Digital Privacy Protection
Against Corporate Actors in the European Union:
Benefits, Flaws and Repercussions

Thesis submitted in partial fulfillment of the
requirements for the degree of
Master of Laws

Carl Vander Maelen
(student code 01204047)

Academic year 2016-2017
Promotor: Prof. Dr. Yves Haeck
Supervisor: Ms. Evelyn Merckx

© Carl Vander Maelen 2017
Ghent University
Spring 2017

Copyright in this work rests with the author. Please ensure that any reproduction
or re-use is in accordance with relevant national copyright legislation.
It would take the average person about 250 working hours every year or about 30 full working days to actually read the privacy policies of the websites they visit in a year.

- "Unlocking the Value of Personal Data", World Economic Forum (February 2013) 11
# Table of contents

1. Introduction .............................................................................................................................................. 1

2. Scope of the research and key definitions ............................................................................................ 6
   A) “Digital privacy protection…” ............................................................................................................. 6
       i) From the ‘right to privacy’ to the ‘right to personal data protection’ ........................................... 6
       ii) Personal data protection as a subset of the right to privacy ....................................................... 11
   B) “… against corporate actors…” ........................................................................................................... 15
   C) “… in the European Union” ................................................................................................................ 17

3. European Union policy to data protection ............................................................................................ 18
   A) Legislation ........................................................................................................................................... 18
       i) The Data Protection Directive and the Charter of Fundamental Rights ....................................... 18
       ii) 2018 and beyond: the General Data Protection Regulation ...................................................... 19
       iii) Evaluating the GDPR .................................................................................................................... 22
   B) Enforcement by the Court of Justice of the European Union .......................................................... 28
       i) The right to personal data protection is not an absolute right ..................................................... 29
       ii) The jurisdictional issue .................................................................................................................. 30
       iii) The right to be forgotten .............................................................................................................. 31
       iv) Future enforcement under the GDPR .......................................................................................... 33
   C) Lacunae ............................................................................................................................................... 34
       i) Legal persons ................................................................................................................................. 34
       ii) Mobile Location Analytics ........................................................................................................... 35
       iii) RFID .......................................................................................................................................... 37

4. Benefits, flaws and repercussions ............................................................................................................ 38
   A) Digital privacy protection and the freedom of expression and information: censorship? ............. 38
   B) The end of the ‘worldwide’ web ......................................................................................................... 43
       i) The fracture of the worldwide web ................................................................................................. 43
       ii) The risk of European digital colonization .................................................................................... 45
   C) Repercussions on corporate policy .................................................................................................... 47

5. Conclusion ................................................................................................................................................ 50

Bibliography ................................................................................................................................................. 53
1. Introduction

The statistics are baffling. Facebook has 1.65 billion monthly active users, who spend a daily average of 50 minutes on this platform. Youtube users watch more than 1 billion hours of videos per day and upload 400 hours of video content every minute. Every second, Snapchat users share more than 8.000 pictures.

Digital services have become an essential part of our modern society, and not only for purely recreational reasons. The desire to communicate is human and universal and this also translates to technological means of communication. Whatsapp users send friends and loved ones 42 billion messages and 1.6 billion photos per day. Business activities have also come to rely upon technology. Take for example the widespread use of in-company communication tool Slack. Moreover, it has become impossible to imagine a world without Google to filter through the tons and tons of information created on the Internet every day. We cannot unplug our society from the digital world anymore.

As corporate actors gain an increasingly large grip on how we communicate and interact with each other in our daily lives, more and more issues emerge concerning their use of our personal information. Services such as Youtube and Snapchat started out with a clearly recreational goal: to facilitate the sharing of videos with the rest of the world, and to quickly and easily exchange photos. Yet, as these services have grown exponentially, their immense popularity attracted the advertising industry, which made these digital services aware of their potential for monetization. One by one, these new media giants have all adopted business models that focus on advertising - including Youtube and Snapchat. The

---

result is that, in the United States alone, advertisers have invested $17.6 billion in digital advertising in Q3 2016.11

The widespread circulation of data has led to massive privacy concerns. The constant evolution of digital technology creates tools that enable corporate actors to advertise in a much more specific and accurate way. Through programmatic advertisements, companies no longer buy ads tied to a certain piece of content, but to target an exact audience:12 the same user is reached across multiple devices.13

Data is a currency.14 Businesses want to know who they can target and how. Any information about an individual’s name, gender, occupation and interests is collected by information submitted by users through digital services such as Facebook and Youtube. It does not stop there. Through the use of cookies, these services also actively collect information that users have not explicitly authorized to be gathered. Cookies are essentially tiny files and programs15 that come in two types. First-party cookies are employed by the website you are currently browsing on, while third-party cookies track your movement on sites which are affiliated with the track company to enable the creation of a full profile.16 The data collected by the cookies is used in algorithms that connect the information with income, geographic location and education - also known as probable behavior data.17 The combination of all these traces can be used to create profiles of natural persons, identifying them in the process.18 This form of information gathering is best exemplified by the methods employed by retailer websites such as Amazon. Every action - from the items looked at and ordered, to the time spent on the website - is carefully recorded and registered to compile profiles coupled to debit or credit card information.19 Even purchases that are not made are registered.20 As a result of these profiles, retailers can make more accurate recommendations and use more specific advertising through data science.21

It is clear that private companies use personal data on an unprecedented scale to pursue their business, while natural persons make more and more personal information available online22 - whether they are aware of it or not. By now ‘a reasonable person should assume that (…) many, if not most or all,
electronic communications are likely accessible, in whole or in (metadata) part, to various private actors’.

The collection of data is not limited to submitting information to a digital service or to browser behavior. Your location is also used, for example to display advertisements for local businesses and services. Brick and mortar stores are also adapting their sales and information gathering methods to stimulate and optimize sales; foot traffic within retail stores is tracked to monitor how long and where exactly you browse. Services such as Euclid, ShopperTrak and RetailNext collect this kind of information, known as Mobile Location Analytics. A service like FaceFirst goes even further and tracks customers by taking a picture of their face whenever they enter a store, which is then added to a database. The companies Realeyes and Synqera have a comparable concept, but also monitor customers’ reactions at the register.

Besides the obvious concerns regarding privacy - leading to instances of public outcry and more and more consumers creating email and social media accounts with false information - there is a multitude of other flaws to be found in the system. Previous incidents have clearly shown that the technology used to determine which ads should be shown in relation to Youtube videos is still prone to mistakes, for example by failing to differentiate between action movie extracts and terrorist videos. Facebook itself has on multiple occasions admitted that anomalies were discovered in how interaction with content was measured. Furthermore, digital advertising is effectively under a duopoly control with Facebook and Google accounting for an estimated 99% of the $2.9 billion in advertising growth in the third quarter of 2016.

The general public is concerned about its privacy, as can be found in the following Eurobarometer studies and surveys.

31 Ibid.

The European Union has taken action to combat these privacy concerns, by taking measures meant to protect personal data. This research seeks to answer three central questions: what is the legal reasoning behind protecting personal data; what policy does the EU set out for corporate actors regarding digital privacy protection via legislation and enforcement; and what are the repercussions of this policy? As a result, this thesis has investigative, descriptive and analytic goals.

To answer the aforementioned questions, a wide variety of written sources have been consulted. First, newspaper articles provide context and real-life situations, while books are helpful to understand the greater framework. Legal instruments by various organizations provide the applicable rules, whereas judgments from the Court of Justice of the European Union and the European Court of Human Rights showcase the enforcement of these rules. Finally, press reports and a myriad of articles from legal journals are essential to dissect in-depth issues. Since this thesis deals with the incredibly fast-moving world of technology, legal articles were the primordial source of information. Most other sources were simply too outdated to still be relevant.

The investigative aspect is the first to emerge in this thesis. Besides the scope of the research, the origins of data protection and key concepts thereof are investigated, as well as the merits of whether or not to consider data protection a standalone right (2). The descriptive character of this thesis manifests itself through a concise yet thorough overview of the European Union’s legislation and enforcement of digital privacy protection; several lacunae are also remarked upon (3). Lastly, this research analyzes the benefits, flaws and repercussions of the Union’s policy, and the dangers it poses in the form of censorship, the possible end of the ‘worldwide’ web and the effects on corporate policy (4). The conclusion reiterates the most striking findings of this thesis (5).

I would like to extend my gratitude to Prof. Dr. Yves Haeck and Ms. Evelyn Merckx for their guidance in writing this thesis, and sincerely thank Angela Coriz for her thorough linguistic editing.
2. Scope of the research and key definitions

The vital role of technology in our modern lives and the widespread privacy concerns regarding its use have made digital privacy protection a rich topic for discussion and research. For the sake of clarity, brevity and depth, it is important to define several of the key concepts used in this study, and to limit the scope of the research in three important ways. First of all *ratione materiae*: not the general human right to privacy, but more specifically the protection of digital privacy is examined (A). Secondly, the scope *ratione personae* centers on the role of corporate actors in the possible violation of digital privacy (B). Intrusions or threats by State actors are irrelevant for this current research. Thirdly, *ratione loci*, the protection of digital privacy against corporate actors in the European Union takes center-stage (C). However, it is impossible not to throw a cursory glance at legislation and enforcement by the Council of Europe and its bodies, as well as regulation in North America and its impact upon general corporate conduct.

A) “Digital privacy protection…”

Digital privacy protection is the focal point of this study. To understand what digital privacy protection implies, several related concepts must be explored. Firstly, the evolution from a general ‘right to privacy’ to a more specific ‘right to personal data protection’ and the meaning of ‘personal data’ is set out (i). Secondly, this thesis follows the approach that the right to personal data protection is a subsidiary of the right to privacy (ii).

i) From the ‘right to privacy’ to the ‘right to digital privacy protection’

The right to personal data protection finds its origins in the historical development of the broader and more general right to privacy. Although this right is enshrined in major human rights treaties - such as article 8 of the ECHR and article 17 of the ICCPR - the term ‘privacy’ is difficult to define. Attempts to do so trace back to the end of 19th century when it was labeled the ‘right of determining ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others’.36 Some definitions speak of the individual’s desire for solitude, intimacy, anonymity, and reserve,37 while yet another labels privacy the ‘freedom from unwarranted and unreasonable intrusions into activities that society recognizes as belonging to the realm of individual autonomy’.38 Comparably, it is called the ‘right to be let alone [which is] the most comprehensive of rights’.39 Nowak describes it as the ‘sphere of individual autonomy’ where an individual can ‘shape one’s life according to one’s own (egocentric) wishes and expectations’.40

The origin of privacy as a fundamental right can be traced to 1948. In that year, the Universal Declaration of Human Rights (UDHR) was published by the United Nations. Its article 12 states:

*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.*41

The second instrument that recognizes privacy as a basic human right is the European Convention on Human Rights (ECHR) by the Council of Europe in 1950. Article 8 of the Convention stipulates:

1. **Everyone has the right to respect for his private and family life, his home and his correspondence.**
2. **There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.**

Sixteen years later, the International Covenant on Civil and Political Rights (ICCPR) was adopted. As an international bill of rights, its importance for human rights protection on an international level cannot be understated. Article 17 ICCPR states:

1. **No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation.**
2. **Everyone has the right to the protection of the law against such interference or attacks.**

It is clear then that these definitions all share several basic foundational elements. The situations and matters that merit protection are identical in all three of the instruments. The ICCPR repeats the exact phrasing of the UDHR by mentioning ‘privacy, family, home or correspondence’ as well as ‘honor and reputation’. The ECHR contains a different wording regarding the protected situations: ‘private and family life, his home and his correspondence.’ Although private and family life are grouped together, this does not create a substantial difference in practice. The lack of the words ‘honor and reputation’ is, however, noteworthy. Nevertheless, while the protection of an individual’s ‘honor’ is not mentioned at all in the ECHR, its article 10, paragraph 2 does foresee in a derogation of the freedom of expression ‘for the protection of the reputation or rights of others.’

Larger differences arise between the instruments and their phrasing concerning the prohibited acts. The UDHR sets out that ‘no one shall be subjected to arbitrary interference (…) nor to attacks’. The ICCPR adds an important nuance to this: ‘No one shall be subjected to arbitrary or unlawful interference (…) nor to unlawful attacks.’ The ICCPR’s a contrario demand that interference or attacks must be ‘lawful’ is echoed in paragraph 2 of article 8 ECHR, which prohibits any interference ‘except such as is in accordance with the law.’ National law must thus grant an authorization to interfere with privacy interests, and interference is only justified in those situations that the law foresees. The ECHR is more restrictive than the ICCPR since it also requires that interferences must be necessary in a democratic society, and that they must pursue a number of legitimate aims.

When these elements are taken together a ‘classic’ right to privacy can be distilled: an individual has the right to respect for his or her privacy, family, home or correspondence, and shall not be subjected to arbitrary or unlawful interference with this right.

---

43 ‘General Comment 16 on the Right to Privacy’, Human Rights Committee (8 April 1988), UN Doc HRI/GEN/1/Rev.9 (Vol. I), paragraph 3.
44 For a similar view, see: CJEU, Joined cases C-92/09 and C-93/09, Volker and Markus Schecke GbR and Hartmut Eifert v. Land Hessen, 9 November 2010, Opinion of Advocate General Sharpston, para 71.
This understanding of privacy was challenged as technology evolved. Manual data processing used to be the norm, but was gradually replaced by automatic data processing - starting as early as 1961 when the American Internal Revenue Service changed its working methods to this quicker way of processing. As more and more public and private organizations resorted to automatic data processing, massive amounts of data about every aspect of the life of individuals became easily available. Personal information had always been available, but there used to be ‘a reasonable de facto expectation of privacy’ because it was hard to collect all this separate information. Through automated processing the separate pieces of information became significantly easier to find. Automated processing magnified the threat to informational privacy. This created a need to differentiate between the classical broad term of ‘privacy’ and a new need to protect an individual’s privacy regarding the personal data used in automatic data processing. In this context, privacy is used as a means to plead for a ‘right to control personal information’.

This quickly became supported by a number of highly influential instruments. The first of these was put forward by the Organization for Economic Co-operation and Development (OECD) when it created a recommendation in 1980 to protect privacy in the context of transborder flows of personal data. It recognized a common interest for Member States in protecting privacy and individual liberties, and that it was necessary to reconcile ‘fundamental but competing values such as privacy and the free flow of information’. In its first article, personal data is defined as ‘any information relating to an identified or identifiable individual (data subject)’. The European Court of Human Rights has also endorsed this definition.

In 1981 the first legally binding international instrument in the field of data protection was adopted by the Council of Europe: the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data by the Council of Europe (Convention 108). It is affirmed once more that there is a need to protect an individual's rights and fundamental freedoms - in particular the right to privacy - during the automatic processing of personal data.

This right to the protection of personal data as a subsidiary of the right to privacy is further developed by the Human Rights Committee in its ‘General Comment No. 16 on the right to privacy under article 17 of the ICCPR’. With remarkable insight into the major technological evolutions which were still to follow, the Committee already stated in 1988:

---

50 Ibid, Preambule.
52 ECtHR, Amann v Switzerland, No. 27798/95, 16 February 2000, para. 65.
54 Ibid., art. 1.
The gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant. In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination.\(^{55}\)

In 1995, the European Union adopted the influential Data Protection Directive.\(^{56}\) There, it stipulated that ‘the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data’ shall be protected by the Member States.\(^{57}\) This follows the same blueprint as the OECD recommendation: information about both identified and identifiable is subjected to rules. It does, however, clearly set out when a person is ‘identifiable’:

‘Personal data’ shall mean any information relating to an identified or identifiable natural person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.\(^{58}\)

Even as the Directive became increasingly outdated due to the rapid technological evolutions and the European Union set out to renew its data protection framework, the Article 29 Working Party confirmed in its preparatory documents that it still prefers a broad notion of ‘personal data’ so that all possible data linked to an individual are comprised within the term.\(^{59}\) This is reflected by the European Commission’s explanation of personal data, which follows the same approach by stating that any information relating to identified or identifiable individuals is targeted (‘any information relating to an individual, whether it relates to his or her private, professional or public life’) but also uses more extensive wording and provides non-exhaustive examples (‘It can be anything from a name, a photo, an email address, bank details, your posts on social networking websites, your medical information, or your computer's IP address’).\(^{60}\)

When the 1980 OECD recommendation, Convention 108, General Comment 16 and the Data Protection Directive are combined ‘personal data protection’ thus forms the protection of the fundamental rights and freedoms of an individual regarding the processing of his or her personal data - in particular concerning a person’s private life - whether by public authorities or private individuals or bodies. Since the protection of personal data seeks to protect in particular an individual’s right to privacy, personal data protection can also synonymously be called ‘digital privacy protection.’

