BALANCING SECURITY AND DATA PROTECTION IN IOT DATA SHARING

GEORGIOS GRIGORIADIS

UNIVERSITY CENTER OF INTERNATIONAL PROGRAMMES OF STUDIES
SCHOOL OF HUMANITIES, SOCIAL SCIENCES AND ECONOMICS

A thesis submitted for the degree of
Master of Laws (LLM) in Transnational and European Commercial Law, Banking Law, Arbitration / Mediation

January 2022
Thessaloniki – Greece

Student Name: Georgios Grigoriadis

SID: 1104200011
Supervisor: Prof. Komninos Komnios

I hereby declare that the work submitted is mine and that where I have made use of another's work, I have attributed the source(s) according to the Regulations set in the Student's Handbook.

January 2022
Thessaloniki - Greece

Abstract

This dissertation was written as part of the LLM in Transnational and European Commercial Law, Banking Law, Arbitration / Mediation at the International Hellenic University.

Today more than ever, it becomes apparent that the rapid improvement of technology offers humanity the opportunity to escape the past and draw new horizons. A great example of an innovation capable of altering the infrastructure of society as we know it today as a whole is Internet of Things. In the sphere of the IoT scheme belong objects (things) that have embedded sensors which inter alias interact with the environment, collect, store, share data and possess the ability to do exactly what the name suggest; create an Internet full of digitalized things.

But everything comes with a price, as the widespread use of IoT devices generates significant challenges regarding the balance between security and data protection. A vital first step that needs to be made in order to resolve effectively this equilibrium exercise is firstly to analyze the existing legal framework concerning security and privacy in the Internet of Things (IoT) scheme and secondly to define the term 'security and to highlight its nuances. As it will be explained later on in Chapter 3, security can either collide directly with relative fundamental rights, such as privacy and data protection, or it can be considered as a precondition that builds the necessary ground for the enjoyment of these rights. Lastly, from a philosophical standpoint, security can take the form of the safety of one's self that is compromised when personal data come into play and is misused.

This dissertation will make an attempt to assess in a concise yet comprehensive manner the aforementioned three-fold dimension of security within the context of Internet of Things data sharing, as well as to illustrate its interplay with data protection and the relevant legal framework.

Acknowledgments: I would like to thank my supervising Professor Dr. Komninos Komnios for guiding me and providing me much-needed feedback that was essential for the completion of this dissertation. I would also like to thank my family for supporting me as well as all of my friends, both old and new, who were there for me throughout this journey.

Keywords: IoT, security, data protection, privacy, identity

Georgios Grigoriadis
January 31st 2022

Contents

Introduction

Bob wakes up every day at around 7 am. He gets up, brush his teeth with his newly purchased smart toothbrush that is connected to the Internet and can provide information to Bob regarding the condition of his gum, the average time that he brushes every day, as well as his overall dental hygiene. Bob feels very fortunate that he was able to get his hands first on this new toothbrush, as it is very convenient for him to have all this information available any time in his phone. He knows that he did not exactly read the terms and conditions of the toothbrush when he decided to buy and activate it, but he is so impatient to use all of its features, that in reality he does not care at all about anything else at this particular moment. After the brushing, he washes his face and goes to his favorite spot, the living room. As mornings are usually gray in his town, he commands his digital voice assistant, Richard, to turn on the lights. Richard turns the lights on and informs Bob about the schedule of the day. The daily activities of Bob are categorized by Richard in relation to their importance. Their importance is determined according to Bob's preexisting wishes and choices and also according to the choices of his employer, who generously pays for the existence of extra and premium features in the digital provider's services.

Bob is aware that his employer has the right to ask Richard directly to hand him offer Bob's data, and sometimes this makes Bob feel that his privacy is being violated, yet he tends not to overstress the matter. In fact, every time he feels overwhelmed or anxious about the fact that his employer has access to very sensitive data of his, he remembers that his friends told him that he is '*one of the lucky ones*' and that '*this job is an opportunity of a lifetime*' and he instantly feels better and ready to seize the day. When Bob returns home some night, he randomly realizes that from the moment he started using the smart toothbrush and the new features of Richard, his home is packed with various new products, including vitamins and mints with no sugar.

Bob was not that kind of a person. In fact, he used to love buying vegetables and packs with gums of various sugary flavors. Curious as he was regarding this unexpected realization, he takes a quick internet search and finds that **a.** the company-owner of the toothbrush is also a multivitamin producer and **b.** that scientific research has found out that daily intake of sugar reduces work productivity. Bob was in a state of complete and utter shock; He finally came to realize that the choices he made during the day were not his at all. '*I do not recognize myself anymore',* he mumbled.

This simplistic yet not so far-fetched example is a reality existing in the environment of Internet of Things ('IoT'). As the use of IoT devices and embedded sensors, capable of gathering all sorts of information about us, is starting to grow very rapidly in all Europe and internationally, is sensible to assume that legal uncertainty will be created and worries will be expressed .The aim of this paper is not to talk about the numerous advantages that the adoption of this technology has in the lives of individuals, but to highlight the risks that the use of IoT pose on security and data protection, due to the partial inadequacy of the existing legal framework to deal with the ever-growing field of IoT and also the malicious intents of third parties (included even the State sometimes). For this goal to be achieved, this dissertation will focus on the normative challenges of the IoT scheme and more specifically will mainly approach the subject from the point of view of law of philosophy.

As far as the structure is concerned, Chapter 1 will make a quick introduction by delving into the past and the present use of IoT and also it will briefly explain what IoT is. Moreover, in Chapter 1 an effort will be made to highlight the importance of security and data protection in the IoT scheme. Chapter 2 shall analyze the most important (according to the author) pieces of current legislation that concern the use and governance of IoT. To be more specific, the corpus of this Chapter is consisted mainly of the analysis of certain very important aspects and provisions of the General Data Protection Regulation ('GDPR') and of the Cybersecurity Act, that both concern IoT. Chapter 3 shall make an attempt to point out the three-fold nature of the term 'security'. In fact, in Chapter 3 it shall be shown that security may **a.** operate as a moral enabler for the attainment of data protection and privacy, **b.** collide directly with relative fundamental rights such as data protection and **c.** take a more human-centered approach and concern the protection of the person itself. In Chapter 4 legislative instruments, proposed or adopted but currently not in force, will be analyzed and assessed in relation to IoT and also the author's views shall be expressed regarding the future of the balancing exercise between security and data protection, the attainment of which requires the adoption of a dynamic type of legislation. Lastly, a conclusion shall be made.

Chapter 1: What is Internet of Things ('IoT')?

It is evident that before this dissertation dives into the deeper aspects of IoT technology, logic dictates that the first vital step towards the accomplishment of the aforementioned end-goal would be for the reader to grasp the concept of what IoT actually means. This shall be realized by defining the term, by flashing back to the early days of this technology as well as by highlighting the importance of security and data protection within the IoT scheme.

1.1.) A quick overview of both the past and present of Internet of Things

It is a relatively unknown fact that the idea of 'Internet of Things' despite the tremendous popularity it has gained in the last twelve years, is not novel. In fact, even before the widespread use of the Internet, at Carnegie Mellon University in the mid 70's an old Coca-Cola vending machine was modified with installation of micro-switches that were able to sense the quantity of bottles available in each of its six columns of bottles. These switches were connected to the main computer of the Computer Science Department and a program was created that was able to keep tabs indicating in real time the availability of the bottles and the temperature of each one of them.[1] Without a doubt, this concept and its execution were the predecessors of the IoT as we know it today.

A couple of decades later, the notion 'ubiquitous computing' which is now strongly related to the essence of what IoT actually represents, was coined by Mark Weiser, a computer scientist and CEO of Xerox PARC. Weiser, in the now well citated paper of his, described the idea of a system comprised of electronic devices connected to a network, that were capable of communicating with each other via the exchange of data[2]. In his paper, Weiser supported the idea that devices such as personal computers and laptops were just a step of a ladder that ultimately leads to an environment where computers are an integral part of everyday life.

Lastly, in 1999 Kevin Ashton, came up with the term 'Internet of Thing', in an effort to describe a system where Internet does not remain purely digital, but also connects to the real world.

Nowadays, IoT devices are, at a certain extent, able to bridge the gap between physical and digital world, by allowing an independent and relatively secure (the aspect of security will be addressed later on), connection and exchange of data and information between devices that exist in physical form[3]. In the IoT scheme the primary focus is wireless sensing and communication between devices.[4] This goal is attained primarily

---

[1] 'The "Only" Coke Machine on the Internet' <https://www.cs.cmu.edu/~coke/history_long.txt> accessed 10 November 2021

[2] Mark Weiser, 'The Computer for the 21st Century' (1991) Scientific American 94, 98

[3] Rafiullah Khan, Sarmad Ullah Khan, Rifaqat Zaheer and Shahid Khan 'Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges' <https://ieeexplore.ieee.org/document/6424332> accessed 8 November 2021

[4] Hugo Landaluce , Laura Arjona , Asier Perallos , Francisco Falcone , Ignacio Angulo and Florian Muralter 'A Review of IoT Sensing Applications and Challenges Using RFID and Wireless Sensor Networks' (2020) 20 Sensors, 1

with the aid of two types of technology; RFID and WSN[5]. Without getting in too much detail, RFID is an automatic technology that helps devices or computers to track down objects and record metadata.[6] The RFID technology is comprised of two devices. The first one, known as reader, by using radio frequency signals identifies the second device known as tag, which has a unique electronic code embedded to it[7]. On the other hand, WSN, as Flammini and Sissini point out, can be defined as *'as the ensemble of spatially distributed, autonomous sensors that cooperate to monitor physical or environmental quantities of interest'*.[8] WSN technology is widely used today for home automation, health and traffic monitoring among other things[9].

1.2.) Importance of privacy and data protection within the IoT scheme

Along with other significant technological advancements, IoT is one of the most promising tech fields today. For the last ten years, all of the seeds for its growth have been constantly planted and now more than ever Internet of Things has become an ever-growing field of blooming opportunities and potential. However, as history has taught humanity countless times, the coin is always double-sided.

