtrusive and ubiquitous nature of IoT makes data collection activities invisible. Users are often unaware of the sensors surrounding them and the data collection processes taking place, thus questioning the existence of meaningful consent. As smart devices are becoming more and more common in shared spaces such as stores and public transportation, it also raises questions how people will be informed about the purposes of the processing of their personal data. Further, in such a situation how can an individual give a valid consent. Moreover, IoT devices such as wearable fitness trackers do not only collect information about their user, but also from people around them. It is difficult to see how the notice and consent model could be an option in "internet of other people's things". The shift from mere smart devices into entire smart environments, moves individuals beyond the realm of control.

The problems with consent are worrisome. As IoT continues to evolve and become more and more common in human environments such as in the domestic and consumer world, the problems with consent will only exacerbate. Due to this, there is a need to rethink alternatives to the dominant consent approach. However, this thesis argues that consent should not be completely abandoned as consent still holds value to individuals' autonomy. Moreover, it is hard to see that consent could be completely set aside considering its fundamental role given

by the Charter. In light of this, this thesis distinguishes two alternative ways forward: improving consent and shifting the focus away from consent.

Due to the information asymmetries plaguing consent, many scholars have focused on improving the informedness of consent. In order to achieve this, scholars are proposing innovative new ways to present privacy notices. These include making notices shorter or otherwise easier to understand, layering notices and making notices visual with images and icons. Others have focused on nudging people to better privacy behavior through design. Although this thesis believes that such approaches are important in mitigating the information asymmetry, it is also questionable does this approach cater for the challenges of screenless IoT devices. Moreover, improving the informedness of consent does not provide a solution for the power asymmetries present between data subjects and controllers.

The emphasis on control and consent puts the responsibility on individuals as the ultimate decision makers. This places a significant burden on data subjects. In order to reduce the burden of individuals, the focus should be shifted away from consent. Several scholars and practitioners have proposed that the burden of data protection should be placed more on companies. Due to information asymmetries, this thesis argues that companies may be better placed to assess the impact of their data processing and to implement appropriate mitigations and safeguards. This thesis sees privacy by design and default, a new normative requirement introduced by the GDPR, especially attractive in terms of IoT. Privacy by design and default aims to embed privacy into the design and engineering process of the smart devices as well as to business practices of stakeholders. Privacy by design shifts the responsibility of data protection to companies and places an accountability requirement for controllers.

This thesis, however, questions whether shifting the responsibility to companies works in practice taken into account the commercial value data holds and the fact that some companies have built their entire business model around personal data. Data has even been labeled as the new oil of the 21st century. Thus, trusting companies' accountability seems overly optimistic. Moreover, considering the power asymmetry that already exists between data subjects and controllers, one has to question whether it is desirable to further decrease individuals' control.

To conclude, this thesis has painted a troubling picture of consent as a tool to exercise control over one's personal data in digital environments. Not only is IoT exacerbating the existing problems with consent, but also creating new ones as the diminishment of private spaces.

Therefore, it seems fair to state that the current model of consent is not adequate to respond to the evolving technological reality. If new alternative ways that complement individuals' autonomy but also assert control over smart devices and data flows cannot be found, our society risks of destroying the concept of privacy and turning into a surveillance society. Therefore, more research is needed in the field of IoT and data protection. Although IoT is already very much present in our everyday lives, much of the research is still stuck on studying data protection in the context of the traditional Internet.

