MASTER THESIS

Titel der Master Thesis / Title of the Master‘s Thesis

„Comparative study on emerging rights- the Right to Be Forgotten and the Right to Data Portability in the European Union and the United States“

verfasst von / submitted by

Khalil Ismayilov

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Laws (LL.M.)

Wien, 2018 / Vienna 2018

Studienkennzahl lt. Studienblatt / Postgraduate programme code as it appears on the student record sheet:	A 992 548
Universitätslehrgang lt. Studienblatt / Postgraduate programme as it appears on the student record sheet:	Europäisches und Internationales Wirtschaftsrecht / European and International Business Law
Betreut von / Supervisor:	Dr. Lukas Feiler

Table of Contents

LIST OF ABBREVIATIONS

AEPD	Agencia Española de Protección de Datos
AG	Advocate General
API	Application Programming Interface
Charter	Charter of Fundamental Rights of European Union
CJEU	Court of Justice of the European Union
CNIL	Commission Nationale de l'informatique et des Libertés
COPPA	Children's Online Privacy Protection Act
DMCA	Digital Millennium Copyright Act
DPD	Data Protection Directive
DSM	Digital Single Market
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EU	European Union
FACT	Fair and Accurate Credit Transactions
FCRA	Fair Credit Reporting Act
FCRA	Fair Credit Reporting Act
FERPA	Family Educational Rights and Privacy Act
GDPR	General Data Protection Regulation
GLBA	Gramm–Leach–Bliley Act
HCI	Human-Computer Interaction
HIPAA	Health Insurance Portability and Accountability Act

HITECH	Health Information Technology for Economic and Clinical Health
PSD	Payment Services Directive
SB	Senate Bill
UK	United Kingdom
US	United States
VPPA	Video Privacy Protection Act
WP	Working Party

INTRODUCTION

In the information-age, the value of personal information is higher than ever before. There are popular social media networks are free of charge, convenient to set up, and are loaded with entertaining applications for users to enjoy. However, these free social media networks that are used by billions of people are not actually free. In exchange for the "free" services individuals give the service providers their own personal information. Such information is then transferred to companies who generate great wealth from the collected data.[1] However, it is not only social media services through which individuals' personal information is collected, stored, and processed by businesses or governments. In daily life, performing routine activities, such as online shopping, doctor visits, paying taxes, or filling out simple registration forms, individuals give out their personal information. Sometimes without even their knowledge or consent, this information is mined by organizations with whom they had never intended to interact.[2]

How do individuals know that their personal information is not being misused? How well is it protected? What kind of rights do individuals have in regards to their personal information? The answers lie with laws and regulations of data protection. "Data protection" is the term used mostly in European jurisdictions, whereas in the USA, Canada and Australia the term "privacy protection" is commonly used.[3] Just as the terms differ, so do the approaches and methods of protection of personal information in each jurisdiction.

In the European Union, data protection is a fundamental right. The European Court of Human Rights (ECtHR) has stated that under Article 8 of the ECHR,[4] the respected states, besides having obligation to refrain from actions that violate the rights laid down by the Convention, have positive obligations to secure effective respect for private and family life.[5]

---

[1] Stacy-Ann Elvy, *'Paying for Privacy and the Personal Data Economy'* 117 Columbia Law Review Association, Inc. (2017) <http://www.jstor.org/stable/44392955> accessed 7 February 2018.
[2] Data protection (Privacyinternational.org) <https://www.privacyinternational.org/node/44> accessed 22 October 2017.
[3] Lee. A. Bygrave, *Data Protection Law* (Kluwer Law International 2002) 1.
[4] European Convention on Human Rights, as amended (ECHR 1950) art 8.
[5] *Handbook on European Data Protection Law* (Publication Office of the European Union 2014) 15.

The Charter of Fundamental Rights of European Union (Charter), adopted in 2000 as a political document, later became legally binding as the EU primary law with adoption of the Lisbon Treaty in 2009. The Charter, besides providing the right to respect for one's private and family life, home and communications,[6] also specifically provides the right to data protection.[7]

Data protection was fully harmonized in the European Union after the adoption of Council Directive[8] on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the DPD) in 1995,[9] known as Directive 95/46/EC. In May of 2018, Directive 95/46/EC will be replaced by the General Data Protection Regulation (GDPR).[10]

The former EU Justice Commissioner Viviane Reding stated that when the Data Protection Directive of the EU was adopted, "only 1% of the EU population was using the Internet" and many of the big Internet giants like Facebook, Google and Amazon did not exist yet.[11] In a digital age, this Directive can be easily called "antiquated".[12] The European Commission stated that GDPR[13] is an important reform towards the strengthening of fundamental rights of citizens in the digital age and on the facilitation of business by simplifying rules for companies in the Digital Single Market.[14][15] The General Data Protection Regulation, *inter alia*, includes two new rights, namely the Right to be Forgotten[16] and the Right to Data Portability,[17] in addition to the rights from the

[6] Charter of Fundamental Rights of the European Union (2000) art 7.
[7] ibid, art 8.
[8] Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995) OJ L281/31 (Data Protection Directive).
[9] *Handbook on European Data Protection Law* (Publication Office of the European Union 2014) 18.
[10] 'Reform of EU Data Protection Rules - European Commission' (Ec.europa.eu, 2017) <http://ec.europa.eu/justice/data-protection/reform/> accessed on 28 October 2017.
[11] Viviane Reding, '*Outdoing Huxley: Forging a High Level of Data Protection for Europe in the Brave New Digital World*', Speech at Digital Enlightenment Forum, 18 June 2012 http://europa.eu/rapid/press-release_SPEECH-12-464_en.htm accessed 2 December 2017.
[12] Mira Burri and Rahel Schär, *'The Reform of the EU Data Protection Framework: Outlining Key Changes And Assessing Their Fitness For A Data-Driven Economy'* 6 Journal of Information Policy (2016) 480 <http://www.jstor.org/stable/10.5325/jinfopoli.6.2016.0479> accessed 7 February 2018.
[13] Council Regulation (EU) 2016/679 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 [2016] OJ L119/1 (General Data Protection Regulation).
[14] For the definition of Digital Single Market (DSM) see European Commission, *Shaping the Digital Single Market*, (European Union 1995-2017)< https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market> accessed on 3 December 2017.
[15] *'Reform of EU Data Protection Rules - European Commission'* (Ec.europa.eu, 2017) <http://ec.europa.eu/justice/data-protection/reform/> accessed on 28 October 2017.
[16] General Data Protection Regulation, art 17.
[17] ibid, art 20.

Data Protection Directive. Although the GDPR acknowledges the other rights, from its text it is clear that "the protection of personal privacy outranks freedom of expression or knowledge".[18] Because of this, it has caused a lot of debates in the field of data protection.

With regards to privacy, the Unites States' policy differs significantly from that of the EU. This is mainly because the United States pursues market-dominated policy which provides limited statutory and common law for the protection of personal information, whereas, the EU has right-dominated approach which demands for its citizens a broad statutory protections.[19]

Although the majority of today's internet giants, like Google, Facebook, Apple, etc. are US based companies, their activities however, are global. Often times, these companies try to export the privacy practices of the United States to other countries. This results in a clash of two different legal systems, and these companies face a lot of challenges outside the US borders. The right to be forgotten and the right to data portability also exist in the United States, however, their scope is not as broad as the rights provided by the GDPR, and are limited to certain types of personal data.

The right to data portability and the right to be forgotten, provided by the GDPR, are probably one of the toughest and most complex privacy rights that the US and as well as EU based companies had ever faced. The right to be forgotten exists only in the State of California, while the right to data portability exists in some sector-specific federal laws. This paper seeks to analyze and assess the right to data portability in the European Union and in the United States, and as well as the right to be forgotten in the EU and the State of California.

[18] George Brock, *The Right To Be Forgotten: Privacy And The Media In The Digital Age* (I. B. Tauris & Co. Ltd 2016) 74.
[19] Joel R. Reidenberg, *'Resolving Conflicting International Data Privacy Rules In Cyberspace'* 52 Stanford Law Review (2000), 1318.

CHAPTER I

1.1 THE RIGHT TO DATA PORTABILITY IN THE EUROPEAN UNION

In the Digital Age, Internet user(s) (under the European law it is called "data subject")[20] spend(s) a lot of time building online data- for instance, e-mail users send and receive emails, and develop address book(s); social media users upload pictures, post their thoughts, make comments on other posts and etc. The new right, "right to data portability", [21]provided by GDPR, enables the users to receive their data as well as to transfer these data from one controller to another. For example, an individual using Yahoo mail has the right to ask Yahoo to transfer all of his or her data to Gmail.

Even though the right to data portability is new in European Union law, the idea of data portability itself is hardly new.[22] Google has long allowed its users to obtain data the company has collected about them.[23] In 2010, in the United States, the Obama Administration launched a series of "My Data Initiatives"[24] that increased the data portability in the fields of healthcare (Blue Button), finance (My Transcript), energy (Green Button) and education (My Student Data). The purpose of data portability was to allow the data subjects to keep their data online, have access to it, and use it how they want.[25]

A year after My Data Initiatives launched in the United States, the Coalition Government of the UK has proposed "midata [voluntary] programme" which was intended to make it easier for the consumers "to compare the different offers available" by providing them access to the information which "companies hold about their transactions in a machine-readable and reusable format".[26] After receiving the transaction history via simple download, the customer may then submit it to

[20] Note: Throughout the paper the terms –'users', 'data subject' and 'consumer' will be used interchangeably
[21] General Data Protection Regulation, art.20.
[22] Alan Mitchell, *'GDPR: Evolutionary or Revolutionary?'* 17 Journal of Direct, Data and Digital Marketing Practice (2016) 217.
[23] ibid, 217.
[24] Alexander Macgillivray and Jay Shambaugh, *'Exploring Data Portability'* (*whitehouse.gov*, 2016) <https://obamawhitehouse.archives.gov/blog/2016/09/30/exploring-data-portability> accessed 17 December 2017
[25] ibid.
[26] *'Review of the Midata Voluntary Programme'* (*Gov.uk*, 2014) 3 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/327845/bis-14-941-review-of-the-midata-voluntary-programme-revision-1.pdf> accessed 2 December 2017.