From the ones that are fitness-oriented and will monitor their heart rate and overall health on their wearables, to the others that will control every appliance of their smart home via an app or a voice command, the conclusion is that our reliance in automation, prediction and "auto-completion" is and will generate fundamental issues to human agents, regarding their security, privacy and data protection. Before proceeding to any further analysis, it is important to make a distinction between two terms that are different from one another but also overlap. These terms are 'privacy' and 'data protection'. As far as the notion of security is concerned, Chapter 3 will focus on illustrating its ambiguous and often confusing nature.

According to Hildebrandt[10], from the European perspective, privacy is an ambiguous negative relative fundamental right that is tightly linked to the unmonitored freedom of a person which unless justified legally, cannot be contained by the government or anyone else, whereas data protection is a positive right that promotes legal certainty by imposing via legislation an exhaustive set of rules and grounds for the lawful processing of data. As a matter of fact, one of the most important pieces of legislation concerning the protection of personal data, the General Data Protection Regulation (GDPR),[11] lays down six legal grounds that justify the processing of a subject's data.[12]

---

[5] Ibid, 2

[6] Xiaolin Jia, Quanyuan Feng, Taihua Fan, Quanshui Lei 'RFID Technology and Its Applications in Internet of Things (IOT)' (2012 2nd International Conference on Consumer Electronics, Communications and Networks, 2012) <https://ieeexplore.ieee.org/document/6201508> accessed 11 November 2021

[7] Landaluce, Arjona, Perallos, Falcone, Angulo and Muralter, supra note 4, at 3

[8] Alessandra Flammini and Emiliano Sisinni 'Wireless Sensor Networking in the Internet of Things and Cloud Computing Era' (2014) 87 Procedia Engineering 672,677

[9] Ibid, 679

[10] Mireille Hildebrandt, *Smart Technologies and the End(s) of Law Novel Entanglements of Law and Technology* (Edward Elgar Publishing Limited 2015) 187-190

[11] 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

This provision of the GDPR, reinforces the idea that certainty and not ambiguity governs the protection of data, in contrast with privacy.
Having made this clarification, it becomes apparent that all of these systems and electronic devices that comprise the IoT, place, both privacy and data protection of human agents, in question. As network and information systems, health and transport sector among others are relying heavily on these emerging technologies, data breaches and malicious targeting of critical infrastructures inter alia constitute daily phenomena, putting at risk personal lives of humans, as well as their well-being.

and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119
[12] Ibid, Article 6

Chapter 2: EU Legal Framework in Internet of Things

In Chapter 1 it has already been mentioned briefly that fundamental rights of human agents are at stake as a direct result of the wide use and constant development of IoT. With this in mind, it is also vital to highlight the fact that European Union has adopted in recent years a series of Regulations and Directives with the goal of reinforcing the protection of its civilians. Moreover, multiple reports and proposals have been issued by various EU institutions and bodies that try to fill the gaps of current legislation, which are created mainly due to the dynamic and unforeseeable character of technology and especially of IoT as well as due to the inability of law to keep up with these dramatic changes. In this Chapter, two of the most important legislative instruments concerning IoT devices shall be analyzed, the General Data Protection Regulation (GDPR) and the Cybersecurity Act.

2.1.) General Data Protection Regulation (GDPR)

Across European Union, the protection of personal data is a fundamental right. According to paragraph 1 of Article 8 of the European Charter of Fundamental Rights, the terms of which are addressed to the institutions and bodies of the Union as well as to national authorities when they are implementing the law of the Union[13]: '*Everyone has the right to the protection of personal data concerning him or her'.*[14]
In an effort to successfully abide by the obligation of Article 8 and to protect personal data, the European Union has implemented various legislative instruments, the most important of which is the General Data Protection Regulation (GDPR).

2.1.1.) A very brief historical overview of the GDPR

In January 2012 the European Commission adopted a package for a reform of the 1995 Data Protection Directive[15], which included among other things a proposal for a Regulation relating to the protection of individuals with regard to the processing of personal data and on the free movement of such data[16]. On this proposal, in March 2012, the European Data Protection Supervisor adopts an opinion[17], supporting inter alias that

[13]European Commission, 'When does the Charter apply?' <https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights/when-does-charter-apply_en> accessed 20 November 2021
[14] Charter of Fundamental Rights of the European Union [2012] OJ C 326/Article 8
[15] European Data Protection Supervisor, 'The history of the General Data Protection Regulation' <https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en> accessed 19 November 2021
[16] Commission (EC), 'Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)' (Communication) COM (2012) 11 final
[17] European Data Protection Supervisor, supra note 15

the proposed Regulation would provide legal certainty to the European Union civilians, economic actors and public bodies and that the implementation of the proposed Regulation would facilitate harmonization in the internal market, something that was not able to be achieved by the 1995 Directive[18]. Indeed, the rationale of the opinion as far as harmonization is considered was correct, given the fact that in European Union Law Directives are transposed into national law, whereas Regulations are applied automatically and uniformly[19]. Hence, Regulation is a more suitable instrument for the achievement of homogenous application of data protection rules[20] across EU.
Following the proposal of the European Data protection Supervisor, the Article 29 working party's opinion and the adoption of GDPR by the European Parliament, the European Parliament, the Council and the Commission reach an agreement on the GDPR[21] and the Regulation enters into force in May 2016, exactly twenty days after its publication in the official journal of the European Union.[22]

2.1.2.) Key provisions of GDPR related to Internet of Things

GDPR without a doubt consists the cornerstone of data protection in the European Union, as it was designed with a broad purpose; to service mankind[23]. Moreover, it is worth noting that the Regulation possesses a very broad territorial scope, as the GDPR is applicable both in the case that a data processing activity takes place in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not, as well as in the case that data processing of data subjects who reside in the Union takes place by a controller or processor not established in the Union[24]. This aforementioned provision applies the establishment principle, according to which the choice of law depends on the place of the entity's establishment. So, it becomes obvious that in order for the GDPR to be considered as an applicable legislative instrument, the decisive factor is not necessarily the place where the data is being processed[25].
Below, an analysis of the most important provisions of GDPR in relation to the Internet of Things shall be made:

---

[18] European data protection supervisor, 'Opinion of the European Data Protection Supervisor on the data protection reform package' (7 March 2012) <https://edps.europa.eu/sites/default/files/publication/12-03 07_edps_reform_package_en.pdf> accessed 20 November 2021
[19] European Commission, 'Types of EU Law' < https://ec.europa.eu/info/law/law-making-process/types-eu-law_en> accessed 19 November 2021
[20] GDPR, supra note 11, at Recital 10
[21] European Data Protection Supervisor, supra note 15
[22] GDPR, supra note 1, Article 99
[23] Ibid, Recital 4
[24] Ibid, Article 3
[25] Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR), a Practical Guide* (Springer 2017) 21

I.) Organizational and compliance requirements

In order to ensure, at a certain extent, that security and data protection are in place when data controllers and data processors act, the GDPR introduces the ideas of accountability and liability (Article 5 GDPR, Article 82 GDPR). This provision puts pressure on data controllers to plan their data processing activities more cautiously[26]. Moreover, the constantly present threat of liability forces data controllers to consider the consequences of failure and to abide by the data protection rules[27].

I.a.) Accountability

Whereas the 1995 Directive did not put its focus on accountability, Article 5 of the GDPR introduces the term of accountability, which obligates the data controller to comply with the requirements of the GDPR and it also imposes the burden of proof for the aforementioned compliance onto the data controller[28]. It is apparent that this provision creates a safety mechanism that contributes to the effective implementation of data protection principles[29].
The essence of the principle of accountability is consisted of the creation and the implementation by the controller of measures that are compliant with the GDPR[30], as well as the responsibility of the data controller to prove compliance with the requirements of the GDPR, upon request of Supervisory and Judicial Authorities[31]. In order to be compliant with the Regulation, the data controller, inter alia, must use "appropriate technical or organizational measures"[32].
For the implementation of the principle of accountability, the role of Data Protection Officer ('DPO'), which is introduced in Article 37 of the Regulation[33], is of vital importance, as the individual or a company that is appointed as a DPO is charged with the application of the relevant accountability tools (such as Data Protection Impact Assessments)[34]. According to Article 37 of the Regulation[35]the designation of a DPO is

[26] Aurelia Tamò-Larrieux, *Designing for Privacy and its Legal Framework, Data Protection by Design and Default for the Internet of Things* (Springer 2018) 96
[27] Ibid
[28] Voigt and von dem Bussche, supra note 25, at 31
[29]Article 29 Data Protection Working Party, [13 July 2010] Opinion 3/2010 on the principle of accountability <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf> accessed 17 November 2021
[30] Γιώργος Ν. Γιαννόπουλος, Λίλιαν Μήτρου, Γρηγόρης Τσολιάς Υποχρεώσεις του υπεύθυνου επεξεργασίας. in Λεωνίδας Κοτσαλής and Κωνσταντίνος Μενουδάκος (eds), *Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων (GDPR), Νομική διάσταση και πρακτική εφαρμογή* (Νομική Βιβλιοθήκη 2018) 173
[31] Voigt and von dem Bussche, supra note 25, at 32
[32] GDPR, supra note 11, at Art 5 para. 1 (f)
[33] Ibid, Article 37
[34] Γιαννόπουλος, Μήτρου και Τσολιάς, supra note 30, at 197
[35] GDPR, supra note 11, at Article 37

obligatory in three cases.[36] Let's imagine a rather simplistic scenario in the IoT universe where the appointment of a DPO would be mandatory according to GDPR:
Let's assume that a company established in the EU (or it could be established outside of EU as well, as the territorial scope of GDPR is very broad as it has already been stated previously) decides to launch a new smart watch in the market, the target audience of which, among others, is European Consumers. It is a rather known fact that smart watches (which are considered IoT devices), possess sensors that collect data relating to sensitive information[37] such as the heartbeat of the user. It is another known fact that by wearing the smart watch during the whole day, the device is able to collect significant amount of data relating to an individual user. These data are collected by the wearable device mainly in two ways. The first way is that the wearable collects the data and then it sends it either to the cloud or to a server on the Internet, with the aim to be saved for offline processing in future[38]. The second way reduces the amount of computing that is required by the wearable. To be more specific, in the second case the IoT device sends the collected data to the Internet for online processing and after the processing takes place the device receives some information that facilitate the operation of the device.[39]In this case, the constant presence of the wearable in the user's wrist, can be considered as 'regular and systematic monitoring of the data subject' according to Article 37 and hence the aforementioned imaginary company would be obliged by the GDPR to appoint a Data Protection Officer.