\(^{55}\) ‘General Comment 16 on the Right to Privacy’, Human Rights Committee (8 April 1988), UN Doc HRI/GEN/1/Rev.9 (Vol. I), para. 10.
\(^{56}\) Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281, 31 (Data Protection Directive).
\(^{57}\) Article 1(1) Data Protection Directive.
\(^{58}\) Article 2(a) Data Protection Directive.
However, the most recent evolutions in European Union personal data legislation seem to change this longstanding approach. At first glance, the General Data Protection Regulation\textsuperscript{61} - which replaces the Directive and will thus form the new legal framework for personal data protection in the European Union when it becomes enforceable from 25 May 2018 onwards - does not bring substantial change. After all, its interpretation of personal data still follows the template set by the definition in the Data Protection Directive. The GDPR does, however, add or replace several noteworthy elements (emphasis added):

\begin{quote}
‘Personal data’ means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person\textsuperscript{62}.
\end{quote}

Where the Directive explains the term ‘identifiable person’, the Regulation defines an ‘identifiable natural person’. This is consistent with the Regulation’s statement that it does not apply to the processing of personal data concerning legal persons\textsuperscript{63} nor to the personal data of deceased individuals\textsuperscript{64}. More importantly, however, the Directive’s concise referral to an ‘identification number’ as a means of identifying a person has gotten a significant and necessary update. In these modern times, where a wealth of information about individuals is available through social media, online retailers and other digital services, the Regulation now also recognizes that identification is possible via ‘an identifier such as a name, an identification number, location data, an online identifier.’ The use of ‘such as’ emphasizes that these identifiers are non-exhaustive, while the extra clarification is more than welcome.

It is however the ‘mission statement’ of the GDPR that drastically differs in wording to what came before and forms a real departure for the data protection regime in Europe:

1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.\textsuperscript{65}

Thus, whereas former instruments stressed that in particular the right to privacy would be protected by regulating the processing of personal data, the Regulation aims to protect in particular the right to personal data protection. The GDPR thus no longer treats personal data protection as an instrument to achieve privacy, but rather as a standalone right separate from the right to privacy. This leads to an important discussion: can the right to personal data protection really be considered a standalone right, or does it function as a subset of the right to privacy?

\textsuperscript{61} 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), L 119/1 (GDPR).

\textsuperscript{62} Article 4(1) GDPR.

\textsuperscript{63} Recital (14) GDPR.

\textsuperscript{64} Recital (27) GDPR. See also: ‘Opinion 4/2007 on the concept of personal data (WP136)’, Article 29 Working Party (20 June 2007) 22.

\textsuperscript{65} Article 1 GDPR; confirmed in recital (2) GDPR.
ii) Personal data protection as a subset of the right to privacy

The discussion of whether or not personal data protection deserves the status of a standalone right because it would deliver additional protection outside the scope of privacy is the topic of much debate.

The approach of the GDPR certainly follows the path previously set out by the Union. The Charter of Fundamental Rights of the European Union (‘the Charter’) was adopted in 2000 and already separated the right to privacy and the right to personal data protection. The former is contained in article 7 of the Charter, whereas the latter is protected under article 8. The Treaty on the Functioning of the European Union (TFEU), one of the primary legal instruments of the European Union, also provides the right to the protection of personal data in its article 16 without mention of privacy.

The fact that EU instruments are so willing to grant personal data protection the status of standalone right is certainly remarkable. The Charter’s Explanatory Memorandum does not clarify where this sudden distinction between privacy and data protection comes from; instead it refers to the Data Protection Directive, Article 8 of the ECHR and Convention 108 as legal bases. Yet, as already discussed, these instruments and their relevant provisions explicitly label data protection as a tool to help protect privacy. Article 286 of the Treaty establishing the European Community (EC) is also too vague of a ground as it stipulates the following: ‘Community acts on the protection of individuals with regard to the processing of personal data and the free movement of such data shall apply to the institutions and bodies set up by, or on the basis of, this Treaty.’ Directive 2002/58 is a further indication that regulations concerning the processing of personal data do not establish a standalone right to personal data protection, but rather aim to protect privacy. This can be deduced from the title itself (Directive 2002/58 concerning the processing of personal data and the protection of privacy in the electronic communications sector) and from its scope and aim, with the Directive itself stating that it seeks ‘to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data’.

The CJEU’s case law does not do personal data protection as a standalone right any favors either. In 2003 - three years after the Charter was adopted, although six years before it became a part of primary EU law through the Treaty of Lisbon - the Rundfunk case treated data protection and privacy as interchangeable concepts and even stressed that the Data Protection Directive should be interpreted in light of the right to privacy. This is backed up by the Promusica case of 2008 in which the Court stated that there is ‘a further fundamental right, namely the right that guarantees protection of personal data and hence of private life’. The Satamedia case of the same year also considers the Directive as an

---

68 Ibid., p. 11.
71 CJEU, Joined cases C-465/00, C-138/01 and C-139/01 Rechnungshof v. Österreichischer Rundfunk and Others and Neukomm and Lauermann v. Österreichischer Rundfunk, 20 May 2003, paras. 37, 68 and 70.
72 CJEU, C-275/06, Productores de Música de España (Promusicae) v. Telefónica de España SAU, 29 January 2008, para 63.
instrument that protects privacy. Post-Treaty of Lisbon judgments continue this reasoning and simply do not view personal data protection as a right that merits a standalone status; the link with privacy protection is always present. This is clear in the Volker case, in the Rynes case, and in the extremely influential and important cases of Google Spain and Digital Rights Ireland. In this last case, the Court literally notes that ‘protection of personal data resulting from the explicit obligation laid down in Article 8(1) of the Charter is especially important for the right to respect for private life enshrined in Article 7 of the Charter’.

At first glance, the Schrems case seems to provide some support for de-coupling the right to privacy and the right to personal data protection, since its paragraph 39 recognizes the importance of both rights separately. Yet only moments later, the Court once more notes that the protection of personal data plays an important role ‘in the light of the fundamental right to respect for private life’. The 2016 Tele2 Sverige case follows the exact same pattern. Where it first recognizes the importance of both articles 7 and 8 of the Charter separately, personal data protection is ultimately used as a tool to protect privacy. The CJEU’s jurisprudence thus does not support a de-coupling of privacy and personal data protection.

Nonetheless, there are certain voices that plead for such a distinction. Advocate General Sharpston separates a classic definition of privacy from a more modern right to data protection. Advocate General Cruz Villalón also stresses that informational self-determination remains a central tenet of the right to data protection and one that distinguishes it from the right to privacy. The Bavarian Lager case, judged by the General Court, also provides support. As Lynskey notes and analyzes in an excellent article on the added value of data protection in the EU the General Court finds that ‘data protection rules prevail only when privacy is undermined. When privacy is not undermined, the freedom of information rules prevail over the data protection rules. Therefore (…) not all data processing adversely affects the right to privacy and (…) data protection applies to a wider variety of personal data processing

---

73 CJEU, C-73/07, Tietosuojavaltuutettu v. Satakunnan Markkinapörssioy and Satamedia Oy, 16 December 2008, para. 54.
74 CJEU, Joined cases C-92/09 and C-93/09, Volker and Markus Schecke GbR and Hartmut Eifert v. Land Hessen, 9 November 2010, para. 52.
75 CJEU, C-212/13, Frantisek Rynes v Urad pro ochranu osobnich udaju, 11 December 2014, para. 29.
76 CJEU, C-131/12, Google Spain, S.L., Google Inc. v. Agencia Española de Proteccion de Datos, 13 May 2014, para. 53 and 74 (Google Spain).
77 CJEU, Joined cases C-293/12 and C-594/12, Digital Rights Ireland and Seitling and Others, 8 April 2014.
78 Ibid., para. 53.
79 CJEU, C-362/14, Maximilian Schrems v. Data Protection Commissioner, 6 October 2015.
80 Ibid., para. 78.
81 CJEU, Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB and Secretary of State for the Home Department, 21 December 2016.
82 Ibid., para. 93.
83 Ibid., para. 96: ‘(…) the protection of the fundamental right to respect for private life at EU level requires that derogations from and limitations on the protection of personal data should apply only in so far as is strictly necessary.’
84 CJEU, Joined cases C-92/09 and C-93/09, Volker and Markus Schecke GbR and Hartmut Eifert v. Land Hessen, 9 November 2010, Opinion of Advocate General Sharpston, para 71. While I too remarked earlier that the classic right to privacy has evolved into a more modern interpretation, I explicitly noted that this modern version aims to achieve ‘digital privacy protection’.
85 CJEU, Joined cases C-293/12 and C-594/12, Digital Rights Ireland and Seitling and Others, 8 April 2014, Opinion of Advocate General Cruz Villalón.
86 General Court (Third Chamber), T-194/04, Bavarian Lager v. Commission, 8 November 2007.
than privacy law. In other words, the material scope of application of the two rights is distinct. However, the Court of Justice later overruled the General Court’s ruling when it decided that privacy and data protection legislation cannot be treated separately. The European Court of Human Rights follows this view as well. In the case of Segerstedt-Wiberg and Others it concluded that the continued storage of personal information in the case at hand was a disproportionate interference with their right to respect for their private life. Case law thus firmly treats data protection as a tool to protect the right to privacy.

National jurisprudence has a more mixed opinion than the CJEU’s view. On one hand, the German Constitutional Court has long since connected data protection to both articles 1 and 2 of the German Constitution, considering it a fundamental right which flows from an individual’s right to ‘informational self-determination’ which itself is based on the right to personality and human dignity. The UK, on the other hand, follows the established approach of using personal data protection as an instrument to protect privacy. In fact, UK courts are only willing to apply data protection rules if the right to privacy of an individual is at stake; personal data is in this view ‘information that affects his privacy, whether in his personal or family life, business or professional capacity’.

In-depth discussions are also found in the academic field. Hijmans says that while the Data Protection Directive ‘puts in place a legal system for the processing of personal data (…) its aim is to (better) protect privacy’. Kowalik-Bariczky and Pollicino also connect personal data protection - in particular the right to be forgotten - to the right to privacy, while Kuner views personal data as a manifestation of an individual’s personality in a digital setting. Other authors do not agree, and follow Sharpston and Villalón in viewing data protection and privacy as two distinct rights. Kranenborg’s primary argument, for example, is that data protection applies to a wider range of data than privacy, which is echoed by Kokott and Sobotta. Lynskey also argues that data protection has a broader scope than privacy. She bases herself on the fact that personal data is not a context-dependent concept, unlike privacy interference, and secondly that personal data encompasses information about unidentified yet identifiable individuals.

This thesis considers personal data protection a subset of the right to privacy, and therefore respectfully disagree with the arguments put forward that personal data protection has a broader field of application than privacy. Every act related to personal data directly or indirectly has an impact on privacy, and every regulation concerning personal data ultimately serves to ensure privacy of the individuals concerned (cf.

88 CJEU, C-28/08, European Commission v Bavarian Lager, 29 June 2010, paras. 58, 59.
89 ECtHR, Segerstedt-Wiberg and Others v. Sweden, No. 62332/00, 6 June 2006.
91 Court of Appeal, Durant v Financial Services Authority, EWCA Civ 1746, 8 December 2003, Auld LJ at para 28. A more recent case has, however, denied that personal data protection would form a part of the right to privacy by stating that article 8 ECHR does not protect personal data, demonstrating that confusion reigns supreme among the national courts. See: High Court, R (on the application of AB) v Secretary of State for the Home Department, EWHC 3453, 7 November 2013, paras. 14 and 16.
98 Ibid., 583 and further.
Hijmans’ argument). This is sufficiently clear from the wording of many instruments cited earlier and from the extensive case law of the CJEU. Deducing the contrary from the CJEU’s judgments seems based on a loose interpretation of those very judgments. For example, Lynskey’s argumentation is party based on the Rundfunk judgment, where the Court decided that the recording by an employer of the names and wages paid to employees ‘cannot constitute an interference with private life’, although it would constitute data processing. Yet it is quite a leap to interpret this statement in such a way that the processing in question would fall under personal data protection and not under the right privacy. What the Court says, in fact, is that this processing of data does fall within the ambit of the right to privacy; in this case there is simply no unlawful interference with privacy. The Court does nothing more than provide a negative answer to the question whether or not the form of data processing in the case at hand interferes with private life. This interpretation is backed up by the earlier finding of the Court that the regulations concerning data processing still have privacy protection as their main goal. The same reasoning holds true when the Herbecq case before the ECommHR would be used to try and prove a distinction between data protection and the right to privacy; the Commission simply decided that the data processing in the Herbecq case did not constitute a violation of the right to privacy. In both cases, the processing of data was used as a tool to evaluate the protection of privacy.

Arguments that data protection helps in the development of the right to informational self-determination which would distinguish it from the right to privacy, are also unconvincing. What else is the choice of whether or not to disclose personal data but to decide what aspects of a person’s private life are disclosed? As Kuner already observed: personal data is a manifestation of an individual’s personality in a digital environment. In turn, selecting which aspects of your private life to reveal or not serves one goal and one goal only: to ensure your privacy.

Some argue that privacy would be a tool that facilitates individual opacity and protects against intrusion, while data protection promotes transparency and accountability. Solove supports this, arguing that privacy concerns confidentiality, reputation and publicity, whereas data protection ‘pertains to the uses and practices associated with our information’. But is not every concern regarding the handling of our data motivated by the thought that an irresponsible use of our data could harm our reputation, breach confidentiality and bring unwanted publicity? Do we not seek ‘transparency and accountability’ in the use of our data, so as to prevent intrusions into our private sphere or at least hold those responsible accountable? Thus, the very argument that the rights that data protection offers would supposedly go beyond the reach of the right to privacy, help to establish data protection as a tool to achieve and protect privacy.

100 CJEU, Joined cases C-465/00, C-138/01 and C-139/01 Rechnungshof v. Österreichischer Rundfunk and Others and Neukomm and Lauermann v. Österreichischer Rundfunk, 20 May 2003, para. 74.
101 Ibid., paras. 68 and 70.
103 The semi-predecessor of the ECtHR.
104 CJEU, Joined cases C-293/12 and C-594/12, Digital Rights Ireland and Seitling and Others, 8 April 2014, Opinion of Advocate General Cruz Villalón.
B) “... against corporate actors...”

This research focuses on the influence of corporate actors on digital privacy; the massive collection, analysis and usage by major corporations which fundamentally impacts our society. The central problem here is the balancing of commercial freedom versus the protection of personal data, as well as the myriad of other societal repercussions that the Union’s policy has caused. The status of digital privacy protection in the relationship between States and individuals (the topic of ‘State surveillance’) merits an entirely separate study.

The *ratione personae* field seems to contain the key challenge regarding the legal protection and enforcement of digital privacy. After all, privacy and personal data protection are defined as fundamental human rights. These are traditionally vertical. The International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social and Cultural Rights (ICESCR), for example, regulate the relationship between a State and the individuals within its territory and subjected to its jurisdiction, 108 while the rights set out in the ECHR must be secured by State Parties to everyone within their jurisdiction. 109 As a result, the right to privacy and - more specifically - the right to *digital* privacy is applicable in the relationship between States and individuals. As non-State actors, enterprises would not fall within this ambit. Yet since they are as powerful as States in the collection and usage of personal data, if not more so, there is a clear need for corporate actors to also be bound by privacy standards. In the words of Stefan Kulk: “Google is making decisions that are publicly relevant. As such it is becoming almost like a court or government, but without the fundamental checks on its power”. 110

Practice shows that this worry about the non-binding nature of the right to privacy to private actors is mainly a doctrinal concern. Almost all jurisdictions expect private actors to take responsibility in protecting human rights in a national context. 111 Furthermore, fundamental rights not only oblige a State to abstain from negative behavior (to respect) but also create positive obligations for States: there is a duty to both protect and fulfill the right to privacy towards its citizens. These positive obligations are reflected in the instruments dealing with personal data protection. Convention 108 states that each State Party vows to undertake the ‘necessary measures in its domestic law to give effect to the basic principles for data protection’. 112 The need to protect personal data from abuse by corporate actors has also explicitly been recognized as early as 1980 by the OECD in its personal data recommendation:

*These Guidelines apply to personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties* 113

Convention 108 also stresses its applicability to both the public and private sectors.

---

108 International Covenant on Civil and Political Rights (ICCPR), 16 December 1966, UNTS vol. 999, 171, article 2(1); International Covenant on Economic, Social and Cultural Rights (ICESCR), 16 December 1966, UNTS vol. 993, 3, article 2(1).