"comparison providers", and the latter will analyze the data and the result would help the customer determine which service provider to choose in the future.[27]

After the 'midata program' was issued, the data portability concept was extended to European Payment Services Directive 2 (PSD 2)[28] which obliges banks through Open Application Programming Interfaces (APIs)[29] to make customers' balance and transactions data available for them.[30] Data protection regulation aims to eliminate obstacles to the free flow of personal data in EU level which enables operators to be able to engage in cross-border data transfer.[31] This, in return, fosters the competition between controllers, and the right to data portability is an important tool to realize this objective.[32]

Perhaps without empowering the users to obtain personal data from the controllers, it would not be easy to keep the free flow of the data across the market. Therefore, the right to data portability is an important element in realization of economic regulation to fix the market imperfections for which market forces cannot find solutions. A user, after obtaining one's own personal data from one controller, can give the personal data directly to another controller or can request the controller send his/her personal data directly to another controller, something the companies would not otherwise want to share with their competitors. This, at least in theory, will keep the free flow of personal data within the Digital Single Market and boost the competition between controllers. Additionally, the right to data portability gives data subjects a sense of satisfaction that they are in control of their own personal data, and can now keep their data anywhere they wish or move it to a new service they like better.

[27] Midata for personal Current Accounts, <http://www.pcamidata.co.uk/> accessed on 3 December 2017.
[28] Council Directive (EU) 2015/2366 of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC OJ L 337/35 (PSD2)
[29] Application Programming Interface (API) means the interfaces of applications or web services made available by data controllers so that other systems or applications can link and work with their systems- Article 29 Data Protection Working Party, *Guidelines on the right to data portability*, (As last Revised and adopted on 5 April 2017), 15.
[30] Alan Mitchell, *'GDPR: Evolutionary or Revolutionary?'* 17 Journal of Direct, Data and Digital Marketing Practice (2016), 218.
[31] Orla Lynskey, *The Foundations Of EU Data Protection Law* (Oxford University Press 2015), 76.
[32] Article 29 Data Protection Working Party, *Guidelines on the right to data portability*, (As last Revised and adopted on 5 April 2017), 3.

1.1.1 Legal perspective of data portability

Article 20 of GDPR provides that –

> "*the data subject shall have the right to **receive** the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to **transmit** those data to another controller without hindrance from the controller to which the personal data have been provided …*"[33]

Article 20 of GDPR conceptually gives the data subject two rights- a "right to receive" and a "right to transmit" the personal data. A "right to receive" gives the data subject a right to obtain his or her own data, "which he or she has provided to a controller in a structured, commonly used, machine-readable and interoperable format."[34] This characteristic is similar to "the right of access"[35] (the right of access was previously provided by Data Protection Directive[36]). However, the right to data portability further strengthens the right of access. With the right of access the controller is required to give the data in a "commonly used format"[37], whereas the right to data portability requires the controller to give the data "in a structured, commonly used, machine-readable and interoperable format".[38]

The "right to transmit" gives the data subject a right to transfer this data to another controller without hindrance.[39] Besides having the right to receive and transmit the data, the GDPR gives the data subject the right to ask the controller to directly transfer his or her data to another controller.[40]

The right to data portability applies only to the personal data processed by automated means,[41] meaning that it does not apply to processing by paper records. Although the wording of the law is

[33] General Data Protection Regulation, art 20 (1).
[34] ibid, art 20 (1), recital 68.
[35] ibid, art 15.
[36] Data Protection Directive, art 12.
[37] General Data Protection Regulation, art 15 (3).
[38] ibid, recital 68.
[39] ibid, art 20 (1), recital 68.
[40] ibid, art 20 (2).
[41] ibid, art 20 (1) (b).

very clear on the matter, Article 29 Working Party[42] (hereinafter the Working Party) in its guidelines, without giving further explanations, stated that the application of the right to data portability is only possible when the data is processed by automated means, and " … therefore, does not cover most paper files."[43] By doing this, the Working Party did not completely rule out the possibility of the application of the right to data portability on the data processing carried out on paper files. Perhaps we will have to wait until the first such case is interpreted in the court of law.

1.1.2 Application of data portability

Article 6 of the GDPR provides lawful bases for the processing of personal data, which are:

a) Consent of the data subject;
b) Required for performance of a contract,
c) Legal obligation of the controller,
d) Protection of vital interests of the data subject,
e) The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller,
f) Legitimate interest of the controller or third party.

The right to data portability applies only in two legal bases: first, consent - where the data subject gave the personal data on the basis of his/her consent; or second, on the basis of performance of a contract.[44] In this regard, consent means "*freely given, specific, informed and unambiguous*" wishes of the data subject.[45] Since the law requires consent to be freely given, it may not apply in

[42] The "Article 29 Working Party" is the short name of the Data Protection Working Party established by Article 29 of Directive 95/46/EC. It provides the European Commission with independent advice on data protection matters and helps in the development of harmonized policies for data protection in the EU Member States.- 'A - European Data Protection Supervisor' (*European Data Protection Supervisor*, 2018) <https://edps.europa.eu/data-protection/data-protection/glossary/a_en> accessed 11 January 2018.
[43] Article 29 Data Protection Working Party, *Guidelines on the right to data portability*, (As last Revised and adopted on 5 April 2017), 9.
[44] General Data Protection Regulation, recital 68.
[45] ibid, art 4 (11).

certain situations where there is a power imbalance between the controller and the data subject, such as consent of an employee.[46]

Furthermore, it was argued that when there is a monopoly, "whether as a result of innovation, network effects, or even acquisitions"[47], consent cannot be freely given since in such case(s) the "reality detracts from even the most fully informed and premediated consent" and the data subject does not "have a choice".[48] Moreover, as mentioned above, when individuals get "free" services, such as Facebook or Gmail, they actually pay for these online services by allowing the service providers to use their data. Nevertheless, in such cases consent would be freely given if the service providers offered an alternative type of service to the users in which the data of the users would not be used for marketing.[49] In the absence of such service, consent cannot be considered as freely given since the user has no choice. However, by allowing users to obtain the data from the controller, the right to data portability "may restore this choice".[50]

The GDPR sets the conditions for consent by declaring that it must be "clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language".[51] For the processing of special categories (sensitive data) of personal data, such as racial and ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or natural person's sex life or sexual orientation, the data subject's explicit consent must be obtained.[52] However, neither the law nor the Working Party has a clear explanation of 'explicit consent' or how it differs from general consent.

Consent requirement is criticized by legal scholar Omer Tene, who argues that consent is not a correct means to make data flow legitimate since the processing of personal data brings many

[46] Article 29 Data Protection Working Party, *Guidelines on the right to data portability*, (As last Revised and adopted on 5 April 2017), 8-9.
[47] Orla Lynskey, *The Foundations Of EU Data Protection Law* (Oxford University Press 2015), 263.
[48] Omer Tene, *'Privacy law's midlife crisis: A critical assessment of the second wave of global privacy laws'* Ohio state law journal [2013], 1233.
[49] Article 29 Data Protection Working Party, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC,* (adopted on 9 April 2014), 47.
[50] Orla Lynskey, *The Foundations Of EU Data Protection Law* (Oxford University Press 2015), 263.
[51] General Data Protection Regulation, art 7 (2).
[52] ibid, art 9 (2).

innovations which would not be possible if there was a consent requirement from every individual.[53] He argues that it is "the biggest public policy challenge of our time" to find a perfect balance between the great benefits of processing data and privacy rights of individuals.[54]

The applicability of the right to data portability in only two legal bases may set limitations on the possibility of obtaining data for data subjects. Companies could avoid obligation to provide individuals their data by processing data on a different legal base- legitimate interest. In such case, a data subject cannot exercise his or her right to data portability. Nevertheless, in order to use the legitimate interest ground to process data, the GDPR requires companies do more than merely "claim legitimate interest", but they also demonstrate their justification of such claim.[55] So far, the legitimate interest ground does not give companies "legal certainty" since a test to determine legitimate interest has not yet been developed enough to put into practice which leaves the companies process data mainly on a ground of consent.[56]

The GDPR provides that the right to data portability does not apply where "processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller",[57] or when processing will "adversely affect the rights and freedoms of others".[58] However, an individual still has the right to object the processing of his or her personal data.[59] In such case, in order to process the data, the controller has to prove that its "compelling legitimate interest overrides" the interests of the individual.[60]

If controllers can prove it, then they have no obligations of making portability available for the data subject. Nevertheless, the Working Party suggests that it would be "a good practice to develop processes to automatically answer portability requests, by following the principles governing the

[53] Omer Tene, '*Privacy law's midlife crisis: A critical assessment of the second wave of global privacy laws'* Ohio state law journal [2013], 1247.
[54] ibid.
[55] *'Data Protection in Europe- Academics Are Taking a Position'* 29 Elsevier: Computer Law & Security Review (2013) 181 <https://www.sciencedirect.com/science/article/pii/S026736491300037X> accessed 2 February 2018.
[56] Omer Tene, '*Privacy law's midlife crisis: A critical assessment of the second wave of global privacy laws'* Ohio state law journal [2013], 1248.
[57] General Data Protection Regulation, art 20 (3).
[58] ibid, art 20 (4).
[59] ibid, art 21, recital 69.
[60] ibid.

right to data portability", such as making personal income tax records available for the data subjects by a government service.[61] On the other hand, defining public interest and what is tantamount to an adverse effect will require "complex legal balancing exercises".[62]

There are conditions set by the GDPR for the right to portability to be applicable. First, the right to data portability applies only to the personal data "concerning" the data subject and "provided to" the controller by the user him or herself.[63] As provided by the law, data portability applies to personal data and thus excludes anonymized data which does not concern the user, but includes pseudonymous data[64] that can be linked to the user.[65] There may be an issue with "data concerning the data subject" when information of third parties, who may not have given consent, is also involved in the data. However, the Working party, in its guideline, stated that in such cases, for example, telephone, interpersonal messaging, or VoIP records, the controller should take not so restrictive interpretation of "data concerning the data subject", because such records are concerning the data subject and therefore, should be given to the data subject upon the data portability request.[66]

Conversely, when the data, which includes information of third parties, is transferred to another data controller, third party data should not be processed by the new controller for any purposes since it would adversely affect the rights and freedom of third parties.[67] Notably, the new controller would not have a legal base of consent, to process the third party data.[68] Nevertheless, the Working party maintains that in cases where personal or third party data are involved, another legal base,