I.b.) Data Protection by Design and Default

Article 25 of the GDPR[40] introduces the term 'data protection by design and by default'. It is obvious, that given the importance of data protection as a matter, the safeguards provided in Article 25 of the GDPR are not entirely novel. In fact, just as Article 25 stipulates, Article 17 of the Data Protection Directive[41] when was in force used to oblige data controllers to implement appropriate technical and organizational

[36] (a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; (b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or (c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.
[37] Ben Zhang, Nitesh Mor, John Kolb, Douglas S. Chan, Nikhil Goyal, Ken Lutz, Eric Allman, John Wawrzynek, Edward Lee, and John Kubiatowicz, 'The Cloud is Not Enough: Saving IoT from the Cloud' (7th USENIX Workshop on Hot Topics in Cloud Computing, Santa Clara, California, 2016)
[38] F. John Dian and others, 'Wearables and the Internet of Things (IoT), Applications, Opportunities, and Challenges: A Survey' [2020] 8 IEEE Access 9
[39] Ibid
[40] GDPR, supra note 11, at Article 25
[41] 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/Article 17

measures in order to protect the data subject's data. Based on the requirements of this provision, the European Commission made an attempt to put the meaning of these measures into practice, by suggesting the use of Privacy Enhancing Technologies ('PETs')[42]which according to the Commission were *'a coherent system of ICT measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, all without losing the functionality of the information system*'[43]. However, these technologies generally, except for cryptography techniques, were not used as a primary source of system designing[44].

This very necessity of the protection of the data subject gave birth to the provision of Article 25 of the GDPR. The essential obligation set out in Article 25 is the implementation by the data controller of the appropriate measures and appropriate safeguards that lead to the effective protection of data subjects' rights and freedoms by design and by default.[45] Essentially, Article 25 relies on all the legal principles stipulated in Article 5 of the Regulation and is tightly linked to the accountability principle*('personal data shall be: a. processed lawfully, fairly and in a transparent manner, b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes, c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed, d. accurate and, where necessary, kept up to date, e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed and f. processed in a manner that ensures appropriate security of the personal data'[46]).* The Article does not specifically mention how these principles shall be achieved, however it explicitly states that for the implementation of the appropriate technical and organizational measures, state of the art must be taken into consideration and that is the reliance on industry standards.[47]Generally speaking, the term 'state of the art' must be translated as a dynamic and complex concept which should be assessed continuously by the data controller, as it continuously progresses and evolves[48]. It is also worth mentioning, that this obligation does not apply only to technical measures but also to organizational ones, such as the obligation of the controller to continuously train their employees on security matters, in order to protect more effectively the personal data of data subjects.[49]

In simple terms, data protection by design means that every system should be designed by its birth in a way that safeguards privacy and data protection principles right

---

[42]Commission (EC), 'on Promoting Data Protection by Privacy Enhancing Technologies (PETs)' (Communication) COM (2007) 228 final

[43] Ibid

[44] Γιαννόπουλος, Μήτρου και Τσολιάς, supra note 30, at 181

[45]European Data Protection Board, [20 October 2020] Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0 <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf> accessed 21 November 2021, 4

[46] GDPR, supra note 11, at Article 5

[47] Tamò-Larrieux, supra note 26, at 209

[48] European Data Protection Board, [20 October 2020], supra note 45

[49] Ibid

from the very start[50] and this design architecture should expand to the whole life cycle of this system.[51]. On the other hand, data protection by default simply means that the data controller should be held accountable for the implementation of settings that ensure the collection of data subject's data only to the extent that is necessary, while at the same time ensure the lawful nature of the processing of the amount of data retained, the period of retention, as well as the accessibility of the data subject to this data.[52]

I.c.) Data breach notification obligation

The GDPR introduces another novel requirement which is considered as a necessary step to safeguard the protection of individuals' personal data and that is the requirement of the notification of a personal data breach to the Supervisory Authority and in some instances to the individuals whose data were affected[53]. According to the opinion of the Article 29 data protection working party which issued in 2018 the revised 'guidelines on personal data breach notification under Regulation 2016/679', the novel notification requirement is in general quite advantageous and beneficial due to the fact that the controllers by notifying the Supervisory Authorities can receive a feedback from the Authority on whether or not it is deemed necessary to inform the affected individuals concerning the actual or a potential data breach.[54] Moreover, the notified individuals acquire knowledge regarding the safety status of their data and at the same time the data controller is obliged to implement all the necessary technical and organisational measures stipulated in Article 32 of the Regulation in order to make sure beforehand that the stored data is out of harm's way.[55] This diligent behaviour of the controller should not under any circumstances be taken for granted, given the fact that seldom do companies reveal to their clients incidents regarding data breaches.[56] According to Article 4 (12) of the Regulation '*personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised*

---

[50]European Commission, 'What does data protection 'by design' and 'by default' mean?' <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en> accessed 20 November 2021

[51]Ann Cavoukian, 'Privacy by Design The 7 Foundational Principles, Implementation and Mapping of Fair Information Practices' [2011]<https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf> accessed 24 November 2021

[52] European Data Protection Board, [20 October 2020], supra note 45

[53]Article 29 Data Protection Working Party, [Revised 6 February 2018] Guidelines on Personal data breach notification under Regulation 2016/67 <https://ec.europa.eu/newsroom/article29/items/612052/en> accessed 17 November 2021

[54] Ibid

[55] Ibid

[56] [56] Γιαννόπουλος, Μήτρου και Τσολιάς, supra note 30, at 221

disclosure of, or access to, personal data transmitted, stored or otherwise processed'.[57] Given the wording of the provision it is clear that it applies to all kinds of data breaches, whether they were caused out of negligence or were the result of intention.[58]

2.1.3.) Notification to the Supervisory Authority

According to Article 33 of the Regulation, the data controller, in case that a data breach has taken place, has the obligation to notify the Supervisory Authority without undue delay and when possible, within 72 hours after having become aware of the breach.[59] So, it is obvious that for the timeframe of the 72 hours to commence, the 'awareness' of data controller is of vital importance. The data controller should be regarded as 'aware' when based on its assessment, the compromise of data due to a security incident is highly likely.[60] An example of a situation where the loss of data would not be a very probable scenario would be the case where data is safely encrypted with a state-of-the-art algorithm, the decryption key is only available to the controller and this key was not compromised in a security breach[61]. However, even if this data was entirely safe from the risk of decryption by the malicious third party, if the controller did not create a backup, not only the Supervisory Authority should be notified, but the data subjects also, as they are negatively affected by this occurrence.[62]Article 33 para. 1 also stipulates an exemption to the general rule of the controller's obligation to notify the Supervisory Authority. According to paragraph 1 of the Article, the notification to the Supervisory Authority is not necessary when '*the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons*[63]*'.* However, should the controller choose not to notify the event of the breach to the Supervisory Authority, it must be certain that the actual risk for the data subjects is actually very low, as a breach of notification obligation comes with considerable fines.[64]

2.1.4.) Notification to the Data Subjects

Article 34 para. 1 of the Regulation stipulates that: '*When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay*[65]*'.* So, by the phrasing of this provision it becomes clear that even though the con-

---

[57] GDPR, supra note 11, at Article 4 (12)
[58] Voigt and von dem Bussche, supra note 25, at 65
[59] GDPR, supra note 11, at Article 33
[60] Article 29 Data Protection Working Party, supra note 53, at 11
[61] Article 29 Data Protection Working Party, [25 March 2014] Opinion 03/2014 on Personal Data Breach Notification <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf> accessed 17 November 2021
[62] Ibid
[63]GDPR, supra note 11, at Article 33 para. 1
[64] Voigt and von dem Bussche, supra note 25, at 68
[65] GDPR, supra note 11, at Article 34 para. 1

troller has the obligation to notify the Supervisory Authorities in case of a data breach with the exception that was stated above, if there is a high risk that puts in danger the rights and freedoms of natural persons, the data controller shall promptly communicate this data breach to the data subjects. The communication can be achieved by various means, such as direct messaging, or postal notification that include information regarding the data breach, as well as possible steps that need to be taken by the data subjects in order to protect their data, or at least minimize the danger.[66]

2.1.5.) Rights of data subjects

Besides the aforementioned organizational requirements laid down in the GDPR, the Regulation has incorporate various rights of data subjects that need to be respected by the data controller when they process the subjects' data. A thorough analysis of each right would exceed the scope of this dissertation, so only a few of these rights that play a crucial role in the IoT scheme shall be further analyzed.
The list of data subjects' rights that has been incorporated in the GDPR is exhaustive and it is set out in Articles 12-22 of the Regulation. The rights of the subjects against the processing of the data controller are the following:

a. Right to be informed (Article 12)
b. Right to access information (Article 15)
c. Right to rectification (Articles 16 and 19)
d. Right to erasure and right to be forgotten (Articles 17 and 19)
e. Right to data portability (Article 20)
f. Right to object to processing of personal data (Article 21)
g. Right to restriction of processing (Article 18)
h. Rights in relation to automated decision making, including profiling. (Article 22)

I.) Right to be informed (Article 12)

According to Article 12 of the GDPR the controller must take the necessary organizational measures that are capable of providing the data subjects with information in a concise, transparent, intelligible and easily accessible form, using clear and plain language.[67] This provision also enhances the principle of transparency that requires '*that any information addressed to the public or to the data subject* should *be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used'*[68]*.*
As far as the form of the communication concerned, it is not subject to a strict series of rules; however, the information provided to the data subject must take place before the activity of processing and it must include among other things both the legal basis of processing as well as its purposes[69]. The information provided to the data subject

[66] Article 29 Data Protection Working Party, supra note 53, at 20-22
[67] GDPR, supra note 11, at Article 12
[68] Ibid, Recital 58
[69] Voigt and von dem Bussche, supra note 25, at 143

prior to the processing activity must be in an easily accessible form, such as in writing or in the case when the communication has taken place via electronic means. When the communication has been made possible via electronic means, the Working Party of Article 29 recommends the use of layered privacy statements/notices when the controller operates a website[70]. Also, according to the Working Party, data controllers could also use along with the layered privacy statements, non-written electronic means such as IoT voice alerts.[71]
It is evident that in the world of IoT, this provision provides the data subject with very important safeguards and burdens the data controllers with quite heavy obligations.