Bibliography

Primary sources

Cases

1) Joined Cases C-203/15 and C- 698/15 *Tele 2 Sverige AB v Post- och telestyrelsen, and Secretary of State for the Home Department v Watson* [2016] ECLI:EU:C:2016:970

2) Case C-673/17 *Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v Planet49 GmbH* [2019] ECLI:EU:C:2019:801

3) BVerfGE 65, 1 – Volkszahlung Urteil des Ersten Senats vom 15. Dezember 1983 auf die ¨ mundliche Verhandlung vom 18. und 19. Oktober 1983 -1 BvR 209, 269, 362, 420, 440, 484/83 in den Verfahren uber die Verfassungsbeschwerden. English Abstract of the German Federal Constitutional Court's Judgment of 15 December 1983 <https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html> accessed 24 September 2021

Legislation

4) Charter of Fundamental Rights of the European Union [2012] OJ C 326

5) Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C 326/47

6) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31

7) 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 (Directive on privacy and electronic communications) [2002] OJ L 201/37

8) 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 [2009] OJ L 337.

9) Regulation (EU) No 1169/2011 of the European Parliament and of the Council of 25 October 2011 on the provision of food information to consumers, amending Regulations (EC) No 1924/2006 and (EC) No 1925/2006 of the European Parliament and of the Council, and repealing Commission Directive 87/250/EEC, Council Directive 90/496/EEC, Commission Directive 1999/10/EC, Directive 2000/13/EC of the European Parliament and of the Council, Commission Directives 2002/67/EC and 2008/5/EC and Commission Regulation (EC) No 608/2004 [2011] OJ L 304

10) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119

Secondary sources

11) Acquisti A, 'Nudging privacy: The behavioral economics of personal information' [2009] IEEE Security & Privacy 72

12) —, 'Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online' (2017) 50(3) ACM Computing Surveys 1 < https://www.ftc.gov/system/files/documents/public_comments/2017/11/00031-141888.pdf> accessed 4 October 2021

13) AEPD, ‘A Guide to Privacy by Design’ (2019) < https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf > accessed 11 October 2021

14) Allen A, *Unpopular Privacy: What Must We Hide?* (Oxford Scholarship, 2011)

15) Article 29 Data Protection Working Party, ‘Opinion 2/2010 on Online Behavioral Advertising’ (WP 171, 22 June 2010)

16) —, ‘Opinion 15/2011 on the definition of consent’ (WP187, 13 July 2011)

17) —, ‘Opinion 03/2013 on purpose limitation’ (WP 203, 2 April 2013)

18) —, ‘Working Document 02/2013 Providing Guidance on Obtaining Consent for Cookies’, (WP 208, 2 October 2013)

19) —, ‘Opinion 8/2014 on the Recent Developments on the Internet of Things’ (WP 223, 16 September 2014)

20) —, ‘Opinion 03/2016 on the evaluation and review of the ePrivacy Directive’ (WP 240, 19 July 2016)

21) —, ’Guidelines on transparency under Regulation 2016/679’ (WP260, 11 April 2018)

22) Baker J, ‘Critics on Croatia’s ePrivacy proposal: Legitimate interest provisions not legitimate’ (IAPP, 25 February 2020) <https://iapp.org/news/a/critics-on-croatias-eprivacy-proposal-legitimate-interest-provisions-not-legitimate/> accessed 15 October 2021

23) Barocas S and Nissenbaum H, ‘Big Data’s End Run around Anonymity and Consent’ in Julia Lane et al. (eds.) *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (Cambridge University Press, 2014)

24) Bashir M et al, 'Online privacy and Informed Consent: The Dilemma of Information Asymmetry' (2016) 52 Proceedings of the Association for Information Science and Technology < https://asistdl.onlinelibrary.wiley.com/doi/epdf/10.1002/pra2.2015.145052010043> accessed 27 September 2021

25) Bastos D et al., 'GDPR Privacy Implications for the Internet of Things' (4th Annual IoT Security Foundation Conference, London, 2018) <https://www.researchgate.net/publication/331991225_GDPR_Privacy_Implications_for_the_Internet_of_Things > accessed 16 August 2021

26) Basaure A, Vesselkov A and Töyli J, ' Internet of things (IoT) platform competition: Consumer switching versus provider multihoming' (2020) 90-91 Technovation < https://doi.org/10.1016/j.technovation.2019.102101> accessed 30 September 2021