[61] Article 29 Data Protection Working Party, *Guidelines on the right to data portability*, (As last Revised and adopted on 5 April 2017), 8.
[62] Lachlan Urquhart, Neelima Sailaja and Derek McAuley, *'Realising the Right to Data Portability for the Internet of Things'* SSRN Electronic Journal [2017] 3<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2933448> accessed 15 December 2017.
[63] General Data Protection Regulation, art 20 (1).
[64] Data are pseudonymised if the identifiers are encrypted- *Handbook on European Data Protection Law* (Publication Office of the European Union 2014) 36.
[65] Article 29 Data Protection Working Party, *Guidelines on the right to data portability*, (As last Revised and adopted on 5 April 2017), 9.
[66] ibid.
[67] ibid.
[68] Lachlan Urquhart, Neelima Sailaja and Derek McAuley, *'Realising the Right to Data Portability for the Internet of Things'* SSRN Electronic Journal [2017] 2 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2933448> accessed 15 December 2017.

such as a legitimate interest,[69] can be demanded by the new controller.[70] However, this applies when, by providing service, the controller intends to enable the data subject to process his or her own data, including third party data, "for purely personal or household activity".[71] In such cases, when an individual processes the data, he or she is solely responsible for the possible damage to the third party, as long as "such processing is not…decided by the controller".[72]

The Working party recommends that in order to lessen the risks of third parties' data being given away, controllers on both sides develop a special tool which would help the data subject take their own data they desire and exclude the data of others.[73] However, privacy experts argue that creating such practical intuitive tools "for Internet of Things will pose HCI [Human-Computer Interaction] issues."[74]

Second, in order for the right to portability to be applicable, the data must be "provided by" the data subject.[75] The Working party argues that besides the data given directly by the data subject through online forms such as mailing address, user name, age, etc., data that results from the observation of the data subject, "such as raw data processed by a smart meter or history of website usage or search activities", should be considered as data "provided by the data subject" but not the data that are created by the data controller through the usage of "data observed or directly provided as input, such as a profile created by analysis of the raw smart metering data collected".[76]

The interpretation of the Working party on "observation of the data subject" is somewhat controversial because Article 20 of GDPR does not mention anything about observed data. Additionally, Recital 68 of GDPR states that "that right [the right to data portability] should apply where the data subject provided the personal data on the basis of his or her consent or the

[69] General Data Protection Regulation, art 6 (1) (f).
[70] Article 29 Data Protection Working Party, *Guidelines on the right to data portability*, (As last Revised and adopted on 5 April 2017), 11.
[71] ibid.
[72] ibid.
[73] ibid, 12.
[74] Lachlan Urquhart, Neelima Sailaja and Derek McAuley, *'Realising the Right to Data Portability for the Internet of Things'* SSRN Electronic Journal [2017] 3 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2933448> accessed 15 December 2017.
[75] General Data Protection Regulation, art 20 (1).
[76] Article 29 Data Protection Working Party, *Guidelines on the right to data portability*, (As last Revised and adopted on 5 April 2017), 9-10

processing is necessary for the performance of a contract."[77] Broad interpretations of the Working party were also criticized by the Commission spokesperson who said "we value the work of [WP29] on [the guidelines], but also have certain concerns that the guidelines might go beyond what was agreed by the co-legislators in the legislative process…"[78]

Moreover, the Working party suggests that in order to meet the purpose of the right to data portability, the term "data provided by the data subject" should be loosely interpreted and data that has been "inferred" or "derived" via analysis accomplished by the controller, such as algorithmic results, should be excluded.[79] This rule could set a limitation on what kind of data users can demand from the controller, and since the data subjects can move the raw data but not the inferences, the right to data portability is not as wide as it seems.[80] "For example, tracking of home occupant movements detected by a Nest learning thermostat", which is a system that learns about the home owner's movement and optimizes temperature in the house while saving energy[81], "interactions could be okay, but not the algorithmically derived heating schedule".[82] Without having an algorithmically derived heating schedule, a home owner would not benefit much from the raw data.

It could be argued that such limitation of obtaining data from the controller may not be in line with the purpose of the right to data portability which was intended from the creation of the concept, *inter alia*, to help the data subject have a chance to compare the services and make a better choice for themselves. By providing only raw data for the users this goal cannot be fully achieved.

[77] General Data Protection Regulation, Recital 68.
[78] *'European Commission, Experts Uneasy over WP29 Data Portability Interpretation | 7Wdata'* (*7wData*, 2018) <http://www.7wdata.be/privacy-issues/european-commission-experts-uneasy-over-wp29-data-portability-interpretation/> accessed 15 January 2018.
[79] Article 29 Data Protection Working Party, *Guidelines on the right to data portability*, (As last Revised and adopted on 5 April 2017), 10.
[80] Lachlan Urquhart, Neelima Sailaja and Derek McAuley, *'Realising the Right to Data Portability for the Internet of Things'* SSRN Electronic Journal [2017] 3, 10 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2933448> accessed 15 December 2017.
[81] *'Nest Learning Thermostat - Install & Explore'* (*Nest*, 2018) <https://nest.com/thermostats/nest-learning-thermostat/tech-specs/> accessed 5 March 2018.
[82]Lachlan Urquhart, Neelima Sailaja and Derek McAuley, *'Realising the Right to Data Portability for the Internet of Things'* SSRN Electronic Journal [2017] 3, 10 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2933448> accessed 15 December 2017.

On the other hand, it would create a problem for controllers when algorithmically-driven data by one controller is sent to another controller. Since such data requires special algorithms and can be considered trade secrets or intellectual property, transferring it to another controller would hurt the business of the controller who created that particular program. Therefore, finding the right balance between the interests of controllers and the data subjects is complex and perhaps not achievable by the right to data portability alone.

Realizing the GDPR's right to data portability in practice will require a lot of team work of legal and IT professionals.[83] Nevertheless, at least theoretically, the right to data portability, provided by the GDPR, besides enhancing competition among service providers, also has great benefits for data subjects. First, it ensures transparency by allowing the users to obtain and keep their data collected by companies. Second, it allows the users to be able to analyze their data and choose better services. Third, it allows the users to change their service providers and take all of the data to the new provider without hindrance.

The GDPR bans data controllers from charging the data subject a fee for providing data portability[84] unless controllers deem the request for data portability by the data subject to be "manifestly unfounded and excessive." The GDPR provides that controllers may reject providing the data to individuals in some cases. Specifically, if the controllers show that it is not possible for them to identify the individual,[85] or second, if the data subject's request for data portability is "manifestly unfounded and excessive."[86]

[83] Lachlan Urquhart, Neelima Sailaja and Derek McAuley, *'Realising the Right to Data Portability for the Internet of Things'* SSRN Electronic Journal [2017] 17 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2933448> accessed 15 December 2017
[84] General Data Protection Regulation, art 12 (5).
[85] ibid, art 12 (2).
[86] ibid, art 12 (5) (b).

1.2 THE RIGHT TO DATA PORTABILITY IN THE UNITED STATES

In the United States, laws on privacy center on providing remedies for "consumer harm" and harmonizing privacy with "efficient commercial transactions."[87] The US Constitution, while providing wide protection for free speech, does not include the word privacy.[88] In fact, general privacy was not recognized as a protected right by the courts in the United States until the 20th century.[89] The recognition of privacy as a protected right in the United States was influenced by the famous article, "The Right to Privacy,"[90] written by lawyers Warren and Brandeis, and published by Harvard Law Review Journal in 1890.[91] They described privacy as the right "to be let alone." [92]

What amounts to personal data in the United States is fundamentally different from the concept held in the EU. In the EU, though definition is general and ambiguous,[93] personal data means "any information relating to an identified or identifiable natural person".[94] However, in the United States, information that is publicly recorded is excluded from "protection as personal information"[95] and the approach comprises "multiple and inconsistent" definitions of personally identifiable information which are mostly narrow.[96]

---

[87] Paul M. Schwartz and Daniel J. Solove, *'Reconciling Personal Information In The United States And European Union'* 102 California Law Review (2014), 877.
[88] Omer Tene, *"Privacy law's midlife crisis: A critical assessment of the second wave of global privacy laws"* Ohio state law journal (2013), 1125.
[89] H. Jeff Smith, Tamara Dinev and Heng Xu, *'Information Privacy Research: An Interdisciplinary Review'* (2011) Vol. 35 No. 4 Management Information Systems Research Center, University of Minnesota, 994.
[90] Samuel D. Warren and Louis D. Brandeis, *'The Right to Privacy'* 4 Harvard Law Review (1890) <http://links.jstor.org/sici?sici=0017-811X%2818901215%294%3A5%3C193%3ATRTP%3E2.0.CO%3B2-C> accessed 10 January 2018.
[91] William L. Prosser, *'Privacy' 48 California Law Review* (1960), 384.
[92] Samuel D. Warren and Louis D. Brandeis, *'The Right to Privacy'* 4 Harvard Law Review (1890) 205 <http://links.jstor.org/sici?sici=0017-811X%2818901215%294%3A5%3C193%3ATRTP%3E2.0.CO%3B2-C> accessed 10 January 2018.
[93] Paul M. Schwartz and Daniel J. Solove, *'Reconciling Personal Information In The United States And European Union*' (2014) Vol. 102 California Law Review, 877.
[94] General Data Protection Regulation, art 4 (1).
[95] Joel R. Reidenberg, *'Resolving Conflicting International Data Privacy Rules In Cyberspace'* (2000) 52 Stanford Law Review, 1344.
[96] Paul M. Schwartz and Daniel J. Solove, *'Reconciling Personal Information In The United States And European Union'* (2014) Vol. 102 California Law Review, 877.