II.) Right to access information and rights in relation to automated decision making, including profiling (Articles 15 and 22)

In Article 15, and going a step further of what it is stipulated in Article 12 of the GDPR, the legislator has provisioned a two-fold right of the data subject; to be more precise, using the power of the right to access information, the data subject has the right to be informed by the data controller regarding whether or not a processing activity has taken place and in the case that the answer is affirmative, the subject is given the right to demand certain information about the processing to be handed to it by the controller within a time period of 1 month after the request[72]. The list of information that the controller is obliged to hand over to the data subject is stipulated in Article 15 para. 1 of the Regulation. As long as the request of the subject concerned is reasonable and not excessive, the controller is obliged to provide the data subject with a copy of their personal data, free of charge. In case the data subject requests more than one copy, the procedure could become onerous and costly for the data controller and thus, the controller may charge a reasonable fee based on administrative costs.[73]
One of the information that the controller is obliged to provide to the data subject according to Article 15 para. 1 (h) of the Regulation concerns the existence of automated decision-making, including profiling. It has become increasingly evident that the rapid growth of IoT devices and the ability to communicate with each other, can lead to a collection of vast amounts of data related to the data subject/user of these devices and thus facilitates the creation of a profile for the user that is strongly connected to their behavior and its habits and also a profile that can lead to a prediction of the future steps of the individuals concerned. This can generate, as it will be explained in Chapter 3, various problems regarding both privacy of the individuals concerned as well as a risk of loss of one's identity.
Profile does not necessarily overlap with automated decision making. For the first to take place, the latter is a prerequisite, as it can be safely assumed reading the provi-

[70] Article 29 Data Protection Working Party, [Revised 11 April 2018] Article 29 Working Party Guidelines on transparency under Regulation 2016/679 < https://ec.europa.eu/newsroom/article29/items/622227/en> accessed 17 November 2021, 10
[70] Ibid
[71] Ibid, 11
[72] Voigt and von dem Bussche, supra note 25, at 150
[73] GDPR, supra note 11, at Article 15 para. 1

sion of Article 4 of the Regulation, whereas the latter (automated decision making) does not always lead to a profiling activity. For example, should a speeding camera installed in the street imposes fines based only on speeding evidence, this activity consists an automated decision (it uses technological means to draw conclusions without human involvement), but it does not consist a profiling activity[74]. Moreover, the activity of automated decision making, including profiling, is lawful if it is compatible with data protection principles of Article 5 and with the lawful bases of processing stipulated in Article 6. However, when processing of sensitive data takes place, the data processing can lawfully take place inter alias, on the condition that the data subject has given its explicit consent[75]. But is this enough? More about consent shall be discussed later on, in par. 2.1.6. and in Chapter 3.

2.1.6.) Legal bases for data processing in the IoT scheme

So far, the most important rights of data subjects in the IoT environment that are stipulated in the GDPR have been mentioned and briefly assessed. In this paragraph, the focus will shift on a very quick examination of the most crucial legal bases under which the processing of personal data in the IoT scheme can be lawful.

I.) Contractual necessity

A first legitimate base of processing is that of contractual necessity, stipulated in Article 6 para. 1 (b) of the GDPR[76]. However, it should be noted that the scope of this provision is narrow as it requires the existence of a causal link between the activity of processing and the performance of the contract expected by the data subject.[77] Due to the very nature of IoT devices, which tend to gather large amounts of data some of which cannot be considered necessary for the contractual performance, this basis cannot be used frequently in a lawful manner by the data controller[78].

II.) Legitimate interests of the controller

Article 6 para. 1 (f) of the GDPR states that a processing activity can take place if it is in the legitimate interests pursued by the data controller or another third party.[79] This

---

[74] Article 29 Data Protection Working Party, [Revised 6 February 2018] Article 29 Working Party Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 <https://ec.europa.eu/newsroom/article29/items/612053/en> accessed 17 November 2021, 8

[75] GDPR, supra note 11, at Article 9

[76] GDPR, supra note 11, at Article 6 para. 1 (b)

[77] Article 29 Data Protection Working Party, [16 September 2016] Opinion 8/2014 on the Recent Developments on the Internet of Things < https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf> accessed 25 January 2022, 15

[78] Voigt and von dem Bussche, supra note 25, at 241

[79] GDPR, supra note 11, at Article 6 para. 1 (f)

basis of processing, along with contractual necessity, may be used lawfully in few occasions, as most of the time the risks posed in the fundamental rights of data subjects (many of which will be analyzed in Chapter 3) as a result of the pervasive nature of IoT, override the legitimate interests of the controller.[80]

III.) Consent

The third and final basis of data processing in the IoT environment, and the most frequently used one, is consent[81]. As the other two previously mentioned bases of lawful data processing could end up fruitless, data controllers rely more and more on consent. More about consent will be mentioned in Chapter 3, but it is critical to remember that consent must be explicit, *'freely given, specific and informed'*[82], inter alias, in order to be considered valid[83].

2.2.) Cybersecurity Act

In 2019 the Cybersecurity Act was put into force. The Act, recognizing that the lack of security by design features in IoT devices poses a great risk for cybersecurity[84], introduces a voluntary cybersecurity certification framework, which enables the creation of risk-based EU certification schemes[85] for categories of products. The intended purpose behind the creation of the certification framework is two-fold[86]; on the one hand, it is believed that its implementation should increase the trust of the consumers in the IoT and ICT devices and on the other hand, its use avoids legal fragmentation within the Union, as some Member States have already implemented certification schemes, which are not however recognized in other Member States.[87]

Each Certification Scheme has the objective inter alia to '*protect stored, transmitted or otherwise processed data against accidental or unauthorized storage, processing or disclosure during the entire life cycle of the product'*[88] and to ensure that '*products are secure by default and by design*[89]*'.* ENISA is burdened with the task of drafting and preparing the requested by the Commission Certification Schemes[90]. According to the Cybersecurity Act, the Regulation also provides European Commission with the option

[80] Article 29 Data Protection Working Party, [16 September 2016], supra note 77, at 15
[81] GDPR, supra note 11, at Article 6 para. 1 (a)
[82] Ibid, Recital 32
[83] Ibid, Article 4 (11)
[84] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) [2019] OJ L 151/Recital 2
[85] European commission (*Questions and Answers - EU Cybersecurity*) <https://ec.europa.eu/commission/presscorner/detail/en/QANDA_19_3369> accessed 23 November 2021
[86] Cybersecurity Act, supra note 84, at Recital 69
[87] Ibid, Recital 67
[88] Ibid, Article 51
[89] Ibid
[90] Ibid, Article 48

to assess whether or not the implementation of a certification scheme should become mandatory.[91]

2.3.) Conclusion on the existing legislation concerning IoT

From the above mentioned, it becomes apparent the current EU legal framework, covers a relatively big fraction of IoT operations;the GDPR is a very powerful tool aiming at the protection of data from potential misuses and the Cybersecurity Act makes a step towards the implementation of certifications that depict certain technical requirements of products placed in the european market. However, a security by design approach in terms of an obligatory practice for the IoT manufacturers is not provisioned in the legislation that is into force and the option given to the Commission by the Cybersecurity Act, that is to make a certification scheme mandatory, cannot be considered as a ground that can provide legal certainty as far as security by design is concerned. So, having all of the aforementioned in mind, in Chapter 4, security-oriented legislative EU instruments, that are not currently in force, will be mentioned and assessed.

[91] European commission (Questions and Answers - EU Cybersecurity), supra note 85

Chapter 3 Security: An ambiguous notion

It can be seen in our everyday lives, that throughout the duration of our day, IoT is everywhere and is always present. The consequence of this reality is that constantly our privacy and our data are under challenge and under threat. The preservation of our personal information and of our personal sphere in general, rely heavily, in almost every scenario on one common denominator: security. In this Chapter the three-fold nature of security in relation with data protection and privacy will be analyzed. Even though this dissertation has the main aim to address the 'hot potatoes' arising out of the relationship between security and data protection, it is important to also include privacy in this conversation, as inevitably a damage dealt to the principle right (privacy) directly affects its manifestations (data protection).

3.1.) Security as a moral enabler

Security is without a doubt the biggest challenge in relation to the IoT scheme[92]. It is indeed a rather heinous task for any scholar or lawmaker to effectively give a satisfying and convincing definition to the term 'security', as a catch-all phrase describing security cannot be possibly capable of capturing all of its delicate nuances. In fact, 'security' can mean a lot of different things. It could be considered as a synonym to one's safety[93]from immediate or potential harm, thus it could take the form of a fundamental human right. It could also be disguised as a moral enabler[94].
Concerning the latter form that security can possibly take, it is a commonly expressed notion by some scholars that the successful protection of data and privacy requires an ex-ante existence of the necessary security guarantees[95]. Going a step further and introducing morality into the debate, a very interesting theory has been developed by Professor Floridi which has been further elaborated in various papers and books of his. According to this theory, an effective way to achieve good governance in a democratic society is the existence of a durable chain that ties rules and procedures with mean-

[92] Giorgio Chiara, 'The Balance Between Security, Privacy and Data Protection in IoT Data Sharing: A Critique to Traditional "Security & Privacy" Surveys' [2021] 7(1) European Data Protection Law Review <https://edpl.lexxion.eu/data/article/16985/pdf/edpl_2021_01-007.pdf> accessed 29 November 2021

[93] Commission (EC), 'Communication from the Commission to the European Parliament, the European Council, the Council, The European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy' (Communiaction) COM (2020) 625 final, 1

[94] Luciano Floridi, *The Ethics of Information* (Oxford University Press 2013) 273