112 Article 4 Convention 108.

The Parties undertake to apply this Convention to automated personal data files and automatic processing of personal data in the public and private sectors.\textsuperscript{114}

Both the 1980 OECD recommendation and Convention 108 thus make the State Parties responsible for private compliance with the automatic data processing provisions, without further ado. Since these are instruments drafted by the State Parties themselves, it is clear that States accept that it is their duty to ensure that corporate actors follow these rules through national legislation and enforcement.

To streamline this process and guarantee the functioning of the Single Market, the European Union laid a clear legal framework for personal data protection by governments against corporate actors. The Data Protection Directive, the progressive enforcement by the CJEU, and national legislation set out these ground rules. The General Data Protection Regulation is the newest instrument to regulate personal data protection and introduces a number of key changes, as will be discussed in the next chapter. One element should be clear, however: it has a broad material scope which encompasses corporate actors, since it applies to ‘applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system’.\textsuperscript{115} The established definitions of data controllers or processors also apply to corporate actors and, lastly, the GDPR explicitly uses the term ‘enterprise’ in its provisions\textsuperscript{116} and defines this notion as ‘a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity’.\textsuperscript{117}

One important question remains. Whether or not one considers personal data protection a subset of the right to privacy or a standalone right, it is still unclear whether or not the EU Charter can be invoked in proceedings between private parties. This lack of clarity applies to both article 7 (privacy) and article 8 (personal data protection). The CJEU refused to give a horizontal direct effect to article 27 of the Charter (which deals with workers’ right to information and consultation within the undertaking) yet it did not exclude this possibility for other rights of the Charter if the relevant article is ‘sufficient in itself to confer on individuals an individual right which they may invoke as such’.\textsuperscript{118} Some authors plead that, indeed, the Charter places horizontal obligations on individuals,\textsuperscript{119} and that corporate actors would thus be obliged to respect the right to privacy for EU citizens.\textsuperscript{120} In any event, further clarification through jurisprudence is needed.

This research will also not handle privacy concerns regarding the internal handling of data of employees within companies, for example in HR matters.\textsuperscript{121} The focus is squarely on corporate actors collecting data from external individuals who make use of their services.

\textsuperscript{114} Article 3(1) Convention 108.
\textsuperscript{115} Article 2(1) GDPR.
\textsuperscript{116} See for example article 30(5).
\textsuperscript{117} Article 4(18) GDPR.
\textsuperscript{118} CJEU, C-176/12, AMS v. Union locale des syndicats CGT and Ors, 15 January 2014, para 47.
\textsuperscript{121} DLA Piper LLP, ‘Preparing for the GDPR: New employee data subject rights could disrupt core HR procedures’, Lexology (18 April 2017) http://www.lexology.com/library/detail.aspx?g=dcbc5cf7-6b07-4017-9ad4-3b8e78d7dc5b.
C) “… in the European Union”

This research provides an overview of the policy of the European Union, and the repercussions thereof. Because of the wealth of legislation and judgments pertaining to digital privacy protection, the Union’s data protection policy proved most interesting to warrant a thorough study.

As mentioned already, the European Union has taken action to create and maintain a framework for personal data protection. Since article 16 of the Treaty on the Functioning of the European Union (TFEU) states that “Everyone has the right to the protection of personal data concerning them”, the European Union has the competence to draw up rules on data protection for all activities within the scope of EU law. It has acted upon this competence by adopting a wide array of directives and regulations. The importance of case law by the Court of Justice of the European Union (CJEU) can also not be understated. Lastly, the Charter of Fundamental Rights of the European Union sets forth in its article 8 that personal data protection is a fundamental human right. Under article 51 of this Charter, both EU institutions as well as Member States must ‘respect the rights, observe the principles and promote the application’ of the Charter ‘in accordance with their respective powers’.

The Council of Europe (CoE) and the European Court of Human Rights (ECtHR) have also added elements to the sphere of data protection in Europe, since all Member States of the EU are also CoE Member States. As a result, there is an overlap in regulation. Insofar that CoE instruments and ECtHR decisions have - or had - a noteworthy impact on general European Union policy, they will also be discussed. However, the focus is on the European Union and its Member States. Therefore, the state of digital privacy protection in CoE parties that are not Member States of the EU (for example Turkey and Russia) will not be discussed. The same holds true for States that have ratified some of the essential instruments but are not EU Member States (for example Uruguay, which acceded to Convention 108 in 2013).

3. European Union policy to data protection

As set out in the previous chapter, States are obliged to protect individuals and to fulfill their human rights needs. As a result, they must take legislative action and enforce these rules to fully realize their obligations. Since 1995, however, the European Union has taken this task upon itself. This chapter provides an overview of the European Union’s legislation concerning personal data protection (A) and the enforcement of its policy by the Court of Justice of the European Union (B). Notwithstanding this extensive policy, several lacunae are noticeable in the data protection regime in the EU (C).

A) Legislation

As instruments to achieve personal data protection, the European Union has relied on the Data Protection Directive for twenty-three years, as well as more recently on the Charter of Fundamental Rights (i). The framework concerning data protection is, however, on the cusp of a sweeping modernization through the introduction of the General Data Protection Regulation (ii). The GDPR introduces or adapts several provisions which result in key changes to the Union’s legislative approach to digital privacy protection (iii).

i) The Data Protection Directive and the Charter of Fundamental Rights

In 1995 the European Union introduced its first instrument to protect personal data: the Data Protection Directive.\(^{123}\) Its adoption served to realize a harmonious free movement of goods, services, people and capital since many individual Member States had already adopted national legislation.\(^{124}\) As a consequence, its scope is limited to the internal market. The Directive sought to ensure an equally high level of protection for all Member States, and not to lessen the protection that national laws already afforded.\(^{125}\) Since all EU Member States (at that time: 15) had already ratified CoE Convention 108, the Directive built upon its principles.

In 2000, Regulation (EC) No. 45/2001 was introduced,\(^{126}\) but the application of this instrument is limited to the institutions and bodies of the EU and their processing of data. In 2002 Directive 2002/58/EC\(^{127}\) - also called the ePrivacy Directive - saw the light of day, with rules for electronic communication service providers (telecommunication companies and internet providers) regarding the management of the data of their subscribers and provides these customers with several rights. Directive 2006/24/EC made its debut in 2006.\(^{128}\)

\(^{123}\) Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281, 31 (Data Protection Directive).

\(^{124}\) Recitals (1), (4), (7) and (8) Data Protection Directive.

\(^{125}\) CJEU, Joined cases C-468/10 and C-469/10, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado, 24 November 2011, paras. 28-29.

\(^{126}\) Regulation (EC) No. 45/2001 on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data (EU Institutions Data Protection Regulation), OJ 2001 L 8.


In 2007, the next big step was taken when the Treaty on the Functioning of the European Union (TFEU)\(^{129}\) was adopted. Its article 16 states: “Everyone has the right to the protection of personal data concerning them”. The European Union thus has the competence to draw up rules on data protection for all activities within the scope of EU law.

The Charter of Fundamental Rights of the European Union is arguably the most important instrument regarding data protection, except for the directives and regulations drawn up specifically to regulate data protection. Adopted in 2000 as a merely political document, the Charter arose to the rank of EU primary law in 2009 upon the entry into force of the Treaty of Lisbon\(^{130}\). Its article 7 reiterates the traditional right to privacy, but article 8 forms the real innovative provision by foreseeing an apparent standalone right to personal data protection. However, as discussed earlier, this thesis considers personal data protection a subset of the right to privacy.

Lastly, and most recently, the European Commission has proposed a revision of the ePrivacy Directive\(^{131}\). One of its most drastic innovations is that it now also protects meta-data\(^{132}\). This is contextual information coupled to electronic messages, such as the exact time and location, and has been recognized as being able to reveal personal and sensitive data\(^{133}\). The existing rules concerning cookies will also be streamlined. The end goal of the revision is to provide ‘a high level of protection for consumers, while allowing businesses to innovate’.\(^{134}\) The updated ePrivacy Directive debuts alongside a much more hotly anticipated instrument: the General Data Protection Regulation.

\[\text{ii) 2018 and beyond: the General Data Protection Regulation} \]

Due to both the age of the Data Protection Directive, adopted in 1995 when the internet was in its infancy, and its nature as a directive, which allows Member States leeway as to the transposition of its rules into national law, the European Commission undertook a review in 2009 to evaluate data protection in the European Union.\(^{135}\) One year later, the Commission concluded that a serious modernization of the Union’s policy was needed.\(^{136}\)

\[\text{---}\]


\(^{130}\) Charter of Fundamental Rights of the European Union, European Union (26 October 2012) 2012/C 326/02.


\(^{132}\) Ibid., article 6.

\(^{133}\) CJEU, Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB and Secretary of State for the Home Department, 21 December 2016.


The European Commission announced its ideas in 2012 by proposing both a General Data Protection Regulation\(^{137}\) (meant to replace the Data Protection Directive) and a General Data Protection Directive.\(^{138}\) A final agreement was made between the Parliament and the Council in 2015, consisting of two separate instruments: the 'General Data Protection Regulation for the protection of Personal Data'\(^{139}\) and the 'Data Protection Directive for Police and Criminal Justice Authorities to Protect Data in a Criminal Investigation Procedure'.\(^{140}\) The latter entered into force on 5 May 2016 and Member States have until 6 May 2018 to translate the directive into national law. However, the former is the most relevant for this current research. The General Data Protection Regulation (GDPR) entered into force on 24 May 2016, and will be enforceable from 25 May 2018 onwards, giving all actors involved time to prepare for their new or adapted obligations.

The GDPR forms a clear next step for digital privacy protection in Europe, and marks the end of the 23-year long regime established by the Data Protection Directive. Even though the Directive successfully raised personal data protection standards, the GDPR recognizes that it resulted in a fragmented approach of data protection in the EU; these different levels of protection in the Member States could - and indeed did\(^{141}\) - hinder the free flow of personal data throughout the Union.\(^{142}\) The main goal of the GDPR is thus to establish a consistent and homogenous data regime for the entire Union.\(^{143}\) This is achieved by the GDPR’s nature as a regulation, whereby any divergence from Member States must be justified.\(^{144}\) To put it simply: the Regulation aims to ensure a Digital Single Market,\(^{145}\) where consumers no longer have to be afraid to make purchases over the internet for fear of abuse of their personal information.\(^{146}\) The regulation hence also aims to achieve a high level of protection of natural persons.\(^{147}\)

After all, it is recognized that several forms of physical, material or non-material damage can result from


\(^{139}\) 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), L 119/1.

\(^{140}\) Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (The directive on protecting personal data processed for the purpose of criminal law enforcement), L 119/89.


\(^{142}\) Recital (9) GDPR.

\(^{143}\) Recital (10) and (13) GDPR.


\(^{146}\) Ibid., 45.

\(^{147}\) Recital (10) and (13) GDPR.
personal data processing, which threatens the rights and freedoms of the natural persons in question.\textsuperscript{148} At the same time, the free movement of personal data within the Union must be ensured.\textsuperscript{149}

Article 5 of the GDPR is absolutely vital to understand the Union’s renewed approach to personal data protection, since it contains the six essential principles regarding the processing of data: ‘lawfulness, fairness and transparency’, ‘purpose limitation’, ‘data minimization’, ‘accuracy’, ‘storage limitation’, ‘integrity and confidentiality’. Subsidiarity has become a central principle: personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means.\textsuperscript{150} The privacy of individuals is paramount; a controller should not acquire additional information about a non-identified data subject for the sole purpose of complying with the Regulation.\textsuperscript{151}

To ensure its broad scope, the GDPR stipulates explicitly that it does not only apply to automated processing, but also to other means of processing ‘which form part of a filing system or are intended to form part of a filing system’.\textsuperscript{152} A filing system is ‘any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis’.\textsuperscript{153}

Although the GDPR explicitly expresses the wish to provide natural persons with a high level of protection, it does not exist solely to their benefit. As mentioned before, the Regulation also aims to establish and protect the Digital Single Market, which is beneficial for enterprises since the further development of e-commerce stimulates business opportunities,\textsuperscript{154} and renews the data protection framework to provide more legal certainty and transparency.\textsuperscript{155}

The GDPR’s goal of benefitting enterprises is also translated into several provisions. For example, the size of enterprises is taken into account so as not to impose an unreasonable burden on micro, small and medium-sized businesses\textsuperscript{156} (SMEs). They enjoy a derogation with regard to record-keeping\textsuperscript{157} and ‘Union institutions and bodies, and Member States and their supervisory authorities, are encouraged to take account of the specific needs’ of these businesses when applying this Regulation.\textsuperscript{158}

Not all activities by private actors are considered in need of regulation. The ‘household exception’, which was already present in the 1995 Data Protection Directive, returns in the GDPR.\textsuperscript{159} This is the situation where a natural person processes personal data without any connection to a professional or commercial activity.\textsuperscript{160} This ‘could include correspondence and the holding of addresses, or social networking and

\textsuperscript{148} Recital (75) GDPR.
\textsuperscript{149} Article 1(3) GDPR.
\textsuperscript{150} Recital (39) GDPR.
\textsuperscript{151} Recital (57) GDPR.
\textsuperscript{152} Article 2(1) GDPR.
\textsuperscript{153} Article 4(6) GDPR.
\textsuperscript{155} Recital (13) GDPR.
\textsuperscript{156} Recital (13) GDPR; article 40(1) GDPR; article 42(1) GDPR. These categories are determined by the ‘Annex to Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises’ (20 May 2003) OJ 2003 L 124, 36, article 2.
\textsuperscript{157} Article 30(5) GDPR.
\textsuperscript{158} Recital (13) GDPR.
\textsuperscript{159} Article 2(2), (c) GDPR.
\textsuperscript{160} Recital (18) GDPR.
online activity undertaken within the context of such activities. Controllers or processors providing the processing means for such personal or household activities are not exempted from the Regulation.

An important nuance to all of the aforementioned is that the GDPR itself clearly recognizes the doctrinal and judicial views that personal data protection is not an absolute right, but must be balanced against other fundamental rights. To that end, it explicitly states:

This Regulation respects all fundamental rights and observes the freedoms and principles recognized in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.

This non-absolute character of the right to personal data protection is discussed later in this thesis (see ‘The right to personal data protection is not an absolute right’ on page 29 and further).

iii) Evaluating the GDPR

The GDPR brings a host of changes to the current data protection regime. Some of them have an enormous impact on the obligations of corporate actors and the rights for data subjects. The following is an overview of some of the key changes that the GDPR brings, and a brief evaluation thereof.

First, the GDPR finally establishes a clear regime regarding territorial jurisdiction. There are three possible situations in which the GDPR applies, as set out by its article 3, which are in line with the existing EU rules concerning consumer protection on the Internet. The first two paragraphs prove to be of most importance:

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

2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
   (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
   (b) the monitoring of their behavior as far as their behavior takes place within the Union.

With regards to paragraph one: the main establishment of a controller is where its central administration is situated, except if the decisions determining the purposes and means of processing are taken in

---

161 Recital (18) GDPR.
162 Recital (18) GDPR.
163 CJEU, Joined cases C-92/09 and C-93/09, Volker and Markus Schecke GbR and Hartmut Eifert v. Land Hessen, 9 November 2010, para. 48.
164 CJEU, C-275/08, Productores de Música de España (Promusicae) v. Telefónica de España SAU, 29 January 2008, para. 68; CJEU, Joined cases C-468/10 and C-469/10, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado, 24 November 2011, para. 48.
165 Recital (4) GDPR.
166 See: CJEU, Joined cases C-585/08 and C-144/09, Pammer and Hotel Alpenhof, 7 December 2010.
another establishment of this same controller somewhere else in the Union. Establishment implies the effective and real exercise of activity through stable arrangements; the legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor. Whether or not the processing of data is carried out there, is also irrelevant.

With regards to paragraph two: provision a) serves to ensure the protection of natural persons whenever a controller or processor envisages to offer services to data subjects in the Union. To establish that this is indeed the intention of a controller or intention, several factors can be taken into account: the possibility of ordering goods and services in a Member State language, the use of a currency which is generally used in one or more Member States, or when customers or users in the Union are mentioned. The mere accessibility of a website, the availability of an email address or general contact details or the use of a language generally used in the country of the controller’s establishment, do not suffice. For provision b) the existence of monitoring must first be ascertained. This is the case when:

(...) natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analyzing or predicting her or his personal preferences, behaviors and attitudes.