There is no comprehensive information privacy law in the United States. When it comes to information privacy,[97] the country relies on sector-specific legislation that have been adopted only in response to specific problems and to offer narrow protection to privacy.[98] Examples include the Fair Credit Reporting Act (FCRA) of 1970 that regulates the work of credit reporting agencies[99]; the Family Educational Rights and Privacy Act (FERPA) of 1974 that regulates privacy of student education records[100]; the Video Privacy Protection Act (VPPA) of 1988 that regulates the work of video tape service providers[101]; the Health Insurance Portability and Accountability Act (HIPAA) of 1996 that regulates the work of health care providers[102]; the Children's Online Privacy Protection Act (COPPA) of 1998 that regulates the online collection and processing of personal information of children under age 13[103]; and the Gramm–Leach–Bliley Act (GLBA) of 1999 that applies to financial institutions.[104]

1.2.1 Data portability in sector specific laws

There is neither state nor federal law on data portability, in the United States that is comparably as comprehensive and broad as the one in the European Union. However, as mentioned earlier, laws that relate to privacy in the United States are sector specific, and some of them provide for the right to data portability for certain types of data, such as data that relates to the health records of an individual. Besides, as mentioned earlier, there were a series of initiatives started by the Obama Administration that were intended to increase data portability in certain areas.

[97] Omer Tene, *'Privacy law's midlife crisis: A critical assessment of the second wave of global privacy laws'* (2013) Ohio state law journal, 1125.
[98] Joel R. Reidenberg, *'Resolving Conflicting International Data Privacy Rules In Cyberspace'* (2000) 52 Stanford Law Review, 1343.
[99] Fair Credit Reporting Act (FCRA) of 1970, 15 U.S.C. § 1681b (2012)
[100] Family Educational Rights and Privacy Act (FERPA) of 1974, 20 U.S.C. § 1232g (2012)
[101] Video Privacy Protection Act (VPPA), 18 U.S.C. § 2710 (2012).
[102] Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191, 110 Stat. 1936.
[103] Children's Online Privacy Protection Act (COPPA) of 1998, 15 U.S.C. §§ 6501–6506 (2012).
[104] Gramm–Leach–Bliley Act (GLBA) of 1999, 15 U.S.C. § 6809(4) (A) (2012).

1.2.2 Telecommunications Act

Although, the right to data portability is a new law in the European Union, elements of data portability is not entirely new in the United States. In the US, the Telecommunications Act of 1996 allowed consumers to carry their phone numbers (also known as "number portability") from one carrier to another.[105] The purpose of the law was to increase competition among telecommunication carriers and lower the prices by allowing consumers to change carriers.[106] From a legal perspective, number portability was not a privacy concern, the law gave ownership of a phone number to the consumer, not to carriers, which created a legal base to allow the owners of phone numbers to switch from one carrier to another and keep the same number.[107] Nevertheless, it has the same effect as data portability.

Inspired by "number portability" provided by the Telecommunications Act, the scholars Guy Rolnick and Luigi Zingales have proposed a new data portability requirement that they call "portability of social graph".[108] They argue that if the law gives individuals ownership of platforms created in social media, they would be able to take their platforms from one social network, such as Facebook, to another one.[109] In return, they assume, this would create an environment in which new social networks could arise and would boost competition in this sector.[110] However, privacy experts ridiculed this idea saying it is difficult to implement, while at least one of them labeled it as "oppressive regulation".[111]

---

[105] Telecommunications Act, 47 U.S.C. § 251 (b) (2)

[106] Luigi Zingales and Guy Rolnik, *'A Way to Own Your Social-Media Data'* (*Nytimes.com*, 2017) <https://www.nytimes.com/2017/06/30/opinion/social-data-google-facebook-europe.html> accessed 3 March 2018.

[107] ibid.

[108] Robert Seamans, *'Data Portability and Competition between Technology Platforms'* (*Forbes.com*, 2018) <https://www.forbes.com/sites/washingtonbytes/2018/03/06/data-portability-and-competition-between-technology-platforms/2/#7422db82658d> accessed 8 March 2018.

[109] Luigi Zingales and Guy Rolnik, *'A Way to Own Your Social-Media Data'* (*Nytimes.com*, 2017) <https://www.nytimes.com/2017/06/30/opinion/social-data-google-facebook-europe.html> accessed 3 March 2018.

[110] ibid.

[111] James Pethokoukis, *'Washington vs. Big Tech: Should You 'Own' All Your Social Network Data? An AEIdeas Online Symposium'* (*AEIdeas*, 2017) <http://www.aei.org/publication/washington-vs-big-tech-should-you-own-all-your-social-network-data-an-aeideas-online-symposium/> accessed 10 March 2018.

1.2.3 Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act (HIPAA), enacted by Congress in 1996, provides the protection of health information of individuals and helps them maintain health insurance.[112] Health information is defined as "any information, including genetic information…which relates to the past, present, or future physical or mental health or condition of an individual."[113] The US Department of Health and Human Services asserted that protected health information is not limited to diagnosis of a patient or payment information, but also means "names, addresses and demographic information" when such information is given in a context that individual was "a patient of a health care provider".[114]

In 2009, the U. S. Congress enacted a law, the Health Information Technology for Economic and Clinical Health Act, also known for its abbreviation HITECH Act, which was part of the American Recovery and Reinvestment Act.[115] By amending HIPAA, the HITECH Act, provided patients the right to receive copy of his or her personal health information in an electronic format.[116] The HITECH Act applies to both a "covered entity" as well as a "business associate". [117]

Covered entity is defined by the law as "a health plan,[118] a health care clearinghouse,[119] and a health care provider[120] who transmits any health information in electronic form in connection with a transaction".[121] A business associate is broadly defined as a person, who is not a member of the workforce of a covered entity or arrangement, but "on behalf of [such] covered entity or of an organized health care arrangement … in which the covered entity participates… creates, receives, maintains, or transmits protected health information for a function or activity regulated by this subchapter" or as an entity which "provides …legal, actuarial, accounting, consulting, data

[112] HIPAA, 42 U.S.C. § § 17921 to 17953.
[113] 45 CFR § 160.103.
[114] Sean Baird, *'GDPR Matchup: The Health Insurance Portability and Accountability Act'* (*Iapp.org*, 2017) <https://iapp.org/news/a/gdpr-match-up-the-health-insurance-portability-and-accountability-act/> accessed 3 March 2018.
[115] HITECH Act, 42 U.S.C. § 17935.
[116] HITECH Act, 42 U.S.C. § 17935(e) (1).
[117] HITECH Act, 42 U.S.C. § 17935 (e) (1) (2).
[118] For the definition of health plan see 42 U.S.C. 300gg-91(a) (2).
[119] For the definition of a health care clearinghouse see 45 CFR § 160.103.
[120] For the definition of a health care provider see 42 U.S.C. § 1395x(r) (u).
[121] 45 CFR § 160.103.

aggregation,... management, administrative, accreditation, or financial service to or for the covered entity".[122] The HIPAA permits the sharing of patient health information between covered entities and their business associates.[123]

The HITECH Act also allows a patient to ask the "covered entity" to send a copy of electronic health records to a third party that he or she has chosen as long as such designation is "clear, conspicuous, and specific".[124] However, while the law obliges the covered entity to provide individuals with electronic health records, a business associate has an option to provide all the information either to the patient or to the designated covered entity.[125]

The HITECH Act gives the right to the covered entity to charge a fee for providing a copy of health records, but said fee, when given in an electronic from, cannot be more than the labor cost of providing such information.[126] However, the law is silent on whether or not a business associate could impose a fee on providing such information.

The law provides that non-compliance with HIPPA may result in fines varying from 100 to 50,000 US dollars until 2009.[127] However, after the adoption of the HITECH Act, penalties for violations were increased up to 1.5 million US dollars depending on the circumstances.[128]

1.2.4 Data portability initiatives

In 2010, the Obama Administration launched the Blue Button initiative which was intended to enable consumers to have access to their health information in a useable format. [129] The usable

[122] 45 CFR § 160.103 (i) (ii).
[123] N. Nina Zivanovic, *'Medical Information as A Hot Commodity: The Need for Stronger Protection of Patient Health Information'* 19 Intellectual Property Law Bulletin (2015) 188.
[124] HITECH Act, 42 U.S.C. § 17935(e) (1).
[125] HITECH Act, 42 U.S.C. § 17935(e) (2).
[126] HITECH Act, 42 U.S.C. § 17935(e) (3).
[127] 45 CFR 160.401; 45 CFR 160.404.
[128] ibid.
[129] Blue Data, 'Blue Button Home' (*Va.gov*, 2017) <https://www.va.gov/bluebutton/> accessed 3 March 2018.

format is possible by simply downloading a file that contains the patient's health record.[130] Government agencies[131] such as the Centers for Medicare and Medicaid Services (CMS), the Department of Defense and the Veterans Health Administration, as well as some private businesses have joined the Blue Button initiative.[132] Reports indicated that prior to 2008, only 9 percent hospitals and 17 percent of physicians kept health records electronically. [133] However, by 2017, because of the Blue Button initiative, 96 percent of hospitals and 78 percent of physicians had systems in place for keeping electronic health records (EHR).[134]

Besides Blue Button, there were other initiatives, such as My Transcript for the financial sector, Green Button for the energy sector, and My Student Data for student data. All of these initiatives have one purpose: to allow the data subjects to have access to their personal information and be able to use it. As of 2018, these initiatives are not laws, they only try to incentivize certain sectors to make data portability available to the consumers.

1.2.5 Right to receive

The right to data portability has two main components: one is a right to receive the data, and the other is the right to transmit the data to others. Some federal and state laws in the US, such as the Fair Credit Reporting Act (FCRA),[135] provides individuals the right to receive their personal data.

The Fair Credit Reporting Act was enacted in 1970 by the United States Congress to safeguard individuals in their relations with credit reporting agencies (CRAs).[136] In this context, consumer means someone who is "obligated" or supposedly "obligated" to a payment of "debt".[137] Consumer

[130] ibid.
[131] Leslie P. Francis, *'When Patients Interact With EHRs: Problems of Privacy and Confidentiality'* 12 Houston Journal of Health Law & Policy (2012) 178.
[132] Blue Data, 'Blue Button Home' (*Va.gov*, 2017) <https://www.va.gov/bluebutton/> accessed 3 March 2018.
[133] Alexander Macgillivray, *'Summary of Comments Received Regarding Data Portability'* (*whitehouse.gov*, 2017) <https://obamawhitehouse.archives.gov/blog/2017/01/10/summary-comments-received-regarding-data-portability> accessed 3 March 2018.
[134] ibid.
[135] FCRA, 15 U.S.C. § 1681.
[136] Austin H. Krist, *'Large-Scale Enforcement of the Fair Credit Reporting Act and the Role of State Attorneys General'* 115 Columbia Law Review (2015) 2311 <http://www.jstor.org/stable/43655764> accessed 20 March 2018.
[137] 15 USC § 1692a (3).

reporting agency is defined by the law as someone "which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties…".[138] Consumer report is "any … communication of any information by a consumer reporting agency" that contains "a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics…".[139] As seen from the definition, the credit report has significant importance for individuals who wish to obtain any kind of credit. Any inaccuracy in the credit report can either greatly cost the consumer or harm the financial sector.