27) Batura O, van Gorp N and Larouche P, 'Online Platforms and the EU Digital Single Market' (2015) A Response to the Call for Evidence by the House of Lord's Internal Market Sub-Committee <https://ec.europa.eu/information_society/newsroom/image/document/2016-7/nikolai_van_gorp_-_response_e-conomics_to_the_uk_house_of_lords_call_for_evidence_14020.pdf > accessed 30 September 2021

28) Bergemann B, 'The Consent Paradox: Accounting for the Prominent Role of Consent in Data Protection' in Hansen M et al. (eds.), *Privacy and Identity Management. The Smart Revolution* (Springer International Publishing, 2018)

29) Bietti E, 'The Discourse of Control and Consent over Data in EU Data protection Law and Beyond' (2020) A Hoover Institution Essay <https://www.hoover.org/research/discourse-control-and-consent-over-data-eu-data-protection-law-and-beyond > accessed 16 September 2021

30) Birnhack M et al, ’Privacy Mindset, Technological Mindset’ (2014) 55 Jurimetrics: Journal of Law, Science & Technology <http://dx.doi.org/10.2139/ssrn.2471415> accessed 11 October 2021

31) Borgesius F Z, ’ Informed Consent: We Can Do Better to Defend Privacy’ (2015) 13 Security & Privacy <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2793769> accessed 27 September 2021

32) Botta M & Wiedemann K, ’The Interaction of EU Competition, Consumer, and Data Protection Kaw in the Digital Economy: The Regulatory Dilemma in the Facebook Odyssey’ (2019) 64 The Untitrust Bulletin 428 <https://doi.org/10.1177/0003603X19863590> accessed 3 October 2021

33) Calo M R, ’Against Notice Skepticism in Privacy (and Elsewhere) (2012) 87 Notre Dame Law Review 1027

34) Campbell C, ‘Apple will require apps to add privacy ‘nutrition labels’ starting December 8th’ (The Verge, 5 November 2020) <https://www.theverge.com/2020/11/5/21551926/apple-privacy-developers-nutrition-labels-app-store-ios-14> accessed 4 October 2021

35) CASAGRAS, ’RFID and the Inclusive Model for the Internet of Things’ (2009) CASAGRAS EU Framework Project, Final Report <www.rfidglobal.eu%20CASAGRAS%20IoT%20Final%20Report%20low%20resolution.pdf> accessed 2 April 2020

36) Cavoukian A, ’Privacy by Design. The 7 Foundational Principles Implementation and Mapping of Fair Information Practices’ (2010) Information and Privacy Commissioner of Ontario < https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf > accessed 11 October 2021

37) Cavoukian A and Popa C, ‘Embedding Privacy into What’s Next: Privacy by Design for the Internet of Things’ (2016) Ryerson University, Privacy & Big Data Institute <

https://www.ryerson.ca/content/dam/pbdce/papers/Privacy-by-Design-for-the-Internet-of-Things.pdf > accessed 11 October 2021

38) Ciocchetti C A, 'The Future of Privacy Policies: A Privacy Nutrition Label Filled with Fair Information Practices' (2008) 26(1) The John Marshall Journal of Information Technology & Privacy Law 1

39) CIPL, 'Comments on the Proposal for an ePrivacy Regulation' (11 September 2017) <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_the_proposal_for_an_eprivacy_regulation_final_draft_11_september_2017.pdf> accessed 15 October 2021

40) —, 'Recommendation for Implementing Transparency, Consent and Legitimate Interest under the GDPR' (19 May 2017) <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_recommendations_on_transparency_consent_and_legitimate_interest_under_the_gdpr_-19_may_2017-c.pdf > accessed 15 October 2021

41) Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) (2020) 5979/20

42) —, Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) (2021) 6087/21

43) Chynoweth P, 'Legal research' in Andrew Knight and Les Ruddock (eds.), *Advanced research Methods in the Built Environment* (Blackwell Publishing, 2008)