These rules concerning territorial jurisdiction have been adopted as the result of high-profile CJEU cases such as the Google Spain case (as will be discussed in the chapter ‘Enforcement’), which sought to address the jurisdictional uncertainties prevailing throughout the Union’s data protection regime. Key here was the concern that a company which provides a service in Europe would not need to obey to European law simply because its headquarters are not situated in the Union. The explicit jurisdictional provisions in the GDPR are set to alleviate many of the uncertainties that ruled before. This added legal certainty and predictability can only be encouraged. However, it must also be noted that the establishment of far-reaching EU jurisdiction can also have repercussions of a negative nature on the global nature of the worldwide web (see ‘Repercussions on corporate policy’ on page 47 and further of this thesis).

Second, the GDPR forms the debut of fines for the non-compliance with personal data protection. Each supervisory authority has the power to impose fines. Article 83 makes a distinction between major and minor infringements. Minor violations lead to a fine of €10 million or 2% of the total worldwide annual turnover, whichever is higher. Major violations lead to a fine of €20 million or 4% of the total worldwide annual turnover, whichever is higher. If the same - or linked - operations violate several provisions of the GDPR, the total fine cannot exceed the fine for the gravest violation. A minor infringement may also be corrected by a simple reprimand.

---

167 Recital (36) GDPR  
168 Recital (22) GDPR  
169 Recital (36) GDPR  
170 Recital (23) GDPR  
171 Recital (23) GDPR  
172 Recital (23) GDPR  
173 Recital (24) GDPR  
175 Article 58(2), i) GDPR.  
176 Article 83(4) GDPR.  
177 Article 83(5) GDPR.  
178 Article 83(3) GDPR.  
179 Recital (148) GDPR.
The introduction of fines is a clear statement by the Union that digital privacy protection is not a subject matter to be taken lightly. Instead of merely being a promotional boon or a philosophical topic, privacy protection now becomes a boardroom concern.\textsuperscript{180} Of course, while this must certainly be encouraged from the viewpoint of the data subject and as an aspect of corporate governance, it also causes major repercussions for corporate policy (see ‘Repercussions on corporate policy’ on page 47 and further of this thesis).

Third, corporations must now also pay more heed to the consent of the data subjects, as well as its withdrawal. Consent for one or more specific purposes is needed for processing to be lawful.\textsuperscript{181} Consent is ‘any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her’.\textsuperscript{182} This means that silence, pre-ticked boxes or inactivity are not sufficient to establish consent.\textsuperscript{183} It is up to the controller to prove that a data subject has consented,\textsuperscript{184} and the data subject can withdraw his or her consent at any time.\textsuperscript{185} The definition and explanations of consent are more extensive and clear than the previous one found in the Data Protection Directive,\textsuperscript{186} and hence very welcome and helpful.

Fourth, under article 33 there is a duty for data controllers to notify without undue delay the national data protection authorities about personal data breaches. These are ‘a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed’.\textsuperscript{187} While the Data Protection Directive already foresaw in such a duty, it did not always contribute to higher protection because of its indiscriminate generality.\textsuperscript{188} Therefore, the regulation focuses on processing operations ‘which are likely to result in a high risk to the rights and freedoms of natural persons by virtue of their nature, scope, context and purposes’.\textsuperscript{189} Bagatelle incidents, which are unlikely to pose a risk to the rights and freedoms of the individuals concerned, must not be communicated.\textsuperscript{190} This certainly alleviates the administrative burden for enterprises, and should be applauded. Furthermore, the notification duty does not exist merely for the telecom sector anymore, but now extends to all data controllers.\textsuperscript{191} This move also enjoyed widespread support.\textsuperscript{192}

\begin{itemize}
\item \textsuperscript{181} Article 6 (1), a) GDPR.
\item \textsuperscript{182} Article 4(11) GDPR.
\item \textsuperscript{183} Recital (32) GDPR.
\item \textsuperscript{184} Article 7(1) GDPR.
\item \textsuperscript{185} Article 7(3) GDPR.
\item \textsuperscript{186} Consent is ‘any freely given specific and informed indication of the data subject’s wishes’. See: Article 2 (h) Data Protection Directive.
\item \textsuperscript{187} Article 4(12) GDPR.
\item \textsuperscript{188} Recital (89) GDPR.
\item \textsuperscript{189} Recital (89) GDPR.
\item \textsuperscript{190} Article 33(1) GDPR.
\item \textsuperscript{191} Article 33(1) GDPR.
\end{itemize}
Fifth, enterprises must not only keep records of their processing activities, but they must now also appoint data protection officers where:

(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 [GDPR] and personal data relating to criminal convictions and offenses referred to in Article 10 [GDPR].

The officer is an expert in data protection law and practices, who assists the controller or processor in all data protection issues. At the very least, the officer must inform and advise, monitor GDPR compliance, assist in conducting a data protection impact assessment and cooperate and consult with supervisory authorities. Although the officer may be a staff member of the enterprise in question, they must be able to perform their responsibilities independently. Comparable to the introduction of fines, this decision will benefit the protection of data subject rights and the corporate governance standards of enterprises. However, it causes an extra administrative and financial burden that might affect corporate policy (see ‘Repercussions on corporate policy’ on page 47 and further of this thesis).

Sixth, the GDPR stresses privacy by design and by default, with article 25 entirely dedicated to these principles. Privacy by design is an internationally recognized approach to technology, meaning that data protection must be an inherent part of the design of a system and the default mode of conduct in any organization. The processing of personal data must take place in a manner that ensures ‘appropriate security and confidentiality of the personal data’, including the prevention of unauthorized access to or use of personal data. Although this approach thus seems paramount, it is somewhat dulled by article 32 and its required level of security for data processing:

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk (…)

Besides obvious worries about the general implementation of such a broad principle, some scholars have also expressed their doubts regarding privacy by default in the particular context of search engines,
claiming that it will ‘encourage politicians, celebrities and other public figures to put their lawyers on track when they find inconvenient information online’.204

Seventh, the right to be forgotten has been given a clear legal basis after its recognition by the CJEU in the Google Spain case (see ‘The right to be forgotten’ on page 31 and further of this thesis). Article 17 stipulates this as the ‘right to erasure’ and sums up six grounds where the controller must erase the personal data without undue delay. In general, the right exists if the retention of data by the controller violates the GDPR, EU law, or the laws of the Member States of the Union which apply to the controller.205 The usefulness of this right is emphasized regarding children, who were ‘not fully aware of the risks involved by the processing’ when they gave their consent and later want to remove this personal data.206 The GDPR aims to strengthen the practical implementation of the right to be forgotten by stating that the controller which is obliged to erase information shall also take ‘reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data’.207 The retention of data should not be considered unlawful in some instances, in particular ‘to the extent that processing is necessary (…) for exercising the right of freedom of expression and information’.208 This tension between the freedom of expression and information and the right to be forgotten, as well as the desirability of the right to be forgotten itself, is the subject of much debate (see ‘Digital privacy protection versus the right to freedom of expression and information: censorship?’ on page 38 and further of this thesis).

Eighth, the issue of profiling is given ample attention in the GDPR. Profiling is defined as

(...) any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.210

The GDPR understands the drastic consequences of profiling, such as targeted advertising. It wishes data subjects to be informed of the existence and consequences of profiling, as well as about the obligation of whether or not data must be provided and what the consequence would be of not doing so.211 Aside from the communication of general information under article 13(1), enterprises have added obligations under article 13 (2), f) as a result of profiling. In particular, they must provide the data subject with ‘meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject’.212 It does not end here. The GDPR also gives data subjects a ‘right to object’ profiling if it is related to direct marketing.213 Legal effects - or any decision which similarly significantly affects a data subject - based on profiling are absolutely not welcome under

204 N. Härtling, ‘Can a Search Engine be “Private by Default”?’, CR Online (14 May 2014) http://www.cr-online.de/blog/2014/05/14/can-a-search-engine-be-private-by-default/.
205 Recital (65) GDPR.
206 Recital (65) GDPR.
207 Article 17(2) GDPR.
208 Recital (65) GDPR.
209 Article 17(3), a) GDPR.
210 Article 17(3), a) GDPR.
211 Article 4(4) GDPR. The wording only differs slightly and non-significantly from that in recital (71) GDPR.
212 Recital (60) GDPR.
213 Article 13 (2), f) GDPR.
the GDPR. Examples would be ‘the automatic refusal of an online credit application or e-recruiting practices without any human intervention’. If profiling would be used, then inaccuracies must be corrected and the risk of errors must be minimized. Lastly, the European Data Protection Board, a Union body established by the GDPR, will provide guidance regarding profiling.

The fact that the GDPR wishes data subjects to pay attention to and have a say about profiling is certainly a good decision. Since the opaque technique of profiling can have an enormous impact on data subjects, it must be applauded that the GDPR wishes to address - with the lack of transparency generally being one of the largest issues concerning data processing by corporate actors. Just recently, the European Commission fined Facebook for providing misleading information that it would not match Facebook user accounts with Whatsapp phone numbers. Despite the European Commission purely concerns merger regulation, this complete lack of transparency and downright deception of customers raises enormous worries regarding privacy protection. Facebook has 1.94 billion accounts - a quarter of the world population - while Whatsapp only comes in a fraction lower, with 1.2 billion users. By coupling an individual’s separate accounts, Facebook gains extra data to compile a more complete profile. After all, data which is shared on Whatsapp but not on Facebook is combined, and vice versa. For example: if an individual would wish not to disclose a visit to Ireland on Facebook out of privacy concerns but instead communicates via private messages on Whatsapp when in Ireland, then the metadata connected to these messages will still enable Facebook to discover that the individual is in Ireland. This is a gross violation of the individual’s choice which information to disclose on which platform, which is a manifestation of the right to informational self-determination.

Lastly, the GDPR also dedicates attention to data protection impact assessments. These are introduced in article 35, where it stipulates the need for such an assessment where processing operations are likely to result in a high risk to the rights and freedoms of natural persons. To conclude that there is such a high risk, one must take into account the nature, scope, context and purposes of processing, while the use of new technologies can be of particular note. This assessment serves ‘to evaluate, in particular, the origin, nature, particularity and severity of that risk’ and the outcome ‘should be taken into account when determining the appropriate measures to be taken’. The stipulations concerning a data protection impact assessment should apply in particular to ‘large-scale processing operations which aim to process a considerable amount of personal data at regional, national or international level’.

---

214 Article 22(1) GDPR.
215 Recital (71) GDPR.
216 Recital (71) paragraph 2 GDPR:
217 Article 68 GDPR.
218 Recital (72) GDPR.
221 For the CJEU’s view on metadata, see: CJEU, Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB and Secretary of State for the Home Department, 21 December 2016.
222 CJEU, Joined cases C-293/12 and C-594/12, Digital Rights Ireland and Seitling and Others, 8 April 2014, Opinion of Advocate General Cruz Villalón.. It must be reminded that this thesis considers information self-determination as a manifestation of the right to privacy.
223 Article 35(1) GDPR.
224 Recital (84) GDPR.
supranational level and which could affect a large number of data subjects\textsuperscript{225} and three situations are of particular importance to conclude that an assessment must be carried out.\textsuperscript{226}

Data protection impact assessments can help raise awareness about the effects of processing operations among both data controllers and processors, and also among data subjects. Hence, they are essential to an enterprise’s corporate governance obligations and can help preventively reduce risks.

\textbf{B) Enforcement by the Court of Justice of the European Union}

Individuals can enforce their right to digital privacy protection. After all, and as mentioned before, articles 7 and 8 of the Charter of Fundamental Rights of the European Union consider privacy and personal data protection fundamental rights. As a result, they can be invoked before the Court of Justice of the European Union (CJEU).

Not only the jurisprudence of the CJEU - the main court of the European Union - is of importance. Where relevant, this section also discusses the case law of the European Court of Human Rights (ECtHR) as the major regional human rights body. Decisions of the ECtHR have an enormous impact on the general evolution of human rights protection, and, furthermore, the interpretation of the ECHR is of great importance to determine the content of European Union law. As article 52(3) of the Charter indicates:

\begin{quote}
\textit{In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection.}
\end{quote}

Article 7 of the Charter provides a general right to privacy\textsuperscript{227} and corresponds to article 8 of the ECHR. However, this raises the question in how far the right to personal data protection - which is closely linked to the right to privacy and other human rights\textsuperscript{228} - under article 8 of the Charter corresponds to the ECHR, even though it does not feature an explicit recognition of the protection of personal data. An answer might be found by turning towards article 53 of the Charter, which pertains to the level of protection of human rights:

\begin{quote}
\textit{Nothing in this Charter shall be interpreted as restricting or adversely affecting human rights and fundamental freedoms as recognized, in their respective fields of application, by Union law and international law and by international agreements to which the Union, the Community or all the Member States are party, including the European Convention for the Protection of Human Rights and Fundamental Freedoms, and by the Member States' constitutions}\textsuperscript{229}
\end{quote}

Thus, the protection of personal data under article 8 of the Charter cannot restrict or adversely affect the protection offered by the ECHR.

\textsuperscript{225} Recital (91) GDPR.
\textsuperscript{226} Article 35(3) GDPR.
\textsuperscript{227} Privacy has long since been recognized as a general principle of EU law by the CJEU. See: CJEU, Case C-136/79, National Panasonic v. Commission, 26 June 1980, paras 18-20.
\textsuperscript{228} See article 9 Data Protection Directive which recognizes the close ties between the right to personal data protection, the right to privacy and the freedom of expression.
\textsuperscript{229} Article 53 of the Charter.
Because the provisions of both instruments and the case law of both courts have become so closely interlinked, it is vital to investigate the approach of both sides with regard to digital privacy protection. This need is further strengthened by the presence of several explicitly corresponding rights of both the Charter and the ECHR that have the potential to clash with personal data protection, such as the freedom of expression found in article 11 of the Charter and article 10 of the ECHR.\textsuperscript{230}

First, the conclusions of both courts are presented that the right to personal data protection is not an absolute right \textit{(i)}. Also of great importance is the jurisdictional issue concerning data protection in the European Union \textit{(ii)} and the recognition of the ‘right to be forgotten’ in the context of search engines by the CJEU \textit{(iii)}. Lastly, future enforcement under the GDPR is briefly set out \textit{(iv)}.

\textit{i) The right to personal data protection is not an absolute right}

Central in the Court’s application of the right to personal data protection is the reasoning that a balancing exercise with other rights is necessary when applying and interpreting Article 8 of the Charter. This has been put into effect in the Satamedia case,\textsuperscript{231} in Promusicae v. Telefónica de España,\textsuperscript{232} as well as in ASNEF and FECEMD v. Estado.\textsuperscript{233} The need for a balancing act is a logical consequence of the fact that the fundamental right to the protection of personal data under Article 8 of the Charter ‘is not, however, an absolute right, but must be considered in relation to its function in society’.\textsuperscript{234} Through article 52(1) of the Charter these limitations must be provided for by law, respect the essence of the rights and freedoms in question and - subject to the principle of proportionality - must be necessary and genuinely meet objectives of general interest recognized by the European Union or the need to protect the rights and freedoms of others.\textsuperscript{235}

The aforementioned must be nuanced concerning the relationship between articles 8 and 11 of the Charter. The CJEU has made far-reaching statements concerning the right to be forgotten and the freedom of expression and information in the Google Spain case, which merit a separate consideration of the policy (see ‘The right to be forgotten’ on page 31) and a thorough analysis of the repercussions (see ‘Digital privacy protection versus the right to freedom of expression and information: censorship?’ on page 38 and further of this thesis).