In order to ensure an adequate level of accuracy in consumer credit reports that are provided by consumer reporting agencies,[140] in 2003 the US Congress amended the FCRA by enacting the Fair and Accurate Credit Transactions Act (FACT).[141] The FACT Act, *inter alia*, permits the consumer to ask credit reporting agencies for all the files that contain the consumer's credit information, though not credit scores or other risk predictors.[142] The law requires the consumer credit report to be provided in writing, unless the consumer requests it in other forms that are available in the credit reporting agency.[143]

SUMMARY OF THE RIGHT TO DATA PORTABILITY IN THE EUROPEAN UNION AND THE UNITED STATES

Based on the research, it can be concluded that while the right to data portability in the EU is shaped by a comprehensive data protection law, the GDPR, in the US there is no comprehensive data privacy law that guarantees the general right to data portability. Instead, there are sectoral

[138] § 603 (f) - FCRA, 15 U.S.C. § 1681.
[139] FCRA, 15 U.S.C. § 1681a.
[140] FCRA, 15 U.S.C. § 1681 (Congressional findings and statement of purpose).
[141] FACT Act, 15 U.S.C. §§ 1681-1681x
[142] FACT Act, 15 U.S.C. § 1681g (a).
[143] FACT Act, 15 U.S.C. § 1681h.

laws at the federal level which only provide the right to data portability for certain types of data such as health data and credit reports. These differences are mainly due to the differences in the legal structures of both legal systems. In the EU, privacy is a fundamental right and guaranteed by the Charter of the Fundamental Rights of the European Union. In the US, privacy is not a fundamental right and thus the policies towards privacy are a market-based approach where laws on privacy center on providing remedies for "consumer harm" and harmonizing privacy with "efficient commercial transactions".[144]

When it comes to the right to data portability, the EU law guarantees every individual the right to receive and to transmit the personal data that belongs to him or her. In the US, individuals have the right to data portability only for certain types of data.

In the EU, non-compliance with the law may result in enormous fines: up to 20 million euro or 4% of the company's annual global turnover, whichever is greater. In the United States, non-compliance with the HITECH Act may result with a penalty as well, but the amount of fine the cover entity would pay is comparatively much lower, only up to 1.5 million US dollars.

The HITECH Act allows covered entities charge a fee for providing data portability, while the GDPR prohibits data controllers to charge a fee except in certain cases. Although the GDPR's right to data portability is not as expansive as it may seem, it is still a strong right that gives power to data subjects to receive and transmit their personal data in a commonly used, machine readable format. In the US, the law does not require data to be provided in such format.

[144] Paul M. Schwartz and Daniel J. Solove, *'Reconciling Personal Information In The United States And European Union'* 102 California Law Review (2014), 877.

CHAPTER II

THE RIGHT TO BE FORGOTTEN

In the digital age, like humans computers also have memories. However, unlike humans who are mortal and whose memory fades over time, digital memory is highly accurate and, without intervention, the information that it has collected can be remembered forever, like Google remembers.[145] Professor Mayer Schönberger, who calls himself the "midwife" of the idea of the right to be forgotten,[146] argues that in the past it was "difficult and costly" to preserve information: however, today it is relatively easy and cheap.[147] Similarly, in earlier times, "forgetting has been the norm and remembering the exception",[148] but in the digital age the balance between remembering and forgetting has changed profoundly.[149] He says that "in our analog past, the default was to discard rather than preserve; today the default is to retain".[150] Although this ability to remember brings with it several benefits, like new discoveries in scientific research, advancements in public health and security[151] and etc., there are also many disadvantages: digital memory can work against us. Things that we have done in the past can be held against us in perpetuity.

In 2007, Andrew Feldmar, a Canadian psychotherapist, was traveling to the United States as he frequently did, when a border control officer decided to search his name in Google, and upon searching, the officer found an article that Mr. Feldmar has written in 2001. [152] Within the article Feldmar mentioned his use of LSD in his youth (roughly 40 years prior), and because of this he

---

[145] Viktor Mayer-Schoenberger, *'Useful Void: The Art of Forgetting in The Age of Ubiquitous Computing'* SSRN Electronic Journal (2007) 1 <http://ssrn.com/abstract=976541> accessed 23 January 2018.

[146] Kate Connolly, *'Right to Erasure Protects People's Freedom to Forget the Past, Says Expert'* (*the Guardian*, 2013) <https://www.theguardian.com/technology/2013/apr/04/right-erasure-protects-freedom-forget-past> accessed 23 January 2018.

[147] Viktor Mayer-Schoenberger, *'Useful Void: The Art of Forgetting in The Age of Ubiquitous Computing'* SSRN Electronic Journal (2007) 5 <http://ssrn.com/abstract=976541> accessed 23 January 2018.

[148] Viktor Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age* (Princeton University Press 2009), 2.

[149] Ibid 92.

[150] Viktor Mayer-Schoenberger, *'Useful Void: The Art of Forgetting in The Age of Ubiquitous Computing'* SSRN Electronic Journal (2007) 4 <http://ssrn.com/abstract=976541> accessed 23 January 2018.

[151] Omer Tene, '*Privacy law's midlife crisis: A critical assessment of the second wave of global privacy laws'* Ohio state law journal (2013) 1247.

[152] Linda Solomon, *'LSD as Therapy? Write About It, Get Barred From US'* (*The Tyee*, 2007) <https://thetyee.ca/News/2007/04/23/Feldmar/> accessed 24 January 2018

was denied an entry to the United States.[153] If not for the search engine, the officer would not likely have read the article that was written six years prior. Due to digital memory, search engines are able to find information in a matter of seconds. Google remembers more things about us than we can do ourselves.[154]

In 2017, a cyclist was photographed showing her middle finger while President Donald Trump's motorcade passed by.[155] The photo was quickly shared on social media, and eventually, the woman identified herself on Facebook.[156] Later, she shared the photo on her own Facebook and Twitter accounts, resulting in termination from her job.[157] Computers make digitalized information easily accessible in a matter of seconds: sometimes to the detriment of individuals.

There is an old saying that time heals all the wounds. Over the years, our priorities, values and views of the world change and we start to forget things. "There is a cognitive dissonance between now and then".[158] For example, instead of one ruminating over a simple mistake for rest of one's life, the human brain forgets certain things with the passage of time and humans rebuild themselves by letting the past live in the past and moving onwards.[159] Modern technology, such as computers and the internet, allows access to memories and information, essentially helping humans to remember everything in perpetuity. Consequently, constant remembering through digitalized memory creates a problem for humans to "reconstruct" themselves.[160]

---

[153] ibid.
[154] Viktor Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age* (Princeton University Press 2009), 7.
[155] Christine Hauser, *'Cyclist Lost Her Job after Raising Middle Finger at Trump's Motorcade'* (*Nytimes.com*, 2017) <https://www.nytimes.com/2017/11/06/us/middle-finger-trump.html> accessed 24 January 2018.
[156] ibid.
[157] ibid.
[158] Kate Connolly, *'Right to Erasure Protects People's Freedom to Forget the Past, Says Expert'* (*the Guardian*, 2013) <https://www.theguardian.com/technology/2013/apr/04/right-erasure-protects-freedom-forget-past> accessed 23 January 2018.
[159] ibid.
[160] ibid.

2.1 THE RIGHT TO BE FORGOTTEN IN THE EUROPEAN UNION

The intellectual origin of the right to be forgotten can be traced to the French law: the 'right to oblivion' (or in French- *'le droit à l'oubli'*).[161] This law specifically provides a convicted criminal who has served his/her sentence, the right to object to the publication of the facts regarding his/her conviction.[162] The right to oblivion is related to privacy in that allows rehabilitated justice-involved individuals to re-enter society without the past conviction harming his/her public image.[163]

Even though, the current data protection law of the European Union, also known as the DPD, does not specifically mention the right to be forgotten, in 2014, the Court of Justice of the European Union (hereinafter the CJEU) found, through the groundbreaking case known as - *Google Spain SL v. Agencia Española de Protección de Datos (AEPD) Mario Costeja González* [164] (hereinafter *Google Spain case*), a right to be forgotten fall within the boundaries of the DPD.

2.1.1 Google Spain Case

In 1998, a Spanish newspaper, *La Vanguardia* published two announcements about a real-estate auction of a property belonging to Mr. Costeja González, a Spanish national living in Spain, for the recovery of social security debts.[165] Later, past and present publications of *La Vanguardia* were digitalized. [166] As a result, a Google search of Mr. González's name revealed hyperlinks to the *La Vanguardia* article associating Mr. González with debt and foreclosure.[167] Mr. González first

[161] Jeffrey Rosen, *'The Right to Be Forgotten'* 64 Stanford Law Review (2012) 88 <https://review.law.stanford.edu/wp-content/uploads/sites/3/2012/02/64-SLRO-88.pdf> accessed 26 January 2018.
[162] ibid.
[163] Lilian Mitrou and Maria Karyda, *'EU'S Data Protection Reform And The Right To Be Forgotten - A Legal Response To A Technological Challenge?'* [2012] 5th International Conference of Information Law and Ethics 2012, Corfu-Greece, June 29-30, 7 <https://ssrn.com/abstract=2165245> accessed 26 January 2018.
[164] Case C-131/12 *Google Spain SL v Agencia Española de Protección de Datos (AEPD) Mario Costeja González* [2014] ECLI: EU: C: 2014:317.
[165] ibid, para 14.
[166] Ibid.
[167] ibid.

contacted the publisher in 2009, and later in 2010 contacted Google requesting the removal of the information or the links but was denied in both instances.[168]

In 2010, Mr. Costeja González filed a complaint with AEPD[169] requesting first, *La Vanguardia* remove or alter those announcements, and second, Google Spain or Google Inc. to remove or conceal the personal data relating to him so that would not appear in the search results.[170] He argued that "the attachment proceedings concerning him had been fully resolved for a number of years and that reference to them was now entirely irrelevant".[171] In other words, although he had paid his debt long ago, because of Google search, his name was still tarnished.