[95] Bernd Carsten Stahl, 'Privacy and security as ideology' [2007] 26(1) IEEE Technology and Society Magazine, 38

ings, values, and ideas[96]. These procedures are given the name of 'infra-ethics', which in reality are the infrastructures that facilitate or hinder morally positive values[97] from taking place. For example, truth (even though this example is highly debatable, as some philosophers like Immanuel Kant would completely disagree with this statement) might not have an intrinsic moral value on its own but can facilitate the building of love in a human relationship. So, it is clear that in order for the good governance that Floridi talks about to occur, a combination between the facilitators (infra-ethics) and the morally good values (e.g., love) needs to be attained.[98]

3.1.1.) Moral theory in practice

To put this theory in the context of security and data protection within the IoT scheme, security can be seen as having an instrumental role and acting as a steppingstone for data protection to be enjoyed.[99] A critical facilitator to the enjoyment of the right of privacy and data protection is the existing legislation. More specifically, for instance the existence of the obligation stipulated in Article 33 of the GDPR, which has been analyzed above, that forces the controller to notify the Supervisory Authority and then is some instances subsequently the data subject in cases where a breach has happened or is likely to happen, definitely operates as a security precondition for the enjoyment of data protection, as the attainment of the morally positive fundamental right could not have possibly become reality if the safety provision of the Regulation had not existed or had not been put into effect yet. Moreover, one of the basic principles introduced in the GDPR that needs to be attained by the data controller, is data minimization. Data minimization means that the controller should collect only the data that is absolutely necessary for the accomplishment of the agreed purpose of processing. This basic principle is of crucial importance as it hinders, at a certain extent anyway, the accumulation of huge amount of data and thus it aids in the reduction of risk of data loss, data breach or even data distortion. This is also true for the purpose limitation principle introduced in Article 5 para. 1 (b) of the GDPR[100], as its function is to prevent inter alias the use of data collected by the data controller for other purposes than the ones initially agreed upon by the parties.[101]

Aside from the GDPR, as it has already been mentioned in Chapter 2, Cybersecurity Act Regulation of 2019 has been designed with the objective to enhance cybersecurity[102], by introducing inter alias a voluntary certification framework.[103] Should the Cybersecurity Act contributes significantly to the enhancement of security it remains to be seen, however it is evident that its purpose is to operate as a legislative infrastructure that

---

[96] Massimo Durante, *Ethics, Law and the Politics of Information: A Guide to the Philosophy of Luciano Floridi* (1nd edn, Springer 2017) 176

[97] Floridi, supra note 94

[98] Ibid

[99] Durante, supra note 96

[100] GDPR, supra note 11, at Article 5 para. 1 (b)

[101] Article 29 Data Protection Working Party, [16 September 2016], supra note 77, at 16

[102] Cybersecurity Act, supra note 84, at Recital 2

[103] European commission, 'The EU cybersecurity certification framework' <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework> accessed 2 December 2021

makes the data protection and privacy of European citizens a more realistic scenario and therefore it operates as an 'infra-ethic'.

3.1.2.) Technical security as a moral enabler

However, aside from the aforementioned, security, can also be viewed from a purely technical standpoint. Nissenbaum argues[104] that the technical nature of security has a three-fold objective, that remains mainly unphased from the rapid technological evolvement and the constant changing of needs: that is a. to keep networks and communications available to all users by keeping viruses and malwares away of their operating systems, b.to keep personal information stored inside the devices uncorrupted and c. to keep this information confidential.[105] So, by using technical security features in order to achieve a morally positive end goal, that is the protection of one's operational system and data[106], technical security takes also the form of the moral enabler-facilitator and operates as an infra-ethical infrastructure.

3.1.3.) The 'art' of obfuscation

Another very interesting and quite clever way that acts as a moral enabler, is the method of data masking called 'obfuscation', that was coined by Brunton and Nissenbaum. 'Obfuscation' is essentially '*the production of noise modeled on an existing signal in order to make a collection of data more ambiguous, confusing, harder to exploit, more difficult to act on, and therefore less valuable.*'[107] So, in simpler terms, we could say that 'obfuscation' is the method of multiplying your existing digital tracks, in order to make their tracking more burdensome a task for the potential tracer. This technique, even though it still relies on the use of a third-party software program, is nevertheless a viable alternative for individuals who do not possess the necessary means to hide their data in other ways (e.g. using strong encryption) and by themselves.[108] So, 'obfuscation' and the decoy it creates, have an instrumental value in building the necessary ground for an enhanced privacy and thus a stronger defense against unproportionate collection of data, as well as data misuse.

3.2.) Security as an ethical value

Security, as it has been pointed out above, can take the form of the moral enabler that facilitates the establishment of privacy and the enhancement of data protection. How-

---

[104] Helen Nissenbaum, 'Where Computer Security Meets National Security' [2005] 7 (Ethics and Information Technology), 63
[105] Ibid
[106] Ibid, 65
[107] Finn Brunton and Helen Nissenbaum, *Obfuscation A User's Guide for Privacy and Protest* (The MIT Press 2015), 46
[108] Ibid, 55

ever, in its most common form, security can be considered as an ethical value colliding directly with the relative fundamental rights of privacy and data protection[109].

3.2.1.) The State as a 'Big Brother'

Undoubtedly, the intervention of State in today's society, that takes the form of surveillance or intelligence[110], creates new problems regarding the equilibrium between security and privacy, as sometimes it puts both the notion of privacy as well as data protection into question.
It is a fact that in the digital era, privacy cannot be taken for granted. Especially outside of one's home (and assuming that the user's IoT devices and sensors installed inside their houses are not spying on them), there is surveillance everywhere, from the city's highways to supermarkets and ATM machines. Of course, in the context of the intervention of State and law enforcement into the lives of civilians, the attack on privacy is in a certain extent justified, due to the exponentially increase in the risk of IoT device and technology misuse by malicious third parties. However, this intervention is often unproportionally intrusive and sometimes deleterious. In these situations, privacy ceases to concern only individuals but at the same time it adopts a rather collective nature. This approach seems to agree with the view that generally privacy is the constitutive element of any civil society[111] and it is not an individual right.

I.) Relevant Case law from the USA

It is known that eavesdropping and visual surveillance have always been frowned upon. From 'Peeping Tom' laws implemented in USA States like South Carolina[112], to 1862 Californian legislation banning wiretapping[113], such practices of severe intervention are considered illegal internationally. Generally speaking, the Courts of the USA have adopted an interesting approach towards privacy, highlighting the difference between privacy at an individual's personal place and privacy in public places. In the Case of United States v. Knotts, the Minnesota law enforcement authorities had reasonable suspicions that an individual was purchasing containers of chloroform, in order to use it as an ingredient for the production of an illegal drug product. For this reason, they decided to frame this individual by placing a radio transmitter inside a container that was sold to him and then by receiving the signals of the transmitter (the container was in the back of his car), the digital traces led them to his illegal laboratory. The US Supreme Court held that this action was legal, and the Fourth Amendment could not be invoked in this case, as the signals that were received by the authorities originated from his automobile which was travelling on public roads and for these reasons the

[109] Chiara, supra note 92, at 24
[110] Ibid
[111] Julie Cohen, 'Examined Lives: Informational Privacy and the Subject as Object' [2000] 52 Stanford Law Review, 1397-1398
[112] Daniel J. Solove, 'A Taxonomy of Privacy' [2006] 154(3) University of Pennsylvania Law Review, 491
[113] Ibid, 492

individual could not have a reasonable expectation of privacy in his movements[114]. It is sensible to assume from the aforementioned stance of the court that the same approach would have been applied for every sensor and/or camera installed in public places, as the individuals would always kept in their minds that their actions are not private. From the analysis of this Case, it becomes apparent that even if this action implemented by the law enforcement could be seen as justifiable, is nevertheless the result of the existence of great asymmetry of power between government and civilians, as the latter have no real option of opting out of the surveillance.[115] Moreover, to some it may seem that surveillance ,whether it is justifiable or not, is a fundamentally problematic concept, as it clearly demonstrates the absence of respect towards the autonomy of the individual.[116]

II.) Relevant Case law from EU

On the other hand, the European Union traditionally has held a more friendly stance concerning the rights of civilians against State interference, data collection and monitoring; in the very recent Case C-140/20[117], the Advocate General Campos Sánchez – Bordona expressed the opinion that the EU legislation precludes national legislation from obligating providers of publicly available electronic communications services to retain in a general manner inter alias the traffic and location data of end users, unless there were legitimate reasons of national security. So, the Advocate General in this situation, made a balancing exercise between the interests of State and the personal data and privacy of the individual and by applying the legal tool of proportionality among other, held that the general retention of such personal data was very onerous comparing to the goal that it aimed to achieve. Another Case that illustrates the collision between security and data protection is the Decision 254/2021[118] of the Greek Supreme Court. The case concerned an individual that attempted to set a car on fire and was caught by the CCTV system that was installed in the garage of an apartment situated in a street nearby. The Court held that the law enforcement is allowed to use the video surveillance footage in order to prove the offence, as there no other less stringent means of proof available and because of the fact that the illegal activity took place in public space and therefore it could not be considered as private. Moreover, to reach this Decision, the Court made a balancing exercise between the defendant's right of personal data protection and the victim's right of access to justice which would be jeopardized in the case that the use of the CCTV footage was considered illegal. The Court held that the defense of the right to access to justice was more important than the respect of the defendant's personal data.

---

[114] United States v. Knotts, 460 US 276 (1983)
[115] Brunton and Nissenbaum, supra note 107, at 53
[116] Solove, supra note 112, 494
[117] Case C-140/20 G.D. v The Commissioner of the Garda Síochána, Minister for Communications, Energy and Natural Resources, Attorney General, Opinion of AG Campos Sánchez – Bordona para. 82
[118] Areios Pagos (A.P.) [Supreme Court] 254/2021, Criminal Law, (Greece)

3.2.2.) Future plans of the EU regarding monitoring

Aside from the existing legislation, the European Union is aiming at strengthening both the State and law enforcement intervention even more. A characteristic example of this is a proposal made by the Commission concerning the creation of a network of Security Operation Centers that will be responsible for monitoring communication networks and with the aid of Artificial Intelligence ('AI'), it will be able to identify threats.[119] At a first glance, this approach adopted by the Commission seems reasonable, as the fast paced development of technologies including IoT, require the adoption of an equally fast and responsive defensive mechanism. However, it should be carefully planned which criteria will be used in order to assess the severity of a threat and also how much data shall be processed and monitored, as it becomes rather obvious that such a strong intervention besides its potential benefits, can also become an excuse for unproportionate and unjustified constant surveillance of citizens.