Even though the ECHR does not have an explicit provision foreseeing a right to personal data protection, the ECtHR has interpreted Article 8 of the ECHR (the right to privacy) to include data protection.\textsuperscript{236} Therefore, the rules pertaining to article 8 can be transposed to consist of the ECtHR’s approach to digital privacy protection. And indeed, limitations to article 8 ECHR are possible here as well. As article 8, paragraph 2 states: a public authority shall not interfere with the right to privacy ‘except such as is in accordance with the law and is necessary in a democratic society’. It then lists a number of situations where derogations are possible:

\begin{itemize}
  \item \textsuperscript{230} See article 9 Data Protection Directive.
  \item \textsuperscript{231} CJEU, C-73/07, Tietosuojavaltuettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy, 16 December 2008, paras. 56, 61 and 62.
  \item \textsuperscript{232} CJEU, C-275/06, Productores de Música de España (Promusicae) v. Telefónica de España SAU, 29 January 2008, para. 68
  \item \textsuperscript{233} CJEU, Joined cases C-468/10 and C-469/10, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado, 24 November 2011, para. 48.
  \item \textsuperscript{234} CJEU, Joined cases C-92/09 and C-93/09, Volker and Markus Schecke GbR and Hartmut Eifert v. Land Hessen, 9 November 2010, para. 48.
  \item \textsuperscript{235} Ibid., para. 50.
  \item \textsuperscript{236} ECtHR, Rotaru v. Romania, No. 28341/95, 4 May 2000.
\end{itemize}
in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.\textsuperscript{237}

This balancing act under the ECHR of the right to privacy - and consequently the right to digital privacy - with the exercise of other rights has been confirmed on multiple occasions by recent case law, such as Vereinigung Bildender Künstler v. Austria,\textsuperscript{238} Mosley v. the UK,\textsuperscript{239} Axel Springer v. Germany,\textsuperscript{240} Von Hannover v. Germany and\textsuperscript{241} Társaság v. Hungary.\textsuperscript{242}

In conclusion, the CJEU recognizes that the right to personal data protection is not an absolute right. The ECtHR's case law supports this with regard to the right to privacy - and by extension the right to digital privacy.

\textit{ii) The jurisdictional issue}

One of the large issues concerning personal data protection was the fact that most data controllers and processors do not carry out their processing operations in the European Union. Thus, the jurisdiction of the CJEU was unclear for a considerable amount of time. The Google Spain case,\textsuperscript{243} however, drastically set a new standard concerning jurisdiction.

Google is a publicly traded company incorporated in Delaware, USA,\textsuperscript{244} with its head office situated in Mountain View, California. Google put forward the argument that since search services are carried out by Google Inc - with the Spanish division merely provides advertising support - the CJEU does not have jurisdiction.\textsuperscript{245} The Court disagreed with this reasoning. Key to the finding that it did indeed possess jurisdiction is that the EU legislation on personal data protection aims 'to prevent individuals from being deprived of the protection guaranteed by the directive and that protection from being circumvented, by prescribing a particularly broad territorial scope'.\textsuperscript{246} Google Spain came within the ambit of the Data Protection Directive since the processing of personal data must not be carried out by the establishment itself; article 4(1)(a) of the Data Protection Directive can apply if the processing takes place 'in the context of the activities of an establishment' when the controller exercises a real and effective activity through a stable arrangement in the territory of a Member State, even if that activity would only be minimal.\textsuperscript{247} The notion of 'in the context of the activities of an establishment' must not be interpreted restrictively.\textsuperscript{248} Even though Google Spain merely helps promote and sell the service, the Court finds that its activities are

\begin{footnotes}
\item[237] Article 8, para. 2 ECHR.
\item[238] ECtHR, Vereinigung bildender Künstler v. Austria, No. 68345/01, 25 January 2007, paras. 26 and 34.
\item[239] ECtHR, Mosley v. the United Kingdom, No. 48009/08, 10 May 2011, paras. 129 and 130.
\item[240] ECtHR, Axel Springer AG v. Germany, No. 39954/08, 7 February 2012, paras. 90 and 91.
\item[241] ECtHR, Von Hannover v. Germany (No. 2), Nos. 40660/08 and 60641/08, 7 February 2012.
\item[242] ECtHR, Társaság a Szabadságjogokért v. Hungary, No. 37374/05, 14 April 2009, see paras. 27 and 36-38.
\item[243] CJEU, Case C-131/12, Google Spain v. Agencia Española de Proteccion de Dato, May 13, 2014.
\item[245] Google Spain, para. 51.
\item[246] Google Spain, para. 54.
\item[247] CJEU, Case C-230/14, Weltimmo s.r.o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság, 1 October 2015, para. 31.
\item[248] Ibid., para. 25.
\end{footnotes}
inextricably linked to the activities of Google; they are the means which make Google ‘economically profitable’ and at the same time the search engine enables those activities to be performed.  

In a nutshell: the Court is concerned that a company providing a service in Europe would not have to comply with European law because its headquarters are situated outside of the Union. To gain jurisdiction, the Court used a technique described as ‘subsidiary jurisdiction’ through which a company based in a third State falls under EU jurisdiction if it has subsidiaries with the ‘nationality’ of an EU Member State. At the same time, the Court also notes that Google Spain is a subsidiary ‘which orientates its activity towards the inhabitants of that Member State’. The Directive is thus interpreted to apply whenever the data of European data subjects is processed, allowing the provisions of the Directive to bind data controllers outside of the EU and achieving an extraterritorial effect.

Although this finding of the Court was generally well received, it must be warned that this extremely broad notion of jurisdiction can have repercussions on the nature of the internet as a worldwide tool (see ‘Repercussions on corporate policy’ on page 47 and further).

iii) The right to be forgotten

It is the introduction of an enforceable ‘right to be forgotten’ for which the CJEU’s Google Spain case will - ironically - always be remembered. In it, mister Mario Costeja Gonzales sought to have Google erase search results concerning decade-old proceedings to recover social security debts. In his own words, he sought the ‘elimination of data that adversely affects people’s honor, dignity and exposes their private lives’. Simply put: he wanted certain information to be ‘forgotten’ by Google.

The Court agreed with Mr. Gonzales’ view that a search engine’s activities may significantly affect the rights to privacy and personal data protection. As a result, it recognized and applied the right to be forgotten, which can be defined as an individual’s entitlement ‘to restrict or terminate dissemination of personal data that he considers to be harmful or contrary to his interests’. Paragraph 94 is the key passage of the judgment:

Therefore, if it is found, following a request by the data subject (…) that the inclusion in the list of results displayed following a search made on the basis of his name of the links to web pages published lawfully by third parties and containing true information relating to him personally is (…)
This paragraph contains all the key elements regarding the right to be forgotten. First, the data subject can request a search engine for search results to be deleted under articles 12(b) and 14(1)(a) of the Data Protection Directive. Second, the right to be forgotten in the context of search engines concerns the results which are displayed when a search is made by using the data subject’s name. Third, the criteria for allowing the request is that the information must be inadequate, irrelevant or no longer relevant, or excessive. Fourth, the relevant information and links in the list of search results must be erased; this does not result in the removal of the name and information on the original web pages. Therefore, it would be more apt to speak of a ‘right to be delisted’.

With its decision, the Court went against the Opinion of Advocate General Jääskinen, who had noted his concerns that to hold Google responsible for the protection of the right to privacy and force the company to remove links from its search results would mean ‘sacrificing pivotal rights such as freedom of expression and information’. It can, however, be seen as an extension of earlier CJEU case law, where it had stated that, when seeking a balance between data protection and the freedom of the press, the derogations and limitations of the right to data protection must apply only insofar as is strictly necessary.

Nonetheless, the Google Spain judgment goes even further than this earlier case law. The Court indicates in the judgment itself how it aims to strike a balance between privacy and the freedom of expression in paragraph 97:

\[
\text{[the rights to privacy and personal data protection] override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in finding that information upon a search relating to the data subject's name. However, that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of inclusion in the list of results, access to the information in question.}
\]

Even though a (vague) exception is made if there is a ‘preponderant interest of the general public’ to having access to the information, the wording of the phrase before it is incredibly worrisome: the rights to privacy and personal data protection ‘override, as a rule (…) the interest of the general public in finding that information upon a search relating to the data subject's name’.

The judgment sparked a massive debate on the benefits and flaws of such a far-reaching right to be forgotten. A thorough analysis is provided further on (see ‘Digital privacy protection versus the right to freedom of expression and information: censorship?’ on page 38 and further of this thesis) but two other

\[260\] Google Spain, para. 94.
\[261\] Google Spain, para. 75.
\[263\] Google Spain, para. 82.
\[264\] Google Spain, Opinion of Advocate General Jääskinen, pt. 133.
aspects are of particular note. First of all, as noted before, the GDPR explicitly contains the right to be forgotten in its article 17. This means that, starting from 25 May 2018, the right to be forgotten will be a part of EU legislation. Article 17 lists an exhaustive set of grounds that trigger the right for the data subject to obtain erasure, which is clearly aimed at alleviating much of the uncertainty that the Google Spain judgment caused. However, it is too soon to tell whether or not the GDPR and the enforcement thereof will prove to be effective in guaranteeing a sound application of the right to be forgotten. Second, the CJEU has muddied the waters of its reasoning by recently deciding that there is no right to be forgotten concerning the personal data contained in the companies register, due to their public nature.266 Whereas the Google Spain case placed privacy above information, the Manni case places information above privacy. Thus, even the Court itself seems not yet sure about the exact application and scope of the right to be forgotten.

The ECtHR has been less explicit in recognizing the right to be forgotten. In the case of Segerstedt-Wiberg and Others267 it found that the continued storage of information about some of the individuals in the case at hand was a disproportionate interference with their right to respect for their private life; although the reasons for the interference were relevant, they were not deemed sufficient. Regarding the tension between the right to be forgotten and the freedom of expression and information, the ECtHR did provide more clarity recently on its stance by stipulating that the right to privacy and the right to freedom of expression deserve equal respect,268 although an evolution can be noted whereby the freedom of expression on the Internet is lower than the Court standard in non-digital freedom of expression cases.269 Nevertheless, when the ECtHR reconciles the right to digital privacy protection and the right to freedom of expression, it considers whether or not the expression at issue contributes to a debate of general public interest as a criterion.270

iv) Future enforcement under the GDPR

From 25 May 2018 onwards, natural persons can enforce the General Data Protection Regulation before a court of law. This is based on article 79 of the GDPR, which explicitly foresees an individual’s right to an effective judicial remedy against a controller or processor ‘where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation’.271 If an individual decides to bring such a claim against corporate actors, then he or she has a choice to either let the proceedings take place before the courts of the Member State where the controller or processor has an establishment, or before the courts of the Member State where the individual has his or her ‘habitual residence’.272 If material or non-material damage is suffered as a result of the infringement, then the individual is entitled to compensation from the controller or processor.273 Claims for compensation must be brought before the competent national courts.274

---

267 ECtHR, Segerstedt-Wiberg and Others v. Sweden, No. 62332/00, 6 June 2006.
268 ECtHR, Wegrzynowski and Smolczewski v. Poland, No. 33846/07, 16 July 2013, para. 56.
271 Article 79(1) GDPR.
272 Article 79(2) GDPR.
273 Article 82(1) GDPR.
274 Article 82(6) GDPR.
The GDPR makes a distinction in liability between the controller and the processor. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor, on the other hand, shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

Furthermore, article 80 of the GDPR gives individuals the right ‘to mandate a not-for-profit body, organization or association which (...) is active in the field of the protection of data subjects’ rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf’. Member States can also provide that these organizations can lodge complaints when it autonomously considers that a data subject’s rights under the regulation have been violated.

The explicit mention of a right to an effective judicial remedy in case of an infringement of the right to data protection is yet another strong sign that the Union is serious about its enforcement. The provision in article 80 will undoubtedly also prove to be useful; data protection procedures can be complex cases which would be too specialized and costly for an individual to carry. Yet, of course, a thorough analysis of the enforcement regime under the GDPR will only be possible once the regulation is put into practice from 25 May 2018 onwards. Still, its provisions provide hope for a strong yet thoughtful judicial application.

C) Lacunae

Although the combination of both legislation and enforcement by the CJEU forms a comprehensive framework for personal data protection, several lacunae still exist. First of all, the lack of regulation of legal persons under the GDPR is a disappointing decision (i). Second, care has to be taken not to overlook the rapid developments in the sector of Mobile Location Analytics (ii). Third, the special status of RFID technology deserves a brief reference (iii).

i) Legal persons

The GDPR does not apply to the processing of personal data concerning legal persons. This means that the name, the form, and the contact information of legal persons are not protected. In doing so, it follows the 1995 Data Protection Directive, which left this topic to national legislation, and the CJEU’s opinion that legal persons must be excluded from the right to data protection.

The decision to explicitly exclude legal persons from protection under the GDPR is not surprising, yet it harms the consistency of digital privacy protection in the EU. First, one of the basic goals of the GDPR is to harmonize the fractured regime of the Data Protection Directive. By again leaving the protection of legal persons up to national regulators, this is at least one aspect where the GDPR has already a priori failed to achieve harmonization. Second, although Convention 108 also deals with the data protection of natural persons in a comparable way, it at least acknowledges that States may wish to extend the rules

---

275 Recital (14) GDPR. Undertakings established as legal persons also do not enjoy protection.
277 Ibid.
278 Art. 80(2) GDPR.
contained in the convention to legal persons.\textsuperscript{281} The GDPR does no such thing. The risk thus exists that every national legislation will come up with wildly different rules. Lastly, and more dangerously, this exclusion by the GDPR stands in contrast to the approach taken by the ECtHR. Not only has the ECtHR found before that private and professional life are not easily distinguished,\textsuperscript{282} but it has accepted claims from legal persons under article 8 ECHR.\textsuperscript{283}

The Charter of Fundamental Rights and its article 7 and 8 also do not offer an easy solution to legal persons seeking legal redress since ‘(…) legal persons can claim the protection of Articles 7 and 8 of the Charter in relation to such identification only in so far as the official title of the legal person identifies one or more natural persons’.\textsuperscript{284} This refers, as indicated earlier, to the CJEU’s finding that only natural persons can rely on data protection.

When the GDPR enters into force in 2018, a dangerous gap between the personal data protection regimes in the EU and under the ECHR might thus emerge: legal persons will not be able to rely on the GDPR if they seek a judicial solution, and even the Charter only offers a limited amount of support. Instead, legal persons have to fall back on the ECHR and its enforcement before the ECtHR. However, this is only possible if State action would be involved in the dispute.

\textbf{ii) Mobile Location Analytics}

A more recent technological trend is that of Mobile Location Analytics (MLA), Where most of the attention concerning digital privacy protection is devoted to digital-only services, traditional brick and mortar stores are also adapting their sales methods by tracking foot traffic within their stores\textsuperscript{285} and monitoring general customer behavior.\textsuperscript{286} The UK’s Information Commissioner’s Office has already published guidelines on MLA-technology,\textsuperscript{287} but the European Union has not yet adopted any instruments regarding mobile location analytics specifically.

Mobile Location Analytics concern the collection and use of data via an exchange of communication between a store’s Wi-Fi network and a smartphone’s media access control (MAC), which is an identification code unique to each device.\textsuperscript{288} The worries regarding the use of this technology are threefold: the processing of the MAC can involve the processing of personal data, individuals are usually not aware that this processing is taking place, and there is a risk that the aggregation of the collected data can be used to identify individuals.\textsuperscript{289}

\textsuperscript{281} Article 3(2), b) Convention 108.
\textsuperscript{282} ECtHR, Amann v Switzerland, No. 27798/95, 16 February 2000, para. 65; ECtHR, Rotaru v. Romania, No. 28341/95, 4 May 2000, para. 43.
\textsuperscript{283} ECtHR, Bernh Larsen Holding AS and Others v. Norway, No. 24117/08, 14 March 2013.
\textsuperscript{284} CJEU, Joined cases C-92/09 and C-93/09, Volker and Markus Schecke GbR and Hartmut Eifert v. Land Hessen, 9 November 2010, para. 53.
As one of the most influential and successful mobile location analytics companies, Euclid’s chief marketing officer Adam Wilson assures that ‘the privacy of the individual is protected’. Yet it cannot be denied that Euclid’s practices balance on a very thin line. Euclid Express, the most basic of the company’s services, uses the basic method described earlier. The MAC unique to each phone is collected and subsequently scrambled to become anonymous. This data is then stored on the Euclid servers. But if a retailer pays for the advanced version of Euclid’s services, then Euclid’s own market data is added to this signal. As Wilson explains:

*So if a customer shows up at three different locations, it might be possible for us to infer information about gender, or about specific age range. There are ways in which we can look across the anonymous data set and even though we don’t collect any personally identifiable information, we might be able to predict their age.*

Big Brother Watch deputy director Emma Carr calls the technology ‘a clear example of profit trumping privacy’ and views the use of surveillance technology to provide a better or more personalized service as ‘totally disproportionate’. She further warns that ‘the long game is about identifying individuals and this technology is getting very close to enabling them to do that’. Euclid CEO Will Smith, from his side, assures that none of the collected information can ever be traced back to an individual. Furthermore, Euclid was among the companies agreeing to a Code of Conduct for mobile location analytics that demands transparency, limits the collection, retention and distribution of the collected data and foresees both opt-in and opt-out stipulations.