The AEPD did not accept the complaint against the newspaper, arguing that its publication was required by law and "intended to give maximum publicity to the auction" to draw more bidders.[172] However, the AEPD granted the complaint against Google Spain and Google Inc. arguing that search engines are data controllers and therefore, are subject to data protection legislation, the DPD. [173] The AEPD required Google Spain and Google Inc. to remove the links to personal data by the request of the data subject, in this case, Mr. González's data.[174] Google Spain and Google Inc. both separately challenged the AEPD decision in *Audiencia Nacional* (National High Court of Spain), and, eventually, the court referred the set of questions concerning the interpretation of the DPD to the European Court of Justice for preliminary ruling.[175]

The *Audiencia Nacional* referred three sets of questions to the CJEU to determine: first, the Territorial Scope of the DPD; second, the Material scope of the DPD; and, finally, in case these two questions are resolved favorably, to what extent Google, as a data controller, is responsible for the erasure of the data and whether a data subject can directly ask for the data to be removed

[168] Case C-131/12 Google Spain SL Google Inc. v Agencia Española de Protección de Datos (AEPD) Mario Costeja González [2013] ECLI: EU: C: 2013:424, Opinion of AG Jääskinen, paras 19-20.
[169] Agencia Española de Protección de Datos (AEPD) – is the Spanish Data Protection Agency.
[170] Case C-131/12 *Google Spain SL v Agencia Española de Protección de Datos (AEPD) Mario Costeja González* [2014] ECLI: EU: C: 2014:317, paras 14-15.
[171] ibid, para 15.
[172] ibid, para 16.
[173] ibid, para 17.
[174] ibid.
[175] ibid, paras 18-20.

("the right to be forgotten") although it was originally published lawfully by the third party.[176] Having a separate legal personality, Google Spain, as a subsidiary of Google Inc., was established to "promote, facilitate and effect the sale of on-line advertising products and services to third parties and the marketing of that advertising".[177]

Before the Court's decision, the Advocate General of the Court of Justice of the European Union (AG), Niilo Jääskinen, in his opinion on the *Google Spain case*[178] answered the *Audiencia Nacional's* questions. AG Jääskinen first found Google Spain as an establishment since, in his opinion "an economic operator must be considered as a single unit".[179] Second, he argued that even though the search engine operator (Google) can be considered a "processor" of personal data, it cannot be considered a "data controller"[180] since it "does not index or archive personal data against the instructions or requests of the publisher of the web page".[181] Third, AG concluded that the DPD does not provide the right to be forgotten "in the sense that a data subject is entitled to restrict or terminate dissemination of personal data that he considers to be harmful or contrary to his interests".[182] The ruling of the CJEU was in line with the construal of the DPD by the AEPD. However, it was contrary to the advice of the Advocate General, which is unusual.[183]

2.1.1.1 Material scope of the Directive 95/46.

The CJEU started with the interpretation of the second question, what is the material scope of the DPD? The CJEU had to determine:

[176] ibid, para 20 (1) (2) (3); Case C-131/12 Google Spain SL Google Inc. v Agencia Española de Protección de Datos (AEPD) Mario Costeja González [2013] ECLI: EU: C: 2013:424, Opinion of AG Jääskinen, para 6.
[177] ibid, para 43.
[178] Case C-131/12 Google Spain SL Google Inc. v Agencia Española de Protección de Datos (AEPD) Mario Costeja González [2013] ECLI: EU: C: 2013:424, Opinion of AG Jääskinen.
[179] ibid, para 66.
[180] ibid, para 100.
[181] ibid, para 138 (3).
[182] ibid, para 108.
[183] John W. Kropf, *'Google Spain SL V. Agencia Española De Protección De Datos (AEPD). Case C-131/12'* 108 The American Journal of International Law (2014), 504 <http://www.jstor.org/stable/10.5305/amerjintelaw.108.3.0502> accessed 6 February 2018.

First, whether the activity of a search engine which consists in finding information published or placed on the internet by third parties, automatic indexing, temporarily storing and user display should be considered as data processing.[184] The DPD provides that "processing of personal data" means any operation or set of operations which is performed upon personal data, whether automatic or not.[185]

If the answer affirmative then, second, can Google be considered a data controller?[186] The DPD provides that "controller" is a natural or legal person which determines the purpose and means of processing the personal data[187]; whereas "processor" is a natural or legal person which processes the personal data on behalf of the controller.[188]

The CJEU concluded affirmatively to both questions. First, "the activity of a search engine consisting in finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference must be classified as "processing of personal data" within the meaning of Article 2(b)"[189]; and Second, since search engine operator "determines the purposes and means" of data processing, it must "be regarded as the "controller" in respect of that processing pursuant to Article 2(d)".[190]

2.1.1.2 Territorial scope of the Directive 95/46

Article 4 (1) (a) (c) of the DPD stipulates that Directive is applicable to the processing of personal data where the processing is carried out in the context of the activities of an establishment of the controller inside the Member State or the controller is not established in the EU territory but uses equipment for purposes of processing personal data within a Member State, unless such equipment

[184] ibid, para 20 (2)
[185] Data Protection Directive, art 2 (b).
[186] Case C-131/12 *Google Spain SL v Agencia Española de Protección de Datos (AEPD) Mario Costeja González* [2014] ECLI: EU: C: 2014:317, para 21.
[187] Data Protection Directive, art 2 (d).
[188] ibid, art 2 (e).
[189] Case C-131/12 *Google Spain SL v Agencia Española de Protección de Datos (AEPD) Mario Costeja González* [2014] ECLI: EU: C: 2014:317, paras 41.
[190] ibid, para 33.

is only used to transit purposes.[191] Google Spain and Google Inc. argued that because the processing of personal data is performed exclusively by Google Inc. Google Spain as a subsidiary does not intervene in this process.[192]

The CJEU had to decide whether Article 4 (1) (a) and (c) of the DPD applies to Google Inc.,[193] since its subsidiary Google Spain's activities are mainly limited to "promoting and selling advertising space",[194] therefore, the search activity is executed in the United States.

The CJEU concluded that because "the promotion and sale of advertising space" … is Google Inc.'s main source of profit, Google Spain, considered a "stable arrangement" in the form of a subsidiary, and Google Inc., are "closely linked".[195] Therefore, Google Spain is an establishment of Google Inc. in the territory of Spain within the meaning of Article 4 of the DPD, in which case Google Inc. is subject to the Directive.[196]

2.1.1.3 Erasure *of the Information- The Right to Be Forgotten*

After answering the *Audiencia Nacional's* first questions favorably and resolving the threshold matters, the CJEU turned to the question of whether or not the data subject has the right to request the deletion of information under DPD.[197]

The CJEU stressed the requirement of balancing opposing rights laid down by the DPD[198] which provides that "the processing of personal data where it is necessary for the purposes of the legitimate interests pursued by the controller or by the third party … except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject… arising

[191] Data Protection Directive 95/46, art 4 (1) (a) (c).
[192] Case C-131/12 *Google Spain SL v Agencia Española de Protección de Datos (AEPD) Mario Costeja González* [2014] ECLI: EU: C: 2014:317, para 51.
[193] ibid, para 20 (1).
[194] ibid, para 20 (1).
[195] ibid, para 46.
[196] ibid para 60.
[197] ibid para 20 (3).
[198] Data Protection Directive, art 7 (f).

from Articles 7 and 8 of the Charter".[199] Moreover, the privacy rights of the data subject override both the economic interest of the search engine[200] as well as "the interest of the general public in having access to that information upon a search relating to the data subject's name".[201] However, a data subject's privacy rights can be overridden "by the preponderant interest of the general public in having…access to the information in question"[202] such as "the role played by the data subject in public life".[203]

The CJEU concluded that DPD besides providing the data subject's right to access, rectify, erasure or block of information,[204] and to object the information,[205] it also affords the data subject the right to or the right to be forgotten.[206] This means that when information regarding the data subject "appears…to be inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing…the information and links concerned in the list of results must be erased".[207]

2.1.2 Reactions to the CJEU's decision

The CJEU decision on the *Google Spain case* prompted wide discussion and questioning of the court's ruling. While many called the ruling "a menace to the public's right to know," advocates held it as a "privacy victory".[208] Critics mainly challenged two aspects of the CJEU's ruling: first, the finding of search engines to be considered data controllers, and second, "the Court's balancing test, which prioritizes privacy rights over nearly all other".[209]

---

[199] Case C-131/12 *Google Spain SL v Agencia Española de Protección de Datos (AEPD) Mario Costeja González* [2014] ECLI: EU: C: 2014:317, para 74.
[200] ibid, para 81.
[201] ibid, para 99.
[202] ibid, para 97.
[203] ibid, para 81.
[204] Data Protection Directive, art 12 (b).
[205] ibid, art 14 (a).
[206] Case C-131/12 *Google Spain SL v Agencia Española de Protección de Datos (AEPD) Mario Costeja González* [2014] ECLI: EU: C: 2014:317, para 94.
[207] ibid, para 94.
[208] B. Van Alsenoy and M. Koekkoek, *'Internet and Jurisdiction after Google Spain: The Extraterritorial Reach of the 'Right to Be Delisted'* 5 International Data Privacy Law (2015), 105.
[209] The Harvard Law Review Association *'Internet Law — Protection Of Personal Data — Court Of Justice Of The European Unioncreates Presumption That Google Must Remove Links To Personal Data Upon Request. —Case C-*

Opponents asserted that the Court's finding of a search engine to be a data controller has broad implications, and argue that the court should have interpreted the DPD more strictly.[210] The report by the British House of Lords ridiculed the ruling and asserted that "if search engines are data controllers, so logically are users of search engines".[211] There was also concern that as controllers search engines "may be unable" to comply with the law, such as the prohibition against the processing of sensitive data.[212] Any kind of sensitive data published by an internet service provider that shows up in search engine results would render the latter non-compliant. For example, a University web-site, after obtaining express consent from the student, publishes the student's religious affiliation online. Later, a search engine result shows this sensitive data publication upon searching the student's name. In this case, the search engine, as opposed to the university web-site, does not have the consent of the student to process his or her sensitive data. As a result, the search engine can be deemed non-compliant with the law. Under the GDPR, non-compliance for the companies may result with heavy fines – "twenty million Euros or 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher".[213]

However, advocates argued differently, saying a search engine "does not merely passively deliver information, [it] sculpts the results"; and it cannot be "a mere conduit" where information just passes through.[214] It was also argued that "Google's own description of how Internet search works

---

131/12, Google Spain SL V. Agencia Española De Protección De Datos' 128 Harvard Law Review (2014), 739 <http://www.jstor.org/stable/24644058> accessed 25 January 2018.