Another goal of the European Union is to create an action plan, in order to expand at an EU and national level the capacity of law enforcement to investigate cases linked to cybercrime[120]. This proposal comes with the guarantee of the European Commission that the plan will '*fully respect fundamental rights and will pursue the required balance between various rights and interests.'*

3.2.3.) Surveillance in the field of employment

Up until this point, security has only been analyzed concerning State intervention and surveillance. However, another rather common form of surveillance can originate from other sources as well, such as the work environment. In the USA, many companies use advanced IoT systems that monitor their employees and generate lots of data about them (including highly sensitive data). Monitoring systems like HyGreene are based on Radio Frequency Identification ('RFID') technology and help hospitals to gain information on the exact time and frequency that the employees wash their hands.[121] The rationale behind the creation of such system is the minimization of risk of safety protocol violation by the employees that treat patients, although it becomes apparent that it needs to be carefully examined whether or not such a vast processing of personal data is proportionate to the respective aim. Another technology that is very commonly used within the working environment are sensor and tracking devices. Many companies, and especially those which operate large fleets, have installed in the automobiles operated by their employees, tracking sensors that are able to pinpoint to the car's exact location, to determine its exact speed, air temperature etc. Of course, this technology does not only collect data concerning the automobile but indirectly also regarding its operator by determining inter alias their driving behavior[122]. The

[119] Commission (EC), 'The EU's Cybersecurity Strategy for the Digital Decade' (Joint Communication) JOIN (2020) 18 final, 6-7
[120] Ibid, 15
[121] Scott R. Peppet, 'Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent' [2014] 93 Texas Law Review, 112
[122] Ibid

Greek Data Protection Authority ('DPA') has tackled this tracking device problem in the Decisions 162/2014, 163/2014 and 165/2014. According to the Greek DPA, the legality of the installation of a geo-locating system inside the automobile of an employee is dependent upon the existence of several prerequisites. First of all, the car must follow a predetermined route which is taking place during working hours. Secondly, the data retention period should be in accordance with the GDPR, and in any case its duration should not exceed 1 month. Thirdly, the data controller must ensure that they have implemented all the necessary technical and organizational measures, in order to keep the employees' data secure (e.g. the use of encryption). Finally, the purpose of tracking must be the amelioration of the predetermined itinerary and not the surveillance of the employee[123]. The stance of the Greek DPA is very well reasoned, as on the one hand it facilitates the better functioning of the company while at the same time makes clear that the surveillance of the employee besides what is necessary for the attainment of the amelioration of the itinerary will not be justified. However, unfortunately, common practice has shown that companies constantly generate new ways of monitoring indirectly the behavior of their personnel.
Having analyzed the above nuance of security, when it clashes directly with other relative fundamental rights, it becomes clear that the finding of the right balance still remains a rather heinous task.

3.3.) An anthropocentric take on security

3.3.1.) Consent: A controversial notion

Security, besides the definitions stipulated above, can also take a third form; More specifically, it can take a more anthropocentic approach and be defined as *'the protection of the conditions for the enjoyment of goods against the threat of dangers that may be subject of anticipation and calculation'*[124].This 'anticipation' and 'calculation' are provided by the legislation, as the main instrument of data protection, the GDPR, has laid down an exhaustive list of grounds as it has been stipulated above, only under which data processing is lawful. Consent is a very important legal basis, but a controversial one as well. According to Article 4 of the GDPR[125], the consent of the data subject is a *'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.'* Freedom that constitutes an indispensable element of the definition of consent, is essentially the possibility of the data subject to have a real choice if he/she wishes to consent or not and the possibility to reject or accept certain terms without this choice having a nega-

[123] Greek Data Protection Authority 'Annual Report' (2014) <https://www.dpa.gr/sites/default/files/201909/ANNUAL_2014_V2.0_WEB_VIEW.PDF> accessed 15 December 2021 97-98
[124] Massimo Durante supra note 124, 372.
[125] GDPR, supra note 11, at Article 4

tive impact[126]. The latter is often the case in the field of employment, as the great imbalance of power that exists between the employer and the employee, often forces the latter to proceed to actions they never intended to, due to the indirect pressure that is put upon them by the former.[127] Such Case is that of the popular brand 'H&M'.[128] The Hamburg Commissioner for Data Protection and Freedom of Information imposed a huge fine (around 35 million euros) to the H&M Service Center, as it was found out that the company kept stored huge amounts of data concerning detailed information about employers' private lives.

Also, regarding consent, the French Data Protection Agency, imposed a 150 million euros fine to Google[129] and a fine of 60 million euros to Facebook. According to the rationale of the decision, the two companies failed to comply with the GDPR and with the relevant provisions of the French legislation, as they provided the end-users with the option to accept relevant cookies with just a click of a button, but they did not provide them with the equivalent alternative to reject them. According to the French Data Protection Agency, the intention of the end-users to quickly visit the webpages of the said companies, may influence their decisions in favor of the acceptance of cookies.[130] In another Case[131], the Norwegian Data Protection Authority concluded that the app Grindr had violated the legal bases of data processing that are stipulated in the GDPR, as it disclosed activities of the end-users to third parties (for behavioral advertisement) without having preciously acquired a legal basis for data processing. Also, the Authority found out that due to the very specific nature of the app (mostly used as a dating app for people of specific sexual orientation), the transferred data made the identification of the user's sexual orientation very easy and the revealing of such information required the explicit consent of the users, as it is considered as sensitive data under the GDPR.

---

[126] Article 29 Data Protection Working Party, [adopted 10 April 2018] Guidelines on consent under Regulation 2016/679
< https://ec.europa.eu/newsroom/article29/items/623051> accessed 29 December 2021, 5

[127] Ibid, 7

[128]European Data Protection Board, 'Hamburg Commissioner Fines H&M 353 Million Euro for Data Protection Violations in Service Centre' (2 October 2020) <https://edpb.europa.eu/news/national-news/2020/hamburg-commissioner-fines-hm-353-million-euro-data-protection-violations_en> accessed 17 December 2021

[129]Commission Nationale Informatique & Libertés, 'Cookies: the CNIL fines GOOGLE a total of 150 million euros and FACEBOOK 60 million euros for non-compliance with French legislation' (-, 6 January 2022) <https://www.cnil.fr/en/cookies-cnil-fines-google-total-150-million-euros-and-facebook-60-million-euros-non compliance> accessed 10 January 2022

[130] Ibid

[131]European Data Protection Board, 'Norwegian DPA imposes fine against Grindr LLC' (13 December 2021) <https://edpb.europa.eu/news/national-news/2021/norwegian-dpa-imposes-fine-against-grindr-llc_en> accessed 5 January 2022

3.3.2.) Pre-emption and the absence of complete safeguards

Generally speaking, whether having the end-users' consent or not as it was illustrated in the Cases above, companies having acquired information about individuals, 'feed' their algorithm-based machines with it, in an effort to gain a competitive advantage and potentially maximize their revenue and their market share. This common practice of profiling generates very grave hazards for the human being, as it infers directly inter alia with his/her personality and identity.

Many data-collecting machines, operate without supervision, as they have been created with the purpose of collecting huge amounts of data and then find patterns that are not visible to the human eye.[132] Often, and especially in the IoT scheme, the collected data is the result of the co-existence of multiple sensors (e.g., accelerometer, gyroscope, magnetometer). This phenomenon is called 'sensor fusion' and essentially has as a result the finding of data which it would not have been possible if there was just one data source.[133] The algorithms under which the collection of the data is based, are biased by design due to the fact that they are designed to follow certain steps in order to reach to a conclusion, while omitting other alternative steps/paths.[134] The problems generated with their method of approach are various. For instance, it is a fact that humans when they are aware that are spied on, may behave differently that they normally would;[135] they might make choices that do not respond to their personality and maybe they follow paths that the majority of others would take, in an attempt not to be criticized by the 'Big Brother' for adopting a 'black sheep' attitude and not following the herd. The machines that collect the data handed to them by the consenting individuals, assess and interpret it based on a quantitive analysis of the individuals' interactions with the digital environment of the online world[136]. Given these facts, it becomes evident that in the process of data interpretation there is always a great risk of error, because even though interpretation and decision-making that is based on data aggregation may be efficient, the end result could be very distant from reality.[137] The likelihood of false interpretation of data creates a chain reaction to other critical aspects of life, such as employment. Employers, in an effort to assess the qualifications of a candidate, can gain access to huge amounts of data concerning the particular individual[138] (as it was previously shown in the H&M Case). For example, a gym when interviewing various candidates, it may ask them to provide it with sensitive information related to their sleeping patterns, fat percentage etc. The algorithmic interpretation of the requested data, could create a discriminatory/biased or false profiling of the candidate, thus costing him/her the position. This is one of the main inherent risks of the

---

[132] Hildebrandt, supra note 10, at 24

[133] Kaivan Karimi, 'The Role of Sensor Fusion and Remote Emotive Computing (REC) in the Internet of Things' <https://www.nxp.com/docs/en/white-paper/SENFEIOTLFWP.pdf> accessed 10 January 2022

[134] Hildebrandt, supra note 10, at 34

[135] Cohen, supra note 111, at 1426

[136] Hildebrandt, supra note 10, at 25

[137] Daniel J. Solove, *The Digital Person, Technology and Privacy in the Information Age* (NYU Press 2004) 44-47