44) Clifford D, Graef I and Valcke P, 'Pre-formulated Declarations of Data Subject Consent- Citizen-Consumer Empowerment and the Alignment of Data, Consumer and

Competition Law protection' (2019) 20 German Law Journal 679 <doi:10.1017/glj.2019.56> accessed 3 October 2021

45) Crabtree A et al, 'Building accountability into the Internet of Things: the IoT Databox model' (2018) 4 Journal of Reliable Intelligent Environment 39

46) De Mooy M, 'Rethinking Privacy Self-Management and Data Sovereignty in the Age of Big Data. Considerations for Future Policy Regimes in the United States and the European Union' (2017) Center for Democracy and Technology < https://cdt.org/wp-content/uploads/2017/04/Rethinking-Privacy_2017_final.pdf> accessed 25 September 2021

47) de Terwangne C, 'The Right to be Forgotten and the Information Autonomy in the Digital Environment' (2013) Publications Office of the European Union < https://publications.jrc.ec.europa.eu/repository/handle/JRC86750> accessed 25 September 2021

48) Edwards L, 'Privacy, Law, Code and Social Networking Sites' in Ian Brown (ed.) *Research Handbook on Governance of the Internet* (Edward Elgar Publishing, 2013)

49) —, 'Privacy, security and data protection in smart cities: a critical EU law perspective' (2016) 2 European Data Protection Law Review <http://dx.doi.org/10.2139/ssrn.2711290> accessed 30 September 2021

50) —, 'Data Protection and e-Privacy: From Spam and Cookies to Big Data, Machine Learning and Profiling' in Lilian Edwards (ed.) *Law, Policy and the Internet* (Hart Publishing, 2019)

51) Edwards L & Vale V, 'Slave to the Algorithm' (2017) 16 Duke Law & Technology Review 18

52) European Commission, 'Internet of Things – An action plan for Europe' COM(2009) 278 final

53) —, ’A Digital Agenda for Europe’ COM(2010)245 final

54) —, ’Impact Assessment. Accompanying the document 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) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data’ (Commission Staff Working Paper) SEC(2012) 72 final.

55) —, ‘Advancing the Internet of Things in Europe’ SWD(2016) 110 final

56) —, ‘Digitising European Industry Reaping the full benefits of a Digital Single Market SWD(2016) 110 final

57) —, Special Eurobarometer 487a: The General Data Protection Regulation (2019) 48

58) —, ‘Preliminary report – Sector Inquiry into Consumer Internet of Things’ SWD(2021) 144 final

59) European Data Protection Board, ‘Statement of the EDPB on the revision of the ePrivacy Regulation and its impact on the protection of individuals with regard to the privacy and confidentiality of their communications’ (25 May 2018) < https://edpb.europa.eu/sites/default/files/files/file1/edpb_statement_on_eprivacy_en.pdf> accessed 18 September 2021

60) —, ‘Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities’ (12 March 2019)

61) —, ’Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications’ (9 March 2021)

62) —, ‘Guidelines 05/2020 on consent under Regulation 2016/679’ (4 May 2020)

63) Enisa, ’Privacy and data protection in mobile applications. A study on the app development ecosystem and the technical implementation of GDPR’ (2017) < https://www.enisa.europa.eu/publications/privacy-and-data-protection-in-mobile-applications> accessed 11 October 2021

64) European Parliament, ’The Internet of Things: Opportunities and challenges’, (Briefing) (May 2015) <https://www.europarl.europa.eu/RegData/etudes/BRIE/2015/557012/EPRS_BRI(2015)557012_EN.pdf> accessed 9 August 2021

65) Europe-v-facabook.org, ‘Response to “audit” by the Irish Office of the Data Protection Commissioner on “Facebook Ireland Ltd.’ (4 December 2012) <http://www.europe-v-facebook.org/report.pdf> accessed 3 October 2021

66) Federal Trade Commission Staff Report, ‘Privacy & Security in a Connected World (January 2015) <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf> accessed 28 August 2021