[210] European Union Committee, House of Lords, 40 *'EU Data Protection Law: A 'Right To Be Forgotten'?*' (The Authority of the House of Lords 2014) para 40 <https://publications.parliament.uk/pa/ld201415/ldselect/ldeucom/40/40.pdf> accessed 6 February 2018; see also The Harvard Law Review Association *'Internet Law — Protection of Personal Data — Court Of Justice Of The European Union creates Presumption That Google Must Remove Links to Personal Data upon Request. —Case C-131/12, Google Spain SL V. Agencia Española De Protección De Datos'* 128 Harvard Law Review (2014), 739 <http://www.jstor.org/stable/24644058> accessed 25 January 2018.

[211] European Union Committee, House of Lords, 40 *'EU Data Protection Law: A 'Right To Be Forgotten'*?' (The Authority of the Housse of Lords 2014), para 41. .<https://publications.parliament.uk/pa/ld201415/ldselect/ldeucom/40/40.pdf> accessed 6 February 2018.

[212] Álvaro Fomperosa Rivero, *'Right to Be Forgotten In the European Court of Justice Google Spain Case: The Right Balance of Privacy Rights, Procedure, And Extraterritoriality'* European Union Law Working Paper, Stanford-Vienna Transatlantic Technology Law Forum (2017), 16 <https://law.stanford.edu/publications/right-to-be-forgotten-in-the-european-court-of-justice-google-spain-case-the-right-balance-of-privacy-rights-procedure-and-extraterritoriality/> accessed 22 January 2017.

[213] General Data Protection Regulation, art 83 (5) (b).

[214] European Union Committee, House of Lords, 40 *'EU Data Protection Law: A 'Right To Be Forgotten'*?' (The Authority of the House of Lords 2014), paras 27-28 <https://publications.parliament.uk/pa/ld201415/ldselect/ldeucom/40/40.pdf> accessed 6 February 2018.

- crawling the web, sorting results, running algorithms to determine what to show, and displaying the final results - neatly mirrors both the legal and intuitive definitions of a data processor and controller", and the CJEU's ruling was based on the construal of DPD's text and "its underlying values".[215]

Opponents also called the ruling "internet censorship"[216] and argued that the Court should have kept the balance between privacy and other rights,[217] "including freedom of information."[218] However, as the Harvard Law Review Association rightly concluded,[219] such criticism of the Court's ruling 'ignores' one important factor- the CJEU interpreted the Directive (DPD) which indeed acknowledges the "the importance of the free flow of data to the economy".[220] Nevertheless, such recognition is "subordinated" by the Directive's objective, enshrined in its first article, of "protect[ing] the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data".[221] In other words, the DPD holds the right to privacy above other rights: therefore, the CJEU's decision on the matter is accurate.

Yale Law professor, Robert Post, asserted that CJEU's decision on the Google Spain case is ambiguous in that it is not clear if the Court wanted to "preserve the right of data subject to control personal information or …to protect the dignity of human being", a concept he calls "dignitary

[215] The Harvard Law Review Association *'Internet Law — Protection of Personal Data — Court Of Justice Of The European Union creates Presumption That Google Must Remove Links to Personal Data upon Request. —Case C-131/12, Google Spain SL V. Agencia Española De Protección De Datos'* 128 Harvard Law Review (2014), 740 <http://www.jstor.org/stable/24644058> accessed 25 January 2018.
[216] Dave Lee, *'Europe Google Ruling 'Astonishing'* (*BBC News*, 2014) <http://www.bbc.com/news/technology-27407017> accessed 7 February 2018.
[217] Martin Husovec, *'Should We Centralize The Right To Be Forgotten Clearing House?'* (*Cyberlaw.stanford.edu*, 2014) <http://cyberlaw.stanford.edu/blog/2014/05/should-we-centralize-right-be-forgotten-clearing-house> accessed 7 February 2018.
[218] The Harvard Law Review Association *'Internet Law — Protection Of Personal Data — Court Of Justice Of The European Union creates Presumption That Google Must Remove Links To Personal Data Upon Request. —Case C-131/12, Google Spain SL V. Agencia Española De Protección De Datos'* 128 Harvard Law Review (2014), 740 <http://www.jstor.org/stable/24644058> accessed 25 January 2018.
[219] ibid, 740.
[220] Data Protection Directive, recital 2.
[221] ibid, art 1.

privacy".[222] He argued that "Google Spain should have interpreted the Directive in a manner that protected dignitary privacy".[223]

2.1.3 The implementation of the ruling of the CJEU

After the decision of the CJEU, Google has created a web form where internet users can request the removal of links they wish to be removed. However, despite its high cost, Google carefully reviews these requests from the data subjects and decides whether or not to remove the link. By February 2018, throughout the European Union, Google had received 2,077,504 URL removal request, but only 43.3% (899,018) of requests were granted, the rest (1,178,486) were denied.[224]

Three years after the *Google Spain case,* the CJEU now must decide two fundamental issues regarding the removal of personal data that the CJEU did not clearly address previously. The first issue came up when four French citizens' requests for delisting were denied by Google and French Data Protection Authority.[225] The CNIL[226] agreed with Google's decision, however, the data subjects took the case to French Supreme Administrative Court (Conseil d'Etat) and eventually the French Court referred the question (case C-136/17) to the CJEU.[227] The CJEU has to decide now if "sensitive personal data, such as the political allegiance of an individual, or a past criminal conviction reported in the press, should always outweigh the public interest".[228] The Working Party, in its guidelines on the implementation of the CJEU judgement on the *Google Spain Case* provided that since sensitive data "has a greater impact on" individuals "than ordinary personal

[222] Robert Post, *'Data Privacy and Dignitary Privacy: Google Spain, The Right To Be Forgotten, And The Construction Of The Public Sphere'* SSRN Electronic Journal [2017], 13 <https://ssrn.com/abstract=2953468> accessed 12 February 2018.
[223] Ibid.
[224] Google Transparency Report '*Search removals under European privacy law*' (*Transparencyreport.google.com*, 2018) <https://transparencyreport.google.com/eu-privacy/overview> accessed 25 February 2018.
[225] Peter Fleischer, *'Three Years of Striking the Right (To Be Forgotten) Balance*' (*Google*, 2017) <https://www.blog.google/topics/google-europe/three-years-right-to-be-forgotten-balance/> accessed 26 February 2018.
[226] Commission Nationale de l'informatique et des Libertés (CNIL) is a French Data protection Regulator.
[227] Peter Fleischer, *'Three Years of Striking the Right (To Be Forgotten) Balance*' (*Google*, 2017) <https://www.blog.google/topics/google-europe/three-years-right-to-be-forgotten-balance/> accessed 26 February 2018.
[228] ibid.

data…[Data Protection Authorities are] more likely to intervene when de-listing requests are refused…".[229]

The second issue came up when the CNIL went against Google's decision to limit the right to be forgotten first only "to Google.fr, and other European Google domains, and then to any Google user based in Europe".[230] Google argued that global delisting will set "a grave precedent" for countries that are not as democratic as France, and it should not be allowed that one country is able to "impose" laws on individuals of another country.[231] The French Data Protection Regulator argued that the right to be forgotten "is only worth anything if it applies universally," otherwise, anyone can circumvent the law by simply changing his or her IP address to a non-EU country or can ask someone from another country to look for information.[232] Google appealed the CNIL's decision to French high court and, in 2017, the French Court has referred the question to the CJEU. [233] The CJEU now has to decide whether or not search engines "have to delete links only in the country that requests it, across the EU, or …globally".[234]

2.1.4 The right to be forgotten under the GDPR

The right to be forgotten has been included in the GDPR, and will enter into force on the 25th of May, 2018. The provision that contains the right to be forgotten, it is believed, will likely be interpreted "in light of Google Spain case".[235]

---

[229] Article 29 Data Protection Working Party, *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González"* C-131/12 (Nov. 26, 2014), 17.

[230] Alex Hern, *'ECJ to Rule on Whether 'Right to Be Forgotten' Can Stretch Beyond EU'* (*the Guardian*, 2017) <https://www.theguardian.com/technology/2017/jul/20/ecj-ruling-google-right-to-be-forgotten-beyond-eu-france-data-removed> accessed 26 February 2018.

[231] Peter Fleischer, *'Three Years of Striking the Right (To Be Forgotten) Balance*' (*Google*, 2017) <https://www.blog.google/topics/google-europe/three-years-right-to-be-forgotten-balance/> accessed 26 February 2018.

[232] Alex Hern, *'ECJ to Rule on Whether 'Right to Be Forgotten' Can Stretch Beyond EU'* (*the Guardian*, 2017) <https://www.theguardian.com/technology/2017/jul/20/ecj-ruling-google-right-to-be-forgotten-beyond-eu-france-data-removed> accessed 26 February 2018.

[233] ibid.

[234] ibid.

[235] Robert Post, *'Data Privacy and Dignitary Privacy: Google Spain, The Right To Be Forgotten, And The Construction Of The Public Sphere'* SSRN Electronic Journal [2017], 5 <https://ssrn.com/abstract=2953468> accessed 12 February 2018.

Article 17 of the GDPR, named "right to erasure" ('right to be forgotten'), provides that:

> "*The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay…*"

The article sets the conditions[236] when the personal data should be deleted:

a) the personal data are no longer necessary in relation to the purpose of their collection/processing;
b) the data subject withdraws his/her consent/explicit consent and there is no other legal ground for processing;
c) the data subject objects the processing;
d) unlawful processing;
e) the personal data has to be erased for compliance with a legal obligation required by law;
f) the personal data has been collected in relation to the offer of information society services concerning Children.