[138] Peppet, supra note 121, at 123

so called 'pre-emptive' computing.[139] So, as individuals are subject more and more to decisions made by Artificial Intelligence ('AI') agents, the need of decision transparency and of legal grounds to challenge these decisions becomes vital.[140] In an effort to regulate the profiling and the automated decision making, GDPR in its definition of 'consent' sets the requirement that consent must be 'informed'.[141] So, the data subject should be informed inter alia about the identity of the data controller, the purpose of data processing, the existence of the right of consent withdrawal and regarding the existence of automated decision making.[142] In Article 22 para. 3 of the Regulation is stipulated that *'the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision'.* Such provision according to Wachter, Mittelstadt and Floridi [143]may offer the right to the data subject to obtain the intervention of human and to object his/her decision, but it does not explicitly provide it with the possibility of an ex-post explanation regarding the functionality of the algorithmic system and the rationale of the final decision.[144] Indeed, the possibility of an explanation regarding the decision making is given only in Recital 71 of the GDPR[145], but as it has been already seen in the relevant EU Case law, Recitals are not legally binding, but they provide a guidance that aids in the implementation of the Articles.[146]

3.3.3.) Hildebrandt's take on personal safety

But the future may be more ominous than the present. With the objective to illustrate the dark future of pre-emptive profiling on the security of the individual, Hildebrandt created a futuristic example (based on which the example in the introduction was written), in which individuals before taking any action always consult their digital personal assistants, which are devices resembling humans that aid them in their daily activities and decision-making, while their creation, life and motives are sponsored by companies, such as banks, employers and insurance companies.[147] In this rather terrifying example, the machine constantly profiles its environment and the individual and tries to pre-empt the user's intentions before even he/she becomes aware of them. Moreover, and sharing the concerns of Hildebrandt, European Commission has highlighted the need for the adoption of safeguards in the IoT environment as it has forethought the

[139] Hildebrandt, supra note 10, at 8
[140] Commission (EC), 'WHITE PAPER On Artificial Intelligence - A European approach to excellence and trust' (Communication) COM (2020) 65 final, 13
[141] GDPR, supra note 11, at Article 4 (11)
[142] Article 29 Data Protection Working Party, [adopted 10 April 2018], supra note 126, at13
[143] Sandra Wachter and others, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' [2017] 7(2) International Data Privacy Law, 79
[144] Ibid
[145] GDPR, supra note 11, at Recital 71
[146] Wachter and others, supra note 143, at 80
[147] Hildebrandt, supra note 10

danger of the creation of a world where humans do not longer roam the world freely but are enslaved to the decisions of machines.[148]
So, as it becomes clear, the uncontrollable flow of data, our 'consensual' sharing of data and our need to make our lives more carefree and comfortable, often at the expense of our own private identity, predict questionable fate for humankind. Of course, IoT plays a vital role in this trend, as within the IoT scheme the exchange of information between devices is rather easy and rapid.

[148] Commission (EC), 'Advancing the Internet of Things' (Staff Working Document) SWD (2016) 110 final

Chapter 4: The future of the balance exercise between security and data protection in the IoT scheme

So far, a quick yet concise introduction has been made on what exactly is IoT. Then, this dissertation proceeded with the illustration of the relevant current legal framework in the EU that governs the function of IoT devices inter alia and in Chapter 3 a distinction was made as far as the definition of the term 'security' is concerned and it was concluded that it is a rather controversial term with an ambiguous meaning. However, it was pointed out that it can be primarily seen as having a three-fold dimension; a. it can function as an infrastructure that facilitates a morally positive value from taking place, b. it may collide directly with other relative fundamental rights, or c. it may be more of a human-centered concept and concern the prevention of calculated and anticipated dangers throughout the life of an individual. This Chapter will put its focus on a proposed EU Regulation and on an adopted EU Delegate Act, both concerning the IoT governance and the impact that their implementation could have on the balance of the three-fold dimension security and data protection. Lastly, a final conclusion shall be made concerning the future of the balancing exercise between security and data protection.

4.1.) E-Privacy Regulation

In 2017 and in response to the great increase in the use of IoT devices, the European Commission proposed a Regulation[149] that governs the privacy in electronic communications and repeals the E-Privacy Directive ('ePD') that is still in force today. This action was primarily initiated by the need of the European legislator to create a more legally certain environment by adapting to rise of new technologies and to make the scope of application of the Regulation more unambiguous than the one existing under the ePD, as nowadays a blurring of the roles of network and communication providers is observed[150], making the existence of a clear scope of application crucial. Moreover, it remains unclear to which extend the ePD applies to IoT, and thus it becomes apparent that an immediate need for clarification is vital. The proposed Regulation makes clear that its application shall also be extended to the IoT scheme. In particular, Recital 12 of the Regulation explicitly states that the Regulation *'should apply to the transmission of machine-to-machine communications'.*[151] Moreover, the Regulation aims to enhance the protection of the end-users' terminal equipment. According to Article 1 of the 2008/63/EC Directive[152], terminal equipment is the *'equipment directly or indirectly*

[149] Commission (EC), '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)' (Communication) COM (2017) 10 final

[150] European Data Protection Supervisor, [22 July 2016] Opinion 5/2016, Preliminary EDPS Opinion on the review of the ePrivacy Directive (2002/58/EC), 10

[151] Commission (EC) Regulation Proposal, supra note 149, at Recital 12

[152] Commission Directive 2008/63/EC of 20 June 2008 on competition in the markets in telecommunications terminal equipment [2008] OJ L 162, Article 1

connected to the interface of a public telecommunications network to send, process or receive information'. In practice, the storage of information and the processing of information by the third parties in the terminal equipment of the end-users shall be allowed by the Regulation primarily under the legal basis of consent (Article 8 of the E-Privacy Regulation), as it has already been defined in the GDPR. Additionally, in order to create safeguards for the efficient protection of the end-users' data, the E-Privacy Regulation contains a provision that obliges the software providers (e.g., web browsers), to make a configuration to their software in the way that it prevents third parties from storing and process/retrieve information about users and their terminal equipment (Recital 23 and Article 10 of the E-Privacy Regulation). So, it becomes evident that the E-Privacy Regulation, by operating as lex specialis[153] to the already established GDPR, shall provide additional safeguards as far as security and data protection of the end user/data subject is concerned.

4.2.) Radio Equipment Directive

In 29.10.2021 a Delegated Act[154] was adopted by the European Commission, concerning the improvement of cybersecurity of IoT devices. The Delegated Act (with which the industry shall comply with until 2024) supplements the Radio Equipment Directive of 2014[155], the aim of which is the establishment of a regulatory framework that enables radio equipment to be placed in the European market.[156]Due to the fact that the current legislative framework does not guarantee the security safety of the IoT devices that enter the market, the Commission decided via the Delegated Act to '*incorporate safeguards to ensure that personal data and privacy'*[157] of internet-connected devices (including wearables) are protected. This development has a two-fold importance; on the one hand, the Directive will aid in the enforcement of the GDPR, as it will oblige manufacturers to comply with certain safety requirements in order to place their product in the European Market, thus security by design will be a must and on the other hand, all the provisions of the Delegated Act shall be directly applicable to all

[153] Commission (EC) Regulation Proposal, supra note 149, at Explanatory Memorandum, 1

[154] Commission Delegated Regulation (EU) 2022/30 of 29 October 2021 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of that Directive [2021] OJ 2 7

[155] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC [2014] OJ 2 153

[156]European Commission, 'Radio Equipment Directive (RED)' (*Internal Market, Industry, Entrepreneurship and SMEs*, -) <https://ec.europa.eu/growth/sectors/electrical-and-electronic-engineering-industries-eei/radio-equipment-directive-red_en> accessed 17 January 2022

[157] Delegated Regulation, supra note 154, at Recital 11

Member States, as the Act takes the form of a Regulation[158] and thus harmonization and legal certainty will be increased. It is evident that the aforementioned legislative approach of the EU, functions both as an infrastructure for the enjoyment of data protection, as it creates safeguards for the protection by design of the IoT devices and also it creates an additional barrier that prevents the misuse of data subject's data.

4.3.) The future of the balance exercise

I.) The effectiveness of European legislation

We have analyzed so far the existing legislation concerning the IoT scheme and the efforts made by the EU to adopt new safeguards, that can better complement the current legislative instruments. It is a fact that due to the uncertain nature of the IoT scheme, practices such as user profiling and data processing/collection, put the data of individuals in danger. The adoption of the General Data Protection Regulation ('GDPR') and of the Cybersecurity Act is definitely a step forward towards the right direction of effectively combatting the most important illegal practices of data collection and of setting the ground for a security by design system. Along with the other legislative instruments that will be adopted by the EU (and that were analyzed in par. 4.1. and 4.2. of this Chapter), it becomes apparent that a law by design approach is the only viable way of dealing with emerging technologies, such as IoT.[159] To be more specific, the legal bases of data processing that are stipulated in the GDPR, as well as the basic principles of processing, (such as data minimization) successfully hinder violations regarding data misuse and provide at a certain extent legal certainty. Also, the Radio Equipment Directive essentially turns legal obligations into technological requirements an IoT device must have in order to be put in the European market.

II.) Profiling and automated decision-making: An urgent need for regulation

However, and besides the aforementioned, a successful protection should under any circumstances face directly and effectively the profiling and automated decision-making problem. As it has been already been mentioned above, Article 22 of the GDPR does not explicitly oblige the data controller to inform the data subject of the rationale under which an automated decision was taken.[160] It is obvious that such a provision should become mandatory[161], as it will contribute to the battle against deterministic and racist algorithms, as well as it will give the people the power of knowledge of how exactly these machines 'think'. Consequently, data subjects will be given the chance to

---

[158] European Commission, 'Questions and Answers: Strengthening cybersecurity of wireless devices and products' (*Q&A: Strengthening cybersecurity of wireless devices*) <https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_5635> accesse d 19 January 2022

[159] Hildebrandt, supra note 10, at 219

[160] See Chapter 3 para. 3.3.

[161] Sandra Wachter and others, supra note 143

profile their profilers themselves and to obtain more concrete evidence and information on how they are being profiled[162].

4.4. Conclusions

As it has already been shown, this dissertation did not have as an aim to analyze the important contribution of IoT to society and the opportunities that it could possibly provide to citizens. These traits of the new technology are uncontestable.
On the contrary, the objective of this paper was to pose questions regarding the dangers of IoT in the security and data of individuals, to provide viable solutions and to assess the normative challenge of IoT. According to the author's own opinion, the attainment of the perfect balance between security and data protection in the IoT scheme is an unachievable scenario, as it would require the existence of a perfectly healthy legislation that is both just and contestable and at the same time not too invasive and intervening, as well as the absence of malicious intent by the State and companies. Of course, it would be very utopian for someone to think that a scenario like that would be feasible in any era. This also means, that the complete opposite dystopian scenario, is also not very probable. The truth lies somewhere in-between, as current and proposed legislation have shown that we can be well-equipped if we are called to fight for our future.