67) Feokristov I, ‘Mobile IoT Apps and All You need to Know About Them’ (Relevant) < https://relevant.software/blog/mobile-iot-apps/ > accessed 1 September 2021

68) Furman J. et al., ’Unlocking digital competition’ (2019) Report of the Digital Competition Expert Panel <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf> accessed 30 September 2021

69) Gonzalez Fuster G and Scherrer A, ‘Big Data and Smart Devices and Their Impact on Privacy’ (2015) Study for the LIBE Committee (European Parliament)

< https://op.europa.eu/en/publication-detail/-/publication/65d436ef-7273-11e5-9317-01aa75ed71a1 > accessed 9 August 2021

70) Hoofnagle C and Whittington J, 'Free: Accounting for the Costs of the Internet's Most Popular Price' (2014) 61 UCLA Law Review 606

71) Hutchinson T, 'The Doctrinal Method: Incorporating Interdisciplinary Methods in Reforming the Law' (2015) 8(3) Erasmus Law Review 130

72) Information Commissioner's Office, '2016 GPEN Sweep – Internet of Things' (2016) <https://ico.org.uk/media/about-the-ico/disclosure-log/1625142/irq0648379-attachment.pdf> accessed 30 September 2021

73) —, 'How do we apply legitimate interest in practice?' < https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/> accessed 15 October 2021

74) Joergensen R F, 'The unbearable lightness of user consent' (2014) 3(4) Internet Policy Review <http://policyreview.info/articles/analysis/unbearable-lightness-user-consent> accessed 4 October 2021

75) Jones M L, 'Privacy Without Screens & the Internet of Other People's Things' [2015] Idaho Law Review 639

76) Koops B-J, 'The Trouble with European Data Protection Law' (2014) 4(4) International Data Privacy Law 250

77) Koops B-J and Leenes R, 'Privacy Regulation Cannot Be Hardcoded. A critical comment on the 'privacy by design' provision in data-protection law' (2014) 28 International Review of Law, Computers & Technology <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2564791> accessed 11 October 2021

78) Kosta E, *Consent in European Data Protection Law* (Martinus Nijhoff Publishers, 2013)

79) Lazaro C and Le Métayer D, 'The control over personal data: True remedy or fairy tale?' (2015) 12 SCRIPT-ed, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2689223 > accessed 27 September 2021

80) Lehtiniemi T and Kortesniemi Y, 'Can the obstacles to privacy self-management be overcome? Exploring the consent intermediary approach' [2017] Big Data & Society < https://doi.org/10.1177/2053951717721935> accessed 27 September 2021

81) Lindqvist J, 'Personal Data Protection on the Internet of Things an EU Perspective' (Doctoral dissertation, University of Helsinki, 2018) 1 <https://helda.helsinki.fi/handle/10138/263707> accessed 1 August 2021

82) Mackay W E, 'Triggers and Barriers to Customizing Software' (1991) Proceedings of the SIGCHI Conference on Human Factors in Computing Systems <https://www.lri.fr/~mackay/pdffiles/CHI91.Triggers.pdf> accessed 2 October 2021

83) Matzner T et al, 'Do-It-Yourself Data protection- Empowerment or Burden?' in Serge Gutwirth, Ronald Leenes and Paul De Hert (eds.), *Data Protection on the Move* (Springer, 2016)

84) Mayer-Schönberger V and Cukier K, *Big Data. A Revolution That Will Transform How We Live, Work and Think* (Houghton Mifflin Harcourt, 2013)

85) McDermott Y, 'Conceptualising the right to data protection in an era of Big Data' (2017) 4(1) Big Data & Society <https://journals.sagepub.com/doi/pdf/10.1177/2053951716686994> accessed 1 August 2021

86) McDonald A M and Cranor L F, 'The Cost of Reading Privacy Policies' [2008] I/S Journal of Law and Policy for the Information Society