Yet caution seems more than warranted. Schwartz and Solove warn that information which appears on its face to be non-identifiable can increasingly be turned into identifiable data. This is done via ‘aggregation’, namely the combination of information which by itself does not qualify as ‘personal data’ or ‘personal identifiable information’, since it does not allow the identification of an individual, with other similar information to achieve a personalized result. Furthermore, it has been shown that, through aggregation, information produces more information. For example, by combining an individual’s birth date and birthplace, a social security number can be fairly reasonably predicted.

It has been suggested that a preemptive opt-out would be the ideal solution to prevent mobile location analytics from gaining information, because of its one-time-only and registered character. Furthermore,

---


291 Ibid.

292 Ibid.

293 Ibid.


299 Ibid.


the privacy by design approach - which is heavily emphasized in the GDPR - could also avoid the misuse of mobile location analytics. Nevertheless, the Union institutions should at the very least adopt guidelines or recommendations to deal with this new form of personal data use by corporate actors.

iii) Radio Frequency Identification (RFID)

Since 2009, the Union also recognized the importance and risks of RFID technology. These are small tags that can be attached to, for example, clothing and collect information for retailers to assess the level of demand for products. Clothing store Zara uses the tags to clearly view which fashions are selling well, and which ones are not. They are ‘passive’ since no personal information is collected, but the non-removal of a RFID label would raise privacy concerns since it could be tracked to a consumer’s home. Except in one instance, the GDPR does not mention the dangers of and rules pertaining to RFID. A separate instrument has instead decided that retailers must notify their customers that RFID tags are used and explain which information they collect. On one hand, the choice not to include these rules in the GDPR feels like a wasted opportunity to centralize all regulations concerning personal data protection. On the other hand, matters concerning RFID technology are sufficiently technical that they merit a separate instrument. Therefore, this omission in the GDPR cannot be viewed as a serious flaw.

---

303 ‘Commission recommendation on the implementation of privacy and data protection principles in applications supported by radio frequency identification’, European Commission (12 May 2009) O.J. L 122/47.
307 Ibid, 117.
308 Recital (30) GDPR.
4. Benefits, flaws and repercussions

The extensive legislation and enforcement by the European Union and its institutions has benefits, flaws and repercussions. Three main points are discussed. First, there is an enormous tension between the protection of digital privacy and the right to freedom of expression and information, leading to grave concerns regarding censorship (A). Second, due to several factors, the ‘worldwide’ nature of the Internet is at risk (B). Lastly, the Union’s legislation and enforcement concerning digital privacy has serious repercussions on corporate policy (C).

A) Digital privacy protection versus the right to freedom of expression and information: censorship?

"Letting bygones be bygones physically is not the only, and sometimes not even the main, strategy in digital contexts: there are also the edit and undo commands.

It is an unprecedented opportunity in human history, which we should not abuse, and that should not promote recklessness."

- Luciano Floridi

When the CJEU recognized and enforced the right to be forgotten in the Google Spain judgment, it did so with noble intentions: to address the Internet’s ability to indefinitely preserve all information about individuals, no matter how unfortunate or misleading.311 Recent, dramatic events in Italy have shown the potential destructive impact of this perpetual availability of information,312 and citizens have been asking to have information removed from Google en masse.313 The search engine giant has granted many of the requests, but in dealing with them it has also stumbled into another issue: the threat of censorship. Several UK news organizations objected upon Google’s removal of several links to their articles, claiming that ‘Google was being too hasty in allowing removal of searches against specific names for information that was not inaccurate, irrelevant or outdated’.314 How should the balancing between digital privacy protection and the freedom of expression take place then?

Personal data protection - whether considered as a standalone right or as a subset of privacy - and the freedom of expression and information are both fundamental rights under the Charter, and can be found respectively in article 8 and article 11(1). The latter reads:

Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.

Freedom of expression and information are basic elements of a society, ‘so that public matters can be discussed with impunity’.\textsuperscript{315} Yet, as has been mentioned before, the CJEU has stated that the rights to privacy and personal data protection ‘override, as a rule (…) the interest of the general public in finding that information upon a search relating to the data subject’s name’.\textsuperscript{316} This has led to several authors expressing their grave worries concerning such a far-reaching right to be forgotten vis-a-vis other fundamental rights,\textsuperscript{317} suggesting that the Court may have underestimated the implications of its judgment granting such an extreme degree of protection to personal data.\textsuperscript{318} The lack of explanation by the Court has been called worrisome, resulting in the judgment feeling incomplete.\textsuperscript{319}

And indeed, it seems like the Court did not consider the major implications of its judgment for article 11 of the Charter. After all, the parties enjoying protection under article 11(1) of the Charter in the context of a search engine are threefold. Not only is a searcher of information protected in his right to receive information, but an information provider should also be included in the index of the search engine so as to be able to reach an audience.\textsuperscript{320} Lastly, a search engine operator also enjoys protection,\textsuperscript{321} since their very nature of aiding in the search of information contributes to the ideals of the freedom of expression and a networked information environment.\textsuperscript{322} If privacy protection overrides the freedom of expression and information ‘as a rule’, then all of those parties are to some degree denied their fundamental right under article 11.

Authoritative voices such as ex-European Commission for Digital Agenda Neelie Kroes have emphasized the importance of the open nature of the Internet, and how it contributes to the freedom of expression and information.\textsuperscript{323} This is echoed by earlier findings of the ECtHR: the Internet enhances the access to news and facilitates ‘the sharing and dissemination of information generally’.\textsuperscript{324} The ECtHR has also expressed that the right to privacy and the right to freedom of expression deserve equal respect,\textsuperscript{325} and generally it tries to reconcile the right to digital privacy and the right to freedom of expression by considering whether or not the expression at issue contributes to a debate of general public interest as a criterion.\textsuperscript{326}

It should come as no surprise then that the right to be forgotten has fierce opponents. The CJEU’s Google Spain judgment has been called ‘erroneous’, ‘profoundly harmful to the operation of the internet’

\textsuperscript{315} US Supreme Court, Gregory v. City of Chicago, 394 U.S. 111, 125-126 (1969)
\textsuperscript{316} Google Spain, para. 97.
\textsuperscript{319} H. Järvinen, ‘ENDitorial: Google Spain vs AEPD – the cup is half full’, EDRI (21 May 2014) https://edri.org/enditorial-google-spain-vs-aepd-the-cup-is-half-full/.
\textsuperscript{324} ECtHR, Neij and Kolmisoppi v. Sweden, No. 40397/12, 19 February 2013, p. 9.
\textsuperscript{325} ECtHR, Wegrzynowski and Smolczewski v. Poland, No. 33846/07, 16 July 2013, para. 56.
and ‘a betrayal of Europe’s great legacy in protecting freedom of expression’.

Reporters Without Borders feared a world where information is manipulated on a large scale. MailOnline publisher Martin Clarke has been quoted as saying: “It [the right to be forgotten] is the equivalent of going into libraries and burning books you don’t like”. This analogy is, however, inaccurate. As explained before, web pages where the information was originally published are left unaltered; links are simply removed from the index of results when an individual requester’s name is used on a search engine. The original content can still be found by using search criteria that leave out the particular name. To clarify via an example:

A document called “Jonathan Zittrain foreclosure of 123 Main St” might be (...) ripe for removal as a result under “Jonathan Zittrain”, but not under “123 Main St foreclosure”.

A more apt analogy than that of Mr. Clarke would be that some books on the library shelves would not be ordered according to the alphabetical order of author names. The book has been put elsewhere, but the pages and words themselves are still fully intact. The relevant information simply becomes harder to find. Because of this, the right to be forgotten in its current form - which only removes links tied to a name and is still available via other means of searching - can also be seen to tip the scales back to how privacy used to exist. Personal information has always been available, but there used to be ‘a reasonable de facto expectation of privacy’ because it was hard to collect all the separate information. This is exactly what the removal of links tied to a name achieves: the pieces of information are not deleted, they just become harder to find because they must be looked up individually.

As a result, the right to be forgotten also has proponents. Some call the Google Spain judgment a reasonable interpretation of the Data Protection Directive and its privacy values. Although generally negative, Zittrain does point out the enormous importance of search engine results that ‘may do more than anything else in the world to define a stranger in others’ estimations’. This is echoed by Randazza and his statement that ‘the Internet has brought us a "mistakes are forever" society’, likening this

---


332 J. Zittrain, ‘Is the EU compelling Google to become about.me?’, Harvard Blogs (13 May 2014) http://blogs.harvard.edu/futureoftheinternet/2014/05/13/is-the-eu-compelling-google-to-become-about-me/.


permanent storage to totalitarian regimes.336 The American nonprofit organization Consumer Watchdog has also been trying to convince the US Federal Trade Commission to oblige Google to also introduce the right to be forgotten in the United States.337

What must not be overlooked, above all, is that the discussion on the balance between privacy and the freedom of expression and information is not a zero-sum game.338 It is not realistic, nor is it desirable, for either privacy or the freedom of expression to gain the upper hand. Instead, a fair balance between both on a case-by-case basis must be achieved.

This is also how the right to be forgotten is currently put into practice. Whereas certain categories of data are deleted by default (the display of national identification numbers, social security numbers, credit card numbers and images of signatures339), requests under the right to be forgotten are be assessed by Google on a case-by-case basis.340 Peter Barron, Google’s director of communication in Europe, has stated that the company is committed to acting responsibly and that it welcomes any feedback since they are ‘learning as we go’.341 Questions have been raised about the fairness of squarely placing such an enormous responsibility on a search engine - which is, in the end, merely an information location tool -342 and about the lack of accountability of entrusting a corporate actor with the task of deciding which public materials must be impeded access, without the participation of any other parties.343

There are not only obligations for search engines: Internet users are also expected to behave responsibly in making a request to be forgotten. Ryan Heath, the spokesman for Ms. Kroes, said the Google Spain ruling should not be an ‘open door for people to create more work for Google or Photoshop their own lives’.344

Much uncertainty about the right to be forgotten still exists, certainly for digital services other than search engines, such as social media.345 Twitter and Facebook store data that individuals provide to it, order it

---

336 M. Randazza, ‘We need a ‘right to be forgotten’ online’, CNN (15 May 2014) http://edition.cnn.com/2014/05/14/opinion/randazza-google-right-to-privacy.
on a web page and offer certain search functions, but is the collection of data by these services the same as a search engine performs? Additional case law is needed to provide further insight, although the Court’s wording in paragraph 21 of Google Spain is so broad in scope that it encompasses a wide arrange of online services.

Regarding future case law, it is important to make a distinction in the manifestation of the right to be forgotten. Currently, it has only been applied in the context of search engines, and the debate has mainly focused on the related tension between information being harder to find and censorship. But this is limited to an index of search results; the original content is left untouched. The application of the right to be forgotten would be even more controversial and problematic if a court would ever find that the right to be forgotten should be applied to original information. One such instance occurred in the German case of Werlé and Lauber v. Wikimedia, where two half-brothers requested to have their names removed from the Wikipedia page of the person of whose murder they had been found guilty. The German Constitutional Court refused this, stating that it would violate the freedom of press. A situation such as this also raises serious questions about the distortion of history, a fear that has been echoed by Wikipedia co-founder Jimmy Wales.

The GDPR is aware of the tension existing between personal data protection and the right to freedom of expression and information, and sets out the following in article 85:

1. Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.

2. For processing carried out for journalistic purposes or the purpose of academic artistic or literary expression, Member States shall provide for exemptions or derogations (...) if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information.

Yet it is important to understand that privacy does not have an inherently negative impact on the freedom of expression. Au contraire: the UN Special Rapporteur on Opinion and Expression has found that the right to privacy is a prerequisite to fully achieve the right to freedom of expression, since privacy incursions limit the exchange of ideas. To combat this idea of opposing rights and reinforce the notion of complimentary rights, Allen has suggested using the interpretative techniques of lex specialis and lex generalis on a case-by-case basis to achieve a fair balance between both rights.

---

347 J. Bruhn, ‘Does a murderer have a right to be forgotten?’, Free Speech Debate (16 November 2012) http://freespeechdebate.com/en/case/does-a-murderer-have-the-right-to-be-forgotten/.
350 Article 85 GDPR.
351 Ibid., [27].
The relationship between the right to digital privacy protection and the right to freedom of expression and information is not an easy one, and the effects of the right to be forgotten have certainly caused much debate. Only time will tell if the GDPR and future enforcement of digital privacy will achieve a proper balance between the right to privacy, and the right to expression and information. It is paramount that this balance is struck, since freedom of speech remains ‘the matrix, the indispensable condition, of nearly every other form of freedom’.\textsuperscript{354} Let us never forget that.

B. The end of the ‘worldwide’ web

It should be clear from the foregoing that the current European enforcement of data protection is strongly centralized and prioritizes privacy over freedom of expression. The right to be forgotten is the clearest manifestation of this preference. The situation differs greatly in the United States, where regulation is scattered and more value is attached to the freedom of speech contained in the First Amendment than the right to privacy.\textsuperscript{355} These different approaches lead to a dangerous situation: the regionalization of data protection, leading to a fracture of the worldwide web (i). At the same time, the far-reaching effects of the European Union’s approach and its migration of ideas could lead to a European digital colonization (ii).

i) The fracture of the worldwide web

The enforcement of the right to be forgotten in Europe means that the search results of search engines become altered.\textsuperscript{356} This is put into practice through the technique of geo-filtering, of which Zittrain identifies two models: the so-called ‘YouTube model’, where certain videos at universal youtube.com links are not accessible in certain jurisdictions when an IP address in that jurisdiction is recognized, and the ‘google.de model’, where links to neo-Nazi speech are removed from google.de but not from google.com, even when the user of google.com is in Germany.\textsuperscript{357} The first model uses the location of the user, whereas the second model uses different country-by-country versions of the same website.

Google used to implement requests under the right to be forgotten via the second model, meaning that search results were only removed from the national Google domain. Thus, if a French request to be ‘forgotten’ was granted, then the search results on google.fr were altered. However, the Article 29 Working Party communicated to Google that this ‘cannot be considered a sufficient means to comply with the [Google Spain] ruling.’\textsuperscript{358} In February 2016, Google then switched to the first model, meaning that URLs are delisted ‘from all European Google Search domains (google.fr, google.de, google.es, etc.) and use geolocation signals to restrict access to the URL from the country of the person requesting the removal’.\textsuperscript{359} Still, the French data regulator Commission Nationale de l'Informatique et des Libertés


\textsuperscript{355} V. Luckerson, ‘Americans Will Never Have the Right to Be Forgotten’, Time (May 14, 2014) \url{http://time.com/98554/right-to-be-forgotten/}.

\textsuperscript{356} R. Cellan-Jones, ‘Google agrees to forget’, BBC (20 May 2014) \url{http://www.bbc.co.uk/news/technology-27634746}.

\textsuperscript{357} J. Zittrain, ‘Is the EU compelling Google to become about.me?’, Harvard Blogs (13 May 2014) \url{http://blogs.harvard.edu/futureoftheinternet/2014/05/13/is-the-eu-compelling-google-to-become-about-me/}.


(CNIL) objected and reiterated that global filtering is the only way to fully enforce the right to be forgotten.\textsuperscript{360} The dispute has resulted in a legal procedure, which is still pending at the time of writing.

Kuner warned for an ‘EU internet’ if Google would only remove the relevant link for persons that are performing the search from the EU territory, but not for persons who are doing so while being physically outside the EU.\textsuperscript{361} By Google’s switch to the ‘Youtube model’, this is exactly what happened. European search results are different from those in the rest of the world, and the fragmentation of the Internet has become a reality. This means that the very nature of the Internet as a ‘worldwide’ source of information is threatened.

It is the transnational nature of the internet makes regionalized protection such an inherently incompatible concept.\textsuperscript{362} Warnings that traditional ‘principles of international jurisdiction, particularly territoriality’ cannot be applied to the internet since the internet is an ‘environment of geographic anonymity’ have long since been spread.\textsuperscript{363} Furthermore, due to cloud computing services, the physical equipment used for the storage and transfer of personal data could in theory be located everywhere in the world.\textsuperscript{364}

However, not all scholars have the same view on fragmentation. Floridi states that the word ‘fragmented’ may just be a synonym of ‘distributed’ and that when ‘branches of the same bank or supermarket offer different services and products, we speak of variety, pluralism, and competition, so the problem is not fragmentation in itself’.\textsuperscript{365} He warns instead for a balkanization where commercial, political, or juridical agents would impose an informational monopoly on a region.\textsuperscript{366}

This leads to the topic discussed earlier which is so strongly interlinked with the CJEU’s enforcement of the right to privacy: the freedom of expression and information. After all, the most unwanted effect of the Court’s right to be forgotten means that it goes against article 11 of the Charter, Article 19 of the Universal Declaration of Human Rights and Article 19 of the International Covenant on Civil and Political Rights, which state that there is a right to freedom of expression and information, regardless of frontiers. European citizens would be limited in their right to information by being within the European Union.