[162] Hildebrandt, supra note 10, at 223

Bibliography

PRIMARY SOURCES

CASES

Areios Pagos (A.P.) [Supreme Court] 254/2021, Criminal Law, (Greece)

Case C-140/20 G.D. v The Commissioner of the Garda Síochána, Minister for Communications, Energy and Natural Resources, Attorney General, Opinion of AG Campos Sánchez – Bordona

United States v. Knotts, 460 US 276 (1983)

LEGISLATION

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

Commission Delegated Regulation (EU) 2022/30 of 29 October 2021 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of that Directive [2021] OJ 2 7

Commission Directive 2008/63/EC of 20 June 2008 on competition in the markets in telecommunications terminal equipment [2008] OJ L 162

Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC [2014] OJ 2 153

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

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

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) [2019] OJ L 151

SECONDARY SOURCES

ARTICLES

Cavoukian A, 'Privacy by Design The 7 Foundational Principles, Implementation and Mapping of Fair Information Practices'[2011] <https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf > accessed 24 November 2021

Chiara G, 'The Balance Between Security, Privacy and Data Protection in IoT Data Sharing: A Critique to Traditional "Security & Privacy" Surveys' [2021] 7(1) European Data Protection Law Review <https://edpl.lexxion.eu/data/article/16985/pdf/edpl_2021_01-007.pdf> accessed 29 November 2021

Cohen J, 'Examined Lives: Informational Privacy and the Subject as Object' [2000] 52 Stanford Law Review

Dian F and others, 'Wearables and the Internet of Things (IoT), Applications, Opportunities, and Challenges: A Survey' [2020] 8 IEEE Access

Flammini A and Sisinni E, 'Wireless Sensor Networking in the Internet of Things and Cloud Computing Era' (2014) 87 Procedia Engineering

Greek Data Protection Authority 'Annual Report' (2014) <https://www.dpa.gr/sites/default/files/201909/ANNUAL_2014_V2.0_WEB_VIEW.PDF > accessed 15 December 2021

Karimi K, 'The Role of Sensor Fusion and Remote Emotive Computing (REC) in the Internet of Things' <https://www.nxp.com/docs/en/white-paper/SENFEIOTLFWP.pdf> accessed 10 January 2022

Khan R, Khan S, Zaheer R and Khan S, 'Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges' <https://ieeexplore.ieee.org/document/6424332> accessed 8 November 2021

Landaluce H, Arjona L, Perallos A, Falcone F, Angulo I and Muralter F, 'A Review of IoT Sensing Applications and Challenges Using RFID and Wireless Sensor Networks' (2020) 20 Sensors

Nissenbaum H, 'Where Computer Security Meets National Security' [2005] 7 (Ethics and Information Technology)

Peppet S, 'Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent' [2014] 93 Texas Law Review

Solove D, 'A Taxonomy of Privacy' [2006] 154(3) University of Pennsylvania Law Review

Stahl B, 'Privacy and security as ideology' [2007] 26(1) IEEE Technology and Society Magazine

Wachter S and others, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' [2017] 7(2) International Data Privacy Law

Weiser M, 'The Computer for the 21st Century' (1991) Scientific American

BOOKS

Brunton F and Nissenbaum H, *Obfuscation A User's Guide for Privacy and Protest* (The MIT Press 2015)

Durante M '*Safety and Security in the Digital Age. Trust, Algorithms, Standards, and Risks*' (2019) in Berkich D and D'Alfonso M (eds.) On the Cognitive, Ethical, and Scientific Dimensions of Artificial Intelligence, Springer Nature

Durante M, *Ethics, Law and the Politics of Information: A Guide to the Philosophy of Luciano Floridi* (1nd edn, Springer 2017)

Floridi L, *The Ethics of Information* (Oxford University Press 2013)

Hildebrandt M, *Smart Technologies and the End(s) of Law Novel Entanglements of Law and Technology* (Edward Elgar Publishing Limited 2015)

Solove D, *The Digital Person, Technology and Privacy in the Information Age* (NYU Press 2004)

Tamò-Larrieux A, *Designing for Privacy and its Legal Framework, Data Protection by Design and Default for the Internet of Things* (Springer

EU COMMUNICATIONS

Commission (EC), 'Communication from the Commission to the European Parliament, the European Council, the Council, The European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy' (Communication) COM (2020) 625 final

Commission (EC), 'On Promoting Data Protection by Privacy Enhancing Technologies (PETs)' (Communication) COM (2007) 228 final

Commission (EC), 'Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data

and on the free movement of such data (General Data Protection Regulation)' (Communication) COM (2012) 11 final

Commission (EC), '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)' (Communication) COM (2017) 10 final

Commission (EC), 'The EU's Cybersecurity Strategy for the Digital Decade' (Joint Communication) JOIN (2020) 18 final
Commission (EC), 'WHITE PAPER On Artificial Intelligence - A European approach to excellence and trust' (Communication) COM (2020) 65 final

CONFERENCE
Jia X, Feng Q, Fan T, Lei Q, 'RFID Technology and Its Applications in Internet of Things (IOT)' (2012 2nd International Conference on Consumer Electronics, Communications and Networks, 2012) <https://ieeexplore.ieee.org/document/6201508> accessed 11 November 2021

EU GUIDELINES
Article 29 Data Protection Working Party, [adopted 10 April 2018] Guidelines on consent under Regulation 2016/679
< https://ec.europa.eu/newsroom/article29/items/623051> accessed 29 December 2021

Article 29 Data Protection Working Party, [Revised 11 April 2018] Article 29 Working Party Guidelines on transparency under Regulation 2016/679 < https://ec.europa.eu/newsroom/article29/items/622227/en> accessed 17 November 2021

Article 29 Data Protection Working Party, [Revised 6 February 2018] Guidelines on Personal data breach notification under Regulation 2016/67 <https://ec.europa.eu/newsroom/article29/items/612052/en> accessed 17 November 2021

Article 29 Data Protection Working Party, [Revised 6 February 2018] Article 29 Working Party Guidelines on Automated individual decision-making and Profiling for the purposes
of Regulation 2016/679 <https://ec.europa.eu/newsroom/article29/items/612053/en> accessed 17 November 2021

European Data Protection Board, [20 October 2020] Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0 <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf> accessed 21 November 2021

EU OPINIONS

Article 29 Data Protection Working Party, [25 March 2014] Opinion 03/2014 on Personal Data Breach Notification <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf> accessed 17 November 2021

Article 29 Data Protection Working Party, [13 July 2010] Opinion 3/2010 on the principle of accountability <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf> accessed 17 November 2021

Article 29 Data Protection Working Party, [16 September 2016] Opinion 8/2014 on the Recent Developments on the Internet of Things < https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf> accessed 25 January 2022
European Data Protection Supervisor, [22 July 2016] Opinion 5/2016, Preliminary EDPS Opinion on the review of the ePrivacy Directive (2002/58/EC)

European data protection supervisor, 'Opinion of the European Data Protection Supervisor on the data protection reform package' (7 March 2012)
<https://edps.europa.eu/sites/default/files/publication/120307_edps_reform_package_en.pdf> accessed 20 November 2021

EUROPEAN COMMISSION STAFF WORKING DOCUMENT (SWD)

Commission (EC), 'Advancing the Internet of Things' (Staff Working Document) SWD (2016) 110 final

WEBSITES

Commission Nationale Informatique & Libertés, 'Cookies: the CNIL fines GOOGLE a total of 150 million euros and FACEBOOK 60 million euros for non-compliance with French legislation' (-, 6 January 2022) <https://www.cnil.fr/en/cookies-cnil-fines-google-total-150-million-euros-and-facebook-60-million-euros-non compliance> accessed 10 January 2022

European commission (*Questions and Answers - EU Cybersecurity*) <https://ec.europa.eu/commission/presscorner/detail/en/QANDA_19_3369> accessed 23 November 2021

European Commission, 'Types of EU Law' < https://ec.europa.eu/info/law/law-making-process/types-eu-law_en> accessed 19 November 2021
European Commission, 'Questions and Answers: Strengthening cybersecurity of wireless devices and products' (*Q&A: Strengthening cybersecurity of wireless devices*) <https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_5635> accessed 19 January 2022

European Commission, 'Radio Equipment Directive (RED)' (*Internal Market, Industry, Entrepreneurship and SMEs*, -) <https://ec.europa.eu/growth/sectors/electrical-and-electronic-engineering-industries-eei/radio-equipment-directive-red_en> accessed17 January 2022

European commission, 'The EU cybersecurity certification framework' <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework> accessed 2 December 2021

European Commission, 'What does data protection 'by design' and 'by default' mean?' <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en> accessed 20 November 2021

European Commission, 'When does the Charter apply?' <https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights/when-does-charter-apply_en> accessed 20 November 2021

European Data Protection Board, 'Hamburg Commissioner Fines H&M 353 Million Euro for Data Protection Violations in Service Centre' (2 October 2020) <https://edpb.europa.eu/news/national-news/2020/hamburg-commissioner-fines-hm-353-million-euro-data-protection-violations_en> accessed 17 December 2021

European Data Protection Board, 'Norwegian DPA imposes fine against Grindr LLC' (13 December 2021) <https://edpb.europa.eu/news/national-news/2021/norwegian-dpa-imposes-fine-against-grindr-llc_en> accessed 5 January 2022

European Data Protection Supervisor, 'The history of the General Data Protection Regulation' <https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en> accessed 19 November 2021

The "Only" Coke Machine on the Internet' <https://www.cs.cmu.edu/~coke/history_long.txt> accessed 10 November 2021

WORKSHOP

Zhang B, Mor N, Kolb J, Chan D, Goyal N, Lutz K, Allman E, Wawrzynek J, Lee E, and Kubiatowicz J, 'The Cloud is Not Enough: Saving IoT from the Cloud' (7th USENIX Workshop on Hot Topics in Cloud Computing, Santa Clara, California, 2016)