<https://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf > accessed 27 September 2021

87) McDonald J, 'ePrivacy Update' (Lexology, 5 February 2021) <https://www.lexology.com/library/detail.aspx?g=77a4c80a-b718-4543-8baf-aa7b580d1485> accessed 15 October 2021

88) Monteleone S, 'Addressing the 'Failure' or Informed Consent in Online Data Protection: Learning the Lessons from Behavior-aware Regulation' (2015) 43(1) Syracuse Journal of International Law and Commerce 69

89) Nissenbaum H, 'A Contextual Approach to Privacy Online' (2011) 140(4) Daedalus 32

90) Nouwens M et al., 'Dark Partterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence' (2020) Conference on Human Factors in Computing Systems <https://arxiv.org/pdf/2001.02479.pdf > accessed 8 August 2021

91) OECD, 'Building Blocks for Smart Networks' (2013) 215 OECD Digital Economy Papers <https://read.oecd-ilibrary.org/science-and-technology/building-blocks-for-smart-networks_5k4dkhvnzv35-en#page1> accessed 27 September 2021

92) Office of the Privacy Commissioner of Canada, 'The Internet of Things. An Introduction to privacy issues with a focus on the retail and home environments' (February 2016) <https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/iot_201602/> accessed 30 September 2021

93) Office of the Victorian Information Commissioner, 'Internet of Things and Privacy – Issues and Challenges' <https://ovic.vic.gov.au/privacy/internet-of-things-and-privacy-issues-and-challenges/> accessed 2 October 2021

94) Oostveen M, *Protecting Individuals Against the Negative Impact of Big Data. Potential and Limitations of the Privacy and Data Protection Law* (Kluwer Law International, 2018)

95) Ostrin O, 'Privacy by design – GDPR's sleeping gian' (IAPP, 15 June 2020) <https://iapp.org/news/a/privacy-by-design-gdprs-sleeping-giant/> accessed 16 October 2021

96) Peppet S R, 'Regulating the Internet of Things: First Steps Towards Managing Discrimination, Privacy, Security & Consent' (2014) 93 Texas Law Review 85

97) Quelle C, 'Not just User Control in the General Data protection Regulation' in A. Lehmann et al. (eds.), *Privacy and Identity Management – Facing up to Next Steps* (Springer, 2017)

98) Ramírez López S, 'Informing Consent: Giving Control Back to the Data Subject from a Behavioral Economics Pespective' (2018) 9 Journal of Intellectual Property, Information Technology and E-Commerce Law 35 <JIPITEC_9_1_2018_35-50_Ramirez_Lopez> accessed 27 September 2021

99) Rosner G and Kenneally E, 'Privacy and the Internet of Things. Emerging Frameworks for Policy and Design' (2018) Center for Long-Term Cybersecurity <https://ssrn.com/abstract=3320670> accessed 30 September 2021

100) —, 'Clearly Opaque: Privacy Risks of the Internet of Things' (2018) IoT Privacy Forum < https://www.iotprivacyforum.org/wp-content/uploads/2018/06/Clearly-Opaque-Privacy-Risks-of-the-Internet-of-Things.pdf?d8bd54&d8bd54 > accessed 15 October 2021

101) Sanches-Rola I et al, 'Can I Opt Out Yet?: GDPR and the Global Illusion of Cookie Control' (2019) The 2019 ACM Asia Conference on Computer and Communication < https://doi.org/10.1145/3321705.3329806 > accessed 3 October 2021

102) Schermer B W, Custers B and van der Hof S, 'The Crisis of Consent. How Stronger Legal Protection may lead to Weaker Consent in Data Protection' [2014] Ethics and Information Technology <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412418 > accessed 27 September 2021

103) Smits J M, 'What is legal doctrine? On the aims and methods of legal-dogmatic research' (2015) Maastricht European Private Law Institute Working Paper No. 2015/06 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2644088 > accessed 8 August 2021