This fragmentation could be avoided, or at the very least corrected, if there was a strong global approach to data protection. Alas, the major differences in how data protection is approached in the European Union and in the United States are absolutely not beneficial in avoiding fragmentation. The EU’s approach to digital privacy protection stems from the European Union itself. There are a limited number of instruments (such as the GDPR and the ePrivacy Directive) adopted by the core institutions of the Union, with Member States only having limited competence to regulate a select few topics - which are mostly extensions of basic rules laid down in the regulation. These instruments flow forth from two central sources: the Charter of Fundamental Rights, which sets out both the right to privacy and the right to

\textsuperscript{360} A. Hern, ‘Google takes right to be forgotten battle to France’s highest court’, The Guardian (19 May 2016) \url{https://www.theguardian.com/technology/2016/may/19/google-right-to-be-forgotten-fight-france-highest-court}.
\textsuperscript{366} Ibid.
personal data protection, and article 16 of the Treaty on the Functioning of the European Union. The regulatory competence in the United States, on the other hand, is scattered. There is no federal law creating a broad data protection regime, but rather separate pieces of federal legislation aimed at addressing issues in specific industries such as the Telemarketing and Consumer Fraud and Abuse Prevention Act, the Children’s Online Privacy Protection Act and the Identity Theft Assumption and Deterrence Act. Furthermore, the states themselves are also competent in creating data protection legislation, resulting in for example 48 different data breach notifications statutes (at the time of writing). This means that there is a sharp juxtaposition between the industry-wide, centralized approach in the EU and the sectorial, de-centralized approach in the US.

The European Union’s strong-handed approach on the one hand, and the United States’ seeming indecisiveness on the other, create a chaotic global situation. The need for international regulation is becoming increasingly clear, as evidenced by calls from both the OECD and the Conference of International Data Protection Commissioners for an international binding agreement concerning personal data processing.

The Google Spain judgment and its right to be forgotten have effectively established an Internet regime in Europe which differs from the rest of the world. This fracture of the worldwide web is a threat to the basic freedom of information, which should know no frontiers. Furthermore, the different regulatory approaches to data protection in the EU and the US make matters worse. Without a clear global regime, the worldwide web will become fractured and, ultimately, completely regionalized.

ii) The risk of European digital colonization

There is not only a danger of the internet becoming fractured, but at the same time there is a risk of - for lack of a better word - colonization of the internet by the European Union. This is the result of two factors. First of all, the global enforcement of the Union’s right to be forgotten, and second, the migration of European ideas.

As mentioned before, the European Union wishes for the right to be forgotten to be enforced globally: the Article 29 Working Party has contacted Google and requested that ‘de-listing should also be effective on all

relevant domains, including [google].com. When Google switched to the so-called ‘Youtube-model’, the French data regulator Commission Nationale de l’Informatique et des Libertés (CNIL) reacted by emphasizing global filtering. Yet orders to alter operations worldwide can have serious consequences. One of the risks would be that when a national court enforces worldwide compliance with a national rule, this compliance in the view of one jurisdiction might create an illegal situation in another jurisdiction. The 2001 Yahoo case illustrates this: Yahoo filed a complaint in California against a French court order which forbade the display of Nazi artifacts via Yahoo’s auction service. The California Court found that, while the US recognizes and enforces foreign judgments, the enforcement of the present French case would violate the constitutional right to free speech that Yahoo possesses under the First Amendment.

The courts have yet to decide if global filtering concerning Google’s search results is indeed necessary, but if this would be the case, then there seems to be no turning back from a global enforcement of the European Union’s right to be forgotten. This stands in stark contrast with the situation in the United States, where courts have concluded that the right to be forgotten is not even recognized. The passive approach of the US (which can also be brought back to the scattered regulation concerning data protection, which has been discussed before) results in a lack of counterweight to the EU’s (over)active policy. Thus, by globally enforcing the removal of information after a request from a European individual, the European policy is more or less forced upon the world.

This effect is most noticeable when the CJEU’s boundary between the acceptance of a request ‘to be forgotten’, and a denial of such a request is examined. The Court states that a request can be denied ‘if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of inclusion in the list of results, access to the information in question’. What is the exact boundary then to conclude a ‘preponderant interest of the general public’ from a global point of view? When does the right to information for a random citizen - say for someone from Bangladesh - end concerning a European individual? Is there a ‘preponderant interest of the general public’ for a politician? Probably, yes. But what about a criminal? Is there such a preponderant interest in Bangladesh concerning a European murderer? It is extremely hard to draw a clear line within Europe, let alone in a foreign country or on a global scale. By globally enforcing the erasure of search results, the European Union would decide what information should be easily available and which should be more difficult to obtain, on a worldwide scale. The Union would effectively become the information police of the world.

The second factor that contributes to the European digital colonization is the migration of the CJEU’s approach and ideas. Simply because a court of such enormous importance has delivered judgments in a field where there is still much uncertainty, courts outside the EU extensively rely on the CJEU's reasoning to increase their own judgments’ legitimacy and persuasiveness. This can be seen for example in the

381 Google Spain, para. 97.
remarkable Canadian case of Equustek Solutions Inc. v. Jack before the Supreme Court of British Columbia, where the Court also forced Google to delete search results. In a way, the court took matters even further than the CJEU did in the Google Spain case, since it did not simply indicate in vague terms that search results had to be delisted, but explicitly noted that not merely the results on ‘google.ca’ but also on ‘google.com’ had to be deleted. Furthermore, it stated that every State in the world could possibly have jurisdiction over Google’s search services, as a result of it conducting business on a global scale.\textsuperscript{384} The British Columbia Court of Appeal confirmed this judgment.\textsuperscript{385}

While it should be applauded that courts pay heed to the decisions of other courts, it is worrisome that the Canadian courts decided to follow a judgment as controversial and widely critiqued as Google Spain, which can have such far-reaching consequences. Only time will tell if other courts are as eager to follow this same approach, but it forms a clear first step for the domination of the European approach.

C) Repercussions on corporate policy

The Union’s personal data legislation and enforcement has serious repercussions on corporate policy, while the impact of future decisions could be even more substantial.

The right to be forgotten creates enormous burdens for the private actors currently bound by it. If even an organization with a near-infinite pool of resources such as Google struggles to evaluate all deletion requests for putting the right to be forgotten into practice (as has been discussed before) then a possible future extension of this right could create an unbearable burden for smaller actors. Sandefur therefore proposes a Centralized Data Protection Agency to receive erasure requests, which would result in a number of important benefits: a specialized agency would weigh the private and public interests at stake, citizens can now direct their request to a single authority, Member States would not implement conflicting solutions, and companies would be relieved from making legal privacy decisions.\textsuperscript{386} This would certainly prove to be a viable solution if other corporate actors than search engines would ever have to comply with the right to be forgotten.

Also problematic in the particular context of search engines, is the difference in treatment that the right to be forgotten in its current incarnation causes. Procedurally, the CJEU claimed jurisdiction in the Google Spain case because Google sells advertisements targeted at EU customers, and has ‘boots on the ground (a corporate subsidiary, servers, salespeople, etc.) in Europe’, yet sites which don’t have any operations outside the US (for example the much smaller DuckDuckGo) steer clear of the CJEU’s gaze, even though their services can be accessed in Europe and they might provide the exact same information as bigger search engines.\textsuperscript{387}

The impact of the GDPR can also not be understated. Its end goal is to establish a Digital Single Market within the European Union, which the European Commission describes as an environment where citizens, individuals and businesses enjoy fair competition and a high level of data protection while

\textsuperscript{384} Ibid., para. 64
\textsuperscript{387} J. Zittrain, ‘Is the EU compelling Google to become about.me?’, Harvard Blogs (13 May 2014) http://blogs.harvard.edu/futureoftheinternet/2014/05/13/is-the-eu-compelling-google-to-become-about-me/.
exercising their online activities.\textsuperscript{388} The result of this would be ‘up to €415 billion in additional growth, hundreds of thousands of new jobs, and a vibrant knowledge-based society’.\textsuperscript{389} The reform and harmonization is projected to reduce administrative burdens with €2.9 billion per year, whereas the cost of compliance with the GDPR is expected to be €580 million; complying with the data breach reporting obligations will cost a further €20 million.\textsuperscript{390}

These cost projections have been called into question. Other research has claimed that the introduction of the GDPR will increase the annual costs for SMEs by up to €7.2 million; this boils down to between 16 and 40 per cent of the annual average IT budgets of these businesses.\textsuperscript{391} Furthermore, regarding the looming GDPR deadline of 25 May 2018, there is great unrest. A survey among 900 executives globally has shown that 47 percent of these global organizations doubt whether or not they will be able to comply with the GDPR when the deadline is reached.\textsuperscript{392} The major concern seems to be regarding ‘what data types enterprises have and where it is stored’, with 39 percent of the business claiming to be unable to locate and identify relevant data.\textsuperscript{393}

Notwithstanding these fears, the hope prevails that the GDPR will put governments outside the Union under pressure to raise their data protection standards so that their economies are allowed access to the digital single market of the EU.\textsuperscript{394} At the moment, the international disparities in data protection create substantial costs for enterprises, which have to comply with different legal requirements of different nations.\textsuperscript{395}

Another effect of the GDPR is that its strict approach to data handling incentivizes companies to maintain higher standards regarding personal data protection in two ways. First of all, the extensive media attention that the GDPR has received means that non-compliance with its provisions could result in a PR disaster with severe damage to a corporation’s reputation. Secondly, the fines foreseen by the GDPR are of such a magnitude that they become an integral part of the financial planning of companies; even a CEO’s attention will be drawn towards personal data protection.\textsuperscript{396} Information Commissioner Elizabeth Denham summarizes these two points as follows:

\begin{itemize}
\item[\textsuperscript{393}] Ibid.
\end{itemize}
If an organization can’t demonstrate that good data protection is a cornerstone of their business policy and practices, they’re leaving themselves open to enforcement action that can damage their public reputation and possibly their bank balance. That makes data protection a boardroom issue.\textsuperscript{397}

While one could argue that this is a benefit, it is not unimaginable that the stricter approach and the extensive sanctions could also have negative repercussions on corporate policy and scare off future investments in Europe. Corporations would also in a great deal lose their advantage concerning information asymmetries, which data protection legislation aims to correct.\textsuperscript{398}

This problem is further highlighted by the many extra administrative obligations that the introduction of both the GDPR and the proposal for a revision of the ePrivacy Directive pose on corporations. The latter, for example, will also make the top services such as Skype and WhatsApp adhere to stricter rules regarding the confidentiality of communication. Until now, only traditional telecommunication companies were bound by these rules. Yet this can also be seen as a breakthrough in the positive sense, closing the gap between over the top services and traditional companies.\textsuperscript{399} At the same time, strict compliance with these obligations would also form a savvy marketing strategy to persuade cautious consumers into becoming customers by flaunting with a product’s high privacy standards.\textsuperscript{400}

The right to be forgotten could possible pose a great burden on a plethora of corporate actors if it would be extended in the future. The same can already be said about the GDPR and the proposed update of the ePrivacy Directive: some of its provisions create a heavy administrative burden for corporations. Yet at the same time, there is also optimism concerning the stimulation of businesses through a more solid data protection framework and the digital single market. Compliance can also be smartly used as a marketing tool.


5. Conclusion

Digital services are now an essential part of our lives. As a result, the corporate actors behind them have gained an enormous grip on our personal data. Technological evolutions have created precise and far-reaching means of collecting and subsequently using this very data for advertising, creating an industry where information is currency. Both online and offline, drastic and obscure methods of using and gathering data have raised concerns regarding privacy intrusions. The European Union recognizes these concerns, and has taken action as a result. This raises three important questions. What is the exact legal reasoning behind protecting personal data? What legislative measures does the EU set out for corporate actors regarding digital privacy protection and how is it enforced? And what are the repercussions of European Union’s policy?

This research started with an investigation. Why does personal data merit protection and what is ‘digital privacy protection’ precisely? Even though the term privacy itself is hard to define, it became a part of the pantheon of human rights through codification in the UDHR, the ECHR and the ICCPR. These instruments share elements which allow us to formulate a ‘classic’ definition of privacy: an individual has the right to respect for his or her privacy, family, home or correspondence, and shall not be subjected to arbitrary or unlawful interference with this right. When automatic data processing emerged and massive amounts of personal data became easily available, the OECD, the Council of Europe, the Human Rights Committee and the European Union understood that privacy needed extra protection. Their combined efforts led to a right to digital privacy protection, which can be defined as the protection of the fundamental rights and freedoms of an individual regarding the processing of his or her personal data - in particular concerning a person’s private life - whether by public authorities or private individuals or bodies.

There is, however, discussion as to whether or not personal data protection is a subset of privacy, or a standalone right. Several European Union instruments - such as the Charter and the General Data Protection Regulation - treat it as a standalone right, even though the extensive case law of the Court of Justice of the European Union does not support this. National judicial decisions do not offer a decisive answer, owed to their support for both approaches, while legal scholars are also divided on this issue. Nevertheless, this research views data protection as a tool to accomplish greater privacy, and not as a standalone right. To that end, several arguments of the pro-standalone side are refuted.

It must be emphasized that this thesis deals with digital privacy protection against corporate actors, and not against States. All data protection instruments clearly recognize that not only States, but also private parties must respect the right to privacy in relation to the automated processing of data. Furthermore, States have positive obligations to protect and fulfill the right to privacy towards its citizens. This includes taking legislative measures with regards to personal data protection, as well as enforcing such a regime. Because of its wealth of legislation and judgments pertaining to digital privacy protection, the choice was made to study the policy and effects of digital privacy protection in the European Union.

Chapter three took a descriptive approach. Starting with the European Union’s legislation concerning data protection, two regimes can be distinguished. The ‘old’ regime under the Data Protection Directive had a scope limited to the internal market and sought to harmonize national legislation. Due to its nature as a directive, this goal was not fully achieved. A host of other, complimentary instruments were also adopted - such as the ePrivacy Directive - but the most significant event occurred when the Charter of Fundamental Rights was elevated to the rank of EU primary law in 2009. Its articles 7 and 8 set out, respectively, the right to privacy and the right to personal data protection. In any event, 25 May 2018 will prove to be the start of the ‘new’ personal data protection regime in Europe. The General Data Protection
Regulation (GDPR) aims to establish a Digital Single Market, which both stimulates businesses and foresees a high level of protection for natural persons.

The GDPR introduces some key changes to the Union’s data protection policy. The clear rules regarding territorial jurisdiction are arguably most important, but the effect of the introduction of fines for non-compliance, the clearer need for consent of data subjects, a stricter notification regime and the appointment of data protection offers can also not be underestimated. Furthermore, the GDPR explicitly recognizes the principles of privacy by design and by default, codifies the Google Spain case’s right to be forgotten, imposes strict rules concerning profiling and sets out conditions in which to conduct data protection impact assessments. Although it should be applauded that the GDPR devotes much attention to important topics such as profiling and many of the new obligations - such as data protection impact assessments - can have a positive influence on an enterprises’ corporate governance duties, the practical implementation of some stipulations (e.g. privacy by design and default) causes uncertainty. Furthermore, the status and desirability of the right to be forgotten is so extremely controversial, that its inclusion in the GDPR seems like a rash decision.

The enforcement of the right to digital privacy protection by the Court of Justice of the European Union (CJEU) is also essential to understand how data protection is put into practice. The influence of the case law by the European Court of Human Rights cannot be understated in this regard. Four aspects regarding enforcement are discussed. First, the CJEU has stated that the right to personal data protection is not an absolute right and must be balanced with other rights - a view supported by the ECtHR. Second, the CJEU has cleared up doubts regarding its jurisdiction by making use of several extension techniques. Third, in the Google Spain case, the CJEU found that there is a right to be forgotten with regards to search engines when several conditions apply; the ECtHR is much less explicit in its recognition of a right to be forgotten. Fourth, the future judicial enforcement under the GDPR is briefly discussed.

Notwithstanding the extensive legislation and enforcement, there are three topics that can be considered lacunae in the data protection regime of the Union. The lack of protection of legal persons is a first consideration. The GDPR foresees no harmonization in this regard, nor does it encourage States to adopt similar rules. Second, the rapidly evolving market of Mobile Location Analytics and their obscure ways of data collection can also not be ignored. It would be advisable for the Union to take legislative action in this regard. Lastly, the GDPR is a missed opportunity for the Union to gather its disparate regulation concerning Radio Frequency Identification (RFID) technology in a single instrument.