104) Snel M V R, 'Source-usage within doctrinal legal inquiry: choices, problems, and challenges' (2014) Law and Method < http://www.lawandmethod.nl/tijdschrift/lawandmethod/2014/06/RENM-D-13-00003/fullscreen> accessed 8 August 2021

105) Solove D J, 'Introduction: Privacy Self-Management and the Consent Dilemma' (2013) 126 Harvard Law Review 1879

106) Statista, Internet of Things (IoT) and non-IoT active device connections worldwide from 2010 to 2025 <https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/> accessed 9 August 2021

107) Susser D, 'Notice After Notice-and-Consent. Why Privacy Disclosures Are Valuable Even If Consent Frameworks Aren't' (2019) 9 Journal of Information Policy 37

108) Tellis S, 'Data is the 21st century's oil, says Siemens CEO Joe Kaeser' (May 24 2018) *The Economic Times* < https://economictimes.indiatimes.com/magazines/panache/data-is-the-21st-centurys-oil-says-siemens-ceo-joe-kaeser/articleshow/64298125.cms> accessed 15 October 2021

109) Tene O and Polonetsky J, ‘To Track or “Do Not Track”: Advancing Transparency and individual Control in Online Behaviorak Advertising’ (2012) 13(1) Minnesota Journal of Law, Science & Technology < http://dx.doi.org/10.2139/ssrn.1920505> accessed 4 October 2021

110) Thaler R H and Sunstein C R, *Nudge: Improving Decisions about Health, Wealth and Happiness* (Yale University Press, 2008)

111) Thobani S, ‘Processing Personal Data and the Role of Consent’ (2020) 2020 European Journal of Privacy Law & Technology 93

112) Urquhart L et al, ’Demonstrably doing accountability in the Internet of Things’ (2019) 27 International Journal of Law and Information Technology 1

113) Urquhart L, “White Noise from the White Goods? Privacy by Design for Ambient Domestic Computing” in Lilian Edwards (ed.), *Future Law: Emerging Technology, Regulation and Ethics* (Edinburgh University Press, 2020)

114) Van Alsenoy B, Kosta E & Dumortier J, ’Privacy notices versus informational self-determination: Minding the gap’ (2014) 28 International Review of Law, Computers &Technology 185

115) van den Berg B, ’Mind the Air Gap. Preventing Privacy Issues in Robotics’ in Serge Gutwirth, Ronald Leenes and Paul De Hert (eds.) *Data Protection on the Move. Current Developments in ICT and Privacy/Data Protection* (Springer, 2016)

116) van de Waerdt P, ’Information asymmetries: recognizing the limits of the GDPR on the data-driven market’ [2020] Computer Law & Security Review < https://pure.rug.nl/ws/portalfiles/portal/128134033/1_s2.0_S0267364920300418_main.pdf> accessed 27 September 2021.

117) Weir M, ‘What are Apple’s Privacy Nutrition Labels? Here’s what you need to know about the new App Store feature that prioritizes user privacy’ (Business Insider, 20 January 2021) <https://www.businessinsider.com/what-are-apple-privacy-nutrition-labels?r=US&IR=T> accessed 4 October 2021

118) Weiser M, ’ The Computer for the 21st Century’ (1991) Scientific American < https://www.ics.uci.edu/~corps/phaseii/Weiser-Computer21stCentury-SciAm.pdf> accessed 1 October 2021

119) Williams M, Nurse J R C and Creese S, ‘The Perfect Storm: The Privacy Paradox and the Internet-of-Things’ (2016) 11th International Conference on Availability, Reliability and Security <https://doi.org/10.1109/ARES.2016.25> accessed 18 September 2021

120) Wiredgov, ‘Privacy regulators study finds Internet of Things shortfalls’ (23 September 2016) <https://www.wired-gov.net/wg/news.nsf/articles/Privacy+regulators+study+finds+Internet+of+Things+shortfalls+23092016092000> accessed 30 September 2021