Chapter four analyzes the benefits, flaws and repercussions of the EU policy on personal data protection. The tension between digital privacy and the freedom of expression and information is explored, particularly concerning the far-reaching right to be forgotten. It seems that the Court underestimated the enormous implications of its Google Spain judgment, which is backed up by the many fierce opponents of the ruling. At the same time, some of their statements must be nuanced. The proponents of the right to be forgotten are also given a voice, and - above all - it is stressed that the discussion should not be a battle between wrong and right, but a dialogue to find an appropriate balancing of rights and interests. The GDPR tries to stimulate this dialogue with its explicit provision in article 85, but only time will tell if this achieves a proper balance in practice.

One of the most alarming findings is that the ‘worldwide’ nature of the Internet is in danger. On one hand, there is already a fracture of the worldwide web. The Internet in Europe is effectively different from the rest of the world because of how the right to be forgotten is put into practice via geo-localization. The lack of any global data regime is sorely felt in this regard, and this is in a large part due to the weak position of

51
the United States; its scattershot regulation of data protection prevents it from developing a strong international view. On the other hand, there is a serious risk of European digital ‘colonization’. Through the global enforcement of the right to be forgotten, Europe is positioning itself as the information police of the world. Due to the absence of the US on the global scale, there is no counterweight to the Union’s policy. At the same time, the ideas of the CJEU are migrating to other jurisdictions. The Canadian case of Equustek shows that even controversial judgments such as Google Spain can be copied in fields where the judges themselves are unsure what to do, thereby simply relying on the authority of a CJEU judgment.

Lastly, the Union’s legislation and enforcement has serious repercussions on corporate policy. Both the right to be forgotten and many provisions of the GDPR create enormous administrative and financial burdens for enterprises. Even though the Commission calculated optimistic financial growth as a result of the reforms, other studies have projected extra costs for corporations. Furthermore, the stricter rules and the introduction of fines might scare off companies looking to invest in the Union. At the same time, there is no doubt that data subjects will benefit from the added protection, and that enterprises can also use compliance with the regulations to their advantage.

In conclusion, the European Union has a wealth of legislation and enforcement in the field of personal data protection, born out of concern for data subjects’ digital privacy. The GDPR is bound to drastically renew the regulatory framework, while questions raised by controversial CJEU cases might see some resolution because of these sweeping changes. At the same time, there is a chance that these problems escalate even further. It is paramount then that the benefits, but also the flaws and the repercussions of the European Union’s policy should not be ignored. Above all, a fair balancing of all fundamental rights must be sought and ensured.
Bibliography

1. International instruments

A) OECD


B) Council of Europe


C) Other


International Covenant on Civil and Political Rights (ICCPR), 16 December 1966, UNTS vol. 999, 171.


2. Legislation

A) EU legislation

Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281, 31.

Regulation (EC) No. 45/2001 on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data, OJ 2001 L 8.


Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic
communications services or of public communications networks and amending Directive 2002/58/EC, OJ 2006 L 105, invalidated on 8 April 2014;


Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, L 119/89.

B) United States legislation


3. EU documents

A) European Commission

‘Commission recommendation on the implementation of privacy and data protection principles in applications supported by radio frequency identification’, European Commission (12 May 2009) O.J. L 122/47.


B) Article 29 Working Party


C) Miscellaneous


4. Judicial decisions

A) Court of Justice of the European Union


CJEU, Joined cases C-465/00, C-138/01 and C-139/01 Rechnungshof v. Österreichischer Rundfunk and Others and Neukomm and Lauermann v. Österreichischer Rundfunk, 20 May 2003.

CJEU, C-275/06, Productores de Música de España (Promusicae) v. Telefónica de España SAU, 29 January 2008.


CJEU, C-28/08, European Commission v Bavarian Lager, 29 June 2010.

CJEU, Joined cases C-92/09 and C-93/09, Volker and Markus Schecke GbR and Hartmut Eifert v. Land Hessen, 9 November 2010.

CJEU, Joined cases C-468/10 and C-469/10, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado, 24 November 2011.

CJEU, C-176/12, AMS v. Union locale des syndicats CGT and Ors, 15 January 2014.

CJEU, Joined cases C-293/12 and C-594/12, Digital Rights Ireland and Seitling and Others, 8 April 2014.

CJEU, C-131/12, Google Spain, S.L., Google Inc. v. Agencia Española de Proteccion de Datos, 13 May 2014.

CJEU, C-212/13, Frantisek Rynes v Urad pro ochranu osobnich udaju, 11 December 2014.

CJEU, Case C-230/14, Weltimmo s.r.o. v. Nemzeti Adatvédelmi és Információszsabadsag Hatósag, 1 October 2015.

CJEU, C-362/14, Maximillian Schrems v. Data Protection Commissioner, 6 October 2015.


B) Opinions of the Advocates General at the Court of Justice of the European Union

CJEU, Joined cases C-92/09 and C-93/09, Volker and Markus Schecke GbR and Hartmut Eifert v. Land Hessen, 9 November 2010, Opinion of Advocate General Sharpston.
C) General Court

General Court (Third Chamber), T-194/04, Bavarian Lager v. Commission, 8 November 2007.

D) ECtHR


ECtHR, Amann v Switzerland, No. 27798/95, 16 February 2000.

ECtHR, Rotaru v. Romania, No. 28341/95, 4 May 2000.

ECtHR, Segerstedt-Wiberg and Others v. Sweden, No. 62332/00, 6 June 2006.


ECtHR, Társaság a Szabadságjogokért v. Hungary, No. 37374/05, 14 April 2009.

ECtHR, Mosley v. the United Kingdom, No. 48009/08, 10 May 2011.

ECtHR, Axel Springer AG v. Germany, No. 39954/08, 7 February 2012.

ECtHR, Von Hannover v. Germany (No. 2), Nos. 40660/08 and 60641/08, 7 February 2012.

ECtHR, Fredrik Neij and Peter Sunde Kolmisoppi v. Sweden, No. 40397/12, 19 February 2013.


ECtHR, Wegrzynowski and Smolczewski v. Poland, No. 33846/07, 16 July 2013.


D) United States


E) Germany
5. Doctrine

A) Books


Solove, D.J., Understanding Privacy (Harvard University Press, 2008).


B) Articles


C) Contributions


D) Blogs


Härting, N., ‘Can a Search Engine be “Private by Default”?’, CR Online (14 May 2014) http://www.cr-online.de/blog/2014/05/14/can-a-search-engine-be-private-by-default/.


Zittrain, J., ‘Is the EU compelling Google to become about.me?’, Harvard Blogs (13 May 2014) http://blogs.harvard.edu/futureoftheinternet/2014/05/13/is-the-eu-compelling-google-to-become-about-me/.
6. Press


Randazza, M., ‘We need a ‘right to be forgotten’ online’, CNN (15 May 2014) http://edition.cnn.com/2014/05/14/opinion/randazza-google-right-to-privacy.


7. Other

A) Speeches


B) Google


C) International Conference of Data Protection and Privacy Commissioners


D) Future of Privacy Forum


E) United Nations


F) Eurobaromater


**G) Miscellaneous**


DLA Piper LLP, 'Preparing for the GDPR: New employee data subject rights could disrupt core HR procedures', Lexology (18 April 2017) [http://www.lexology.com/library/detail.aspx?g=dcbc5cf7-6b07-4017-9ad4-3b8e78d7dc5b](http://www.lexology.com/library/detail.aspx?g=dcbc5cf7-6b07-4017-9ad4-3b8e78d7dc5b).
Digitale diensten vormen een essentieel deel van onze moderne levenswijze. Als gevolg daarvan hebben de bedrijven verantwoordelijk voor deze diensten onze persoonlijke gegevens in hun greep. Technologische evoluties hebben tot precieze en verregaande middelen geleid om deze gegevens te verzamelen en vervolgens te gebruiken voor advertenties, wat resulteert in een industrie waar informatie gelijk staat aan geld. Zowel online als offline roepen de obscure methodes tot het vergaren en gebruiken van deze gegevens vragen op omtrent privacy. De Europese Unie erkent deze zorgen en heeft als gevolg actie ondernomen. Dat leidt tot drie belangrijke vragen. Wat is de juridische grondslag tot het beschermen van persoonlijke data? Welke wetgevende maatregelen heeft de Unie uiteengezet voor bedrijven inzake databescherming en hoe wordt dit afgedwongen? En wat zijn de gevolgen van dit beleid?

Deze thesis begint met een onderzoek. Waarom verdient persoonlijke data bescherming en wat houdt ‘digitale privacy bescherming’ in? Hoewel het begrip privacy moeilijk te definiëren valt, is het een onomstotbaar mensenrecht door de codificatie in de Universele Verklaring voor de Rechten van de Mens, het Europees Verdrag voor de Rechten van de Mens en het Verdrag inzake Burgerlijke en Politieke Rechten. Deze instrumenten delen elementen waaruit we een ‘klassieke’ definitie van privacy kunnen afleiden: een individu heeft het recht op respect voor zijn of haar privacy, familie, thuis of correspondentie, en zal niet onderworpen worden aan een willekeurige of onwettige inmenging in dit recht. Toen de automatische verwerking van data diens intrede deed in onze maatschappij en massale hoeveelheden gegevens eenvoudigweg beschikbaar werden, zagen de Organization for Economic Co-operation and Development, de Raad van Europe, het Human Rights Committee en de Europese Unie dat er nood was aan extra bescherming om privacy te garanderen. Die gecombineerde inspanningen hebben geleid tot een recht op digitale privacy, wat gedefinieerd kan worden als de bescherming van de fundamentele rechten en vrijheden van een individu wat betreft de verwerking van zijn of haar persoonlijke data - in het bijzonder met betrekking tot diens privé leven - zij het door publieke autoriteiten, of door private individuen of organisaties.

Er is echter discussie of de bescherming van persoonlijke data een onderdeel is van het recht op privacy, of dat het een opzichzelfstaand recht is. Verschillende instrumenten van de Europese Unie - zoals het Charter van de Fundamentele Rechten en de Algemene Verordening Gegevensbescherming (General Data Protection Regulation) - behandelen het als een opzichzelfstaand recht, hoewel de uitgebreide rechtspraak van het Hof van Justitie van de Europese Unie dat er nood was aan extra bescherming om privacy te garanderen. Die gecombineerde inspanningen hebben geleid tot een recht op digitale privacy, wat gedefinieerd kan worden als de bescherming van de fundamentele rechten en vrijheden van een individu wat betreft de verwerking van zijn of haar persoonlijke data - in het bijzonder met betrekking tot diens privé leven - zij het door publieke autoriteiten, of door private individuen of organisaties.

Het moet benadrukt worden dat deze thesis handelt over databescherming tegenover zakelijke actoren, en niet tegenover publieke instanties. Alle instrumenten inzake databescherming erkennen daarbij dat niet enkel Staten maar ook private partijen het recht op privacy betreffende de automatische verwerking van gegevens moeten respecteren. Bovendien hebben Staten de positieve verplichtingen om het recht op privacy tegenover diens burgers te beschermen en te vervullen. Dat houdt in dat een Staat wetgevende maatregelen moet nemen, alsook diezelfde regels moet afdwingen. Gezien de rijkdom aan wetgevende instrumenten en rechterlijke uitspraken inzake databescherming, is de keuze gemaakt om het beleid van de Europese Unie onder de loep te nemen, alsook de verregaande effecten daarvan.

De AVG introduceert enkele belangrijke veranderingen in het beleid van de Unie. Er zijn nu duidelijke regels inzake territoriale juridictie, boetes voor niet-naleving van de regels, een duidelijke nood aan toestemming van de individuen wiens gegevens worden verwerkt, er is een strikter regime inzake meldingsplicht voor datalekken, en er moet ook een functionaris voor gegevensbescherming worden aangesteld in bepaalde gevallen. De impact kan ook niet onderschat worden van de expliciete erkenning van de principes privacy by design en by default, van de strenge regels inzake profiling, van de voorwaarden om een data protection impact assessment uit te voeren en ten slotte van de codificatie van het ‘recht om vergeten te worden’ zoals erkend in de Google Spain zaak. Hoewel het lof verdient dat de AVG aandacht besteedt aan deze belangrijke onderwerpen en sommige bepalingen een enorm positieve impact kunnen hebben op de corporate governance verplichtingen van bedrijven, valt het nog maar zeer af te wachten hoe sommige ideeën in de praktijk ten uitvoer gelegd kunnen worden. Voorts is de status en de wenselijkheid van het ‘recht om vergeten te worden’ zodanig controversieel dat diens opname in de AVG een wel zeer gewaagde keuze is.

De afdwinging van het recht op databescherming door het Hof van Justitie moet ook in aanmerking genomen worden om te begrijpen hoe deze rechten in de praktijk functioneren. De invloed van de rechtspraak van het Europees Hof voor de Rechten van de Mens (EHRM) valt niet te onderschatten in deze context. Vier grote aspecten inzake afdwinging worden besproken. Eerst en vooral hebben beide hoven besloten dat het recht op databescherming geen absoluut recht is. Ten tweede heeft het Hof van Justitie twijfel inzake diens juridictie opgeheerd via enkele uitbreidingstechnieken. Ten derde heeft ditzelfde Hof in de Google Spain zaak besloten tot een ‘recht om vergeten te worden’ inzake zoekmachines onder bepaalde voorwaarden; het EHRM is echter veel minder expliciet in diens erkenning van datzelfde recht. Ten slotte wordt ook de toekomstige afdwinging onder de AVG kort besproken.

Niettegenstaande de uitgebreide wetgeving en afdwinging, zijn er toch bepaalde lacunes waar te nemen in de vorm van drie onderwerpen. Zo genieten rechtspersonen te weinig bescherming onder het huidige regime. Ook de AVG voorziet geen harmonisatie van dit onderwerp, noch moedigt het Staten aan om gelijkaardige regels aan te nemen. Dit kan leiden tot zeer uiteenlopende wetgeving. De Unie mag bovendien de snel evoluerende markt van de Mobile Location Analytics niet uit het oog verliezen, alsook hun verregaande manieren om data te verzamelen. Ten slotte is de AVG ook een gemiste kans voor de Unie om diens uiteenlopende regels inzake Radio Frequency Identification (RFID) technologie te bundelen.

Hoofdstuk vier analyseert de voordelen, nadelen en algemene gevolgen van het EU beleid inzake databescherming. De spanning tussen digitale privacy en de vrijheid van meningsuiting en informatie wordt verkend, zeker in de context van het recht om vergeten te worden. Het lijkt daarbij dat het Hof de enorme implicaties van diens Google Spain oordeel heeft onderschat, een visie die de vele hevige
tegenstanders van de beslissing volgen. Tegelijk moeten sommige van hun meningen worden genuanceerd. De voorstanders van het recht om vergeten te worden krijgen ook een stem. Bovenal benadrukt dit onderzoek echter dat de discussie geen gevecht tussen juist of fout is, maar wel een dialoog om een balans te vinden tussen de relevante rechten en belangen. De AVG probeert deze dialoog te stimuleren door in artikel 85 expliciet een balans weer te geven, maar de tijd zal uitwijzen of dit ook in de praktijk wordt uitgevoerd.

De meest alarmerende bevinding is dat de ‘wereldwijde’ aard van het internet in gevaar is. Aan de ene kant is er reeds een verbrokkeling van het wereldwijde web. Het internet verschilt in Europa van de rest van de wereld door hoe het recht om vergeten te worden wordt geïmplementeerd via geo-localisatie. Het gemis van een globaal databeschermingsregime komt hier duidelijk tot uiting, en dit is in grote mate te wijten aan de zwakke positie van de Verenigde Staten. Diens versplinterde aanpak van databescherming belet het om een sterk international standpunt in te nemen. Aan de andere kant is er ook een serieus gevaar van Europese digitale ‘kolonisatie.’ Indien het recht om vergeten te worden globaal wordt geïmplementeerd - zoals sommigen bepleiten - zou Europe zichzelf opwerpen als de informatiepolitie van de wereld. Door de afwezigheid van de Verenigde Staten in dit gebied is er geen tegengewicht voor het beleid van de Unie. Tegelijk migreren de ideeën van het Hof van Justitie naar andere jurisdicties. De Canadese zaak Equustek toont dat zelfs controversiële uitspraken zoals Google Spain gekopieerd kunnen worden als rechters zich onzeker voelen, simpelweg door te steunen op de autoriteit van het Hof.