Regarding children's data, the data subject has the right to ask for erasure of the personal data provided to the controller when the data subject was a child at "any time".[237] However, the controller's obligation does not end with the erasure of the data subject's data. The law requires that where the controller has made the personal data public and has been obliged to erase the data, under the conditions mentioned above, "the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, …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".[238]

The GDPR also requires that "in order to ensure fair and transparent processing" of personal data, controllers shall inform the data subjects about the existence of the right to rectification or erasure

[236] General Data Protection Regulation, art 17 (1).
[237] *'Can I Ask A Company To Delete My Personal Data?'* (*European Commission - European Commission*, 2018) <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/can-i-ask-company-delete-my-personal-data_en> accessed 8 February 2018; see also General Data Protection Regulation, recital 65.
[238] General Data Protection Regulation, art 17 (2), recital 66.

(the right to be forgotten) as well as right to data portability.[239] This requirement is applicable both when the data are collected directly[240] from the data subject as well as indirectly[241] from third parties.

There are also some exceptions where the right to be forgotten may be denied to the data subject. The GDPR provides that the right to be forgotten shall not apply when processing is necessary:[242]

a) for exercising the right of freedom of expression and information;
b) for compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
c) for reasons of public interest in the area of public health;
d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes; or
e) for the establishment, exercise or defense of legal claims.

2.1.5 Removing the data under the GDPR

Finding the right balance between the right to privacy and the right to freedom of expression can be quite a challenge for the controllers, especially when the data subject is a public figure or well-known to the public. The European Court of Human Rights (ECtHR) has ruled differently in similar situations. In *Von Hannover vs. Germany case (2004)*, the ECtHR found that "anyone, even if they are known to the general public, must be able to enjoy a "legitimate expectation" of protection and respect for their private life".[243] Therefore, the Court ruled that the German Court's decision that allowed the photographs taken of Carolina von Hannover, the Princess of Hannover, in public places as a violation of her right to respect for her private and family life.[244] However, in *Von Hannover vs. Germany case No.2 (2012)*,[245] the ECtHR ruled differently. The Court found Princess Carolina as a "public figure"[246] and ruled that there was no violation of her right to privacy.

[239] ibid, art 13 (2) (b).
[240] ibid, art 13.
[241] ibid, art 14.
[242] General Data Protection Regulation, art 17 (3).
[243] Von Hannover v. Germany no 59320/00 (ECtHR, 24 June 2004) para 69.
[244] Von Hannover v. Germany no 59320/00 (ECtHR, 24 June 2004).
[245] Von Hannover v. Germany (no. 2) nos. 40660/08 and 60641/08 (ECtHR, 7 February 2012).
[246] ibid, para 90.

The issues as complex as in the above-mentioned cases will be problematic for the controllers when it comes to deciding whether to take down certain information or to keep it. Given that non-compliance with the GDPR could lead to heavy fines, controllers, especially the small ones, will likely not take a risk and will remove data upon request.

Another problem with removing the data arises "when [an] individual asks for the deletion of content about them by a third party".[247] For example: persons A and person B have taken a picture together. Said photo was later posted on a social media site by person A. Person B requests the deletion of the picture, while person A wants to keep it. In such a case, the law has to strike a balance among the rights of four parties: the data subject who requests the removal, the controller, the person who put the information online, and the people who wish to see the information.[248] The GDPR delineates the legal conditions in a way that it is doubtful that finding the right balance in serving the right of each of these parties is entirely possible.[249] This could be an issue not only for controllers but also for Data Protection Authorities and the Courts since they each have to be "weighing the interests of all four parties".[250]

2.2 THE RIGHT TO BE FORGOTTEN IN THE UNITED STATES OF AMERICA

In the United Sates, California is a state that is well-known for its progressiveness. As mentioned above, the US Constitution does not have any mention of privacy: however, the state constitution of California provides for a right to privacy to its citizens.[251] California was the first state to enact

[247] George Brock, *the Right to Be Forgotten: Privacy and the Media in the Digital Age* (I.B. Tauris & Co. Ltd 2016) 77.
[248] Daphne Keller, *'The GDPR'S Notice and Takedown Rules: Bad News For Free Expression, But Not beyond Repair'* (*Cyberlaw.stanford.edu*, 2015) <http://cyberlaw.stanford.edu/blog/2015/10/gdpr%E2%80%99s-notice-and-takedown-rules-bad-news-free-expression-not-beyond-repair> accessed 12 February 2018.
[249] George Brock, the *Right to Be Forgotten: Privacy and the Media in the Digital Age* (I.B. Tauris & Co. Ltd 2016) 77.
[250] ibid, 77.
[251] Constitution of the State of California, art 1.

a law that requires companies to notify their customers of a security breach.[252] In 2003, by adoption of the Online Privacy Act,[253] California became the first state in the United States to require an operator of a commercial web site or online service to have privacy policies on its web site that describes for the users how their personal data are handled.[254] In 2013, an amendment was made to the Online Privacy Act which required companies to "disclose how they respond to "do not track" requests" of Internet and mobile app users.[255]

Since 2014, it has been a criminal offense in California[256] to intentionally make video recordings or photos of an individual that contains intimate body parts and to distribute it without the consent of the data subject. [257] Doing so may cause which causes the latter "serious emotional distress."[258] However, this law, also known as the law against "revenge porn"[259], does not require the posted content to be erased, it only holds the person who posts the content "liable for a misdemeanor."[260]

There is no comprehensive Federal privacy law similar to the GDPR that provides for the right to be forgotten in the United States. There is a federal law, called the Digital Millennium Copyright Act (DMCA), adopted by the US Congress in 1998, that requires providers to "expeditiously remove" or block access to online content when there is a copyright infringement notification.[261] However, this law applies only to copyright infringement, not to privacy.

---

[252] Somini Sengupta, *'Sharing, With A Safety Net'* (*Nytimes.com*, 2013) <http://www.nytimes.com/2013/09/20/technology/bill-provides-reset-button-for-youngsters-online-posts.html> accessed 2 March 2018.

[253] The Online Privacy Protection Act of 2003, Cal. Bus. & Prof. Code §§ 22575 - 22579 (Cal. 2003) <https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=8.&chapter=22.&lawCode=BPC> accessed 2 March 2018.

[254] Somini Sengupta, *'Sharing, With A Safety Net'* (*Nytimes.com*, 2013) <http://www.nytimes.com/2013/09/20/technology/bill-provides-reset-button-for-youngsters-online-posts.html> accessed 2 March 2018.

[255] Travis Crabtree, *'Does California's Amended Online Privacy Law Mean We All Have To Change Our Privacy Policies? | Emedia Law Insider'* (*eMedia Law Insider*, 2013) <https://www.emedialaw.com/does-californias-new-law-mean-we-all-have-to-change-or-privacy-policy/> accessed 2 March 2018.

[256] Assembly Bill 2643, 2014 Leg., 2013-2014 Sess. (Cal. 2014) <https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140AB2643>accessed 16 March 2018.

[257] California Penal Code § 647(j) (4) (A).

[258] ibid.

[259]Eric Goldman, *'California's New Law Shows It's Not Easy to Regulate Revenge Porn'* (*Forbes.com*, 2013) <https://www.forbes.com/sites/ericgoldman/2013/10/08/californias-new-law-shows-its-not-easy-to-regulate-revenge-porn/#368a490427bb> accessed 2 March 2018.

[260] Lawrence Siry, *'Forget Me, Forget Me Not: Reconciling Two Different Paradigms Of The Right To Be Forgotten'* 103 Kentuky Law Journal (2014) 339.

[261] DMCA, 17 U.S.C. § 512

There was a case law in 1931, *Melvin v. Reid*,[262] in which consideration or, as one author said, "the ghosts" of the right to be forgotten can be seen.[263] The plaintiff was an ex-prostitute who was also charged with murder. [264] However, she was acquitted, and had left her past behind her.[265] She had married and had "led a life of rectitude in respectable society" without any of her friends knowing about her past.[266] The defendant in *Melvin v. Reid* made a movie based on plaintiff's life, called "The Red Kimono", in which her real name was used.[267] This public exposure of the plaintiff's past caused her friends to abandon and condemn her.[268]

The California Appellate Court noted that "there was a social value in having one's past forgotten", and asserted that "one of the major objectives of society as it is now constituted, and of the administration of our penal system, is the rehabilitation of the fallen and the reformation of the criminal". [269] The Court ruled in favor of the plaintiff by holding that the movie violated her "right to privacy".[270] Even though this is "no longer good law", because later the case was overturned, it shows that the right to be forgotten is not an absolutely alien notion in the law of the United States.[271]

2.2.1 Legal forgiveness (right to oblivion)

The right to oblivion does exist in the United States and such laws are intended to help people with past convictions be able to return to society by providing rights to conceal their past activities, such as "non-violent juvenile" crimes or "old credit information".[272] Some states have laws that

[262] Melvin v. Reid, 112 Cal. App. 285 (Cal. Ct. App. 1931).
[263] Ravi Antani, *'The Resistance Of Memory: Could The European Union's Right To Be Forgotten Exist In The United States'* 30 Berkeley Tech. L.J. (2015), 1185.
[264] William L. Prosser, '*Privacy*' 48 California Law Review (1960), 392.
[265] ibid.
[266] ibid.
[267] ibid.
[268] ibid.
[269] Ravi Antani, *'The Resistance Of Memory: Could The European Union's Right To Be Forgotten Exist In The United States'* 30 Berkeley Tech. L.J. (2015), 1185.
[270] ibid, 1185.
[271] ibid, 1185.
[272] Ravi Antani, *'The Resistance Of Memory: Could The European Union's Right To Be Forgotten Exist In The United States'* 30 Berkeley Tech. L.J. (2015), 1196.

permit "sealing" of juvenile criminal records, and these laws are intended to prevent actions done in a person's youth to negatively affect him or her when in adulthood.[273]

The Bankruptcy Code[274] of the United States, *inter alia*, also provides for legal forgiveness. In order to give a second chance to individuals, unable to be economically productive because of past debt, the bankruptcy discharge principle provides that a debtor's "financial obligations" should be forgiven.[275] Furthermore, the Bankruptcy Code prohibits "public and private actors to limit opportunities because of the [bankruptcy] information",[276] such as employment.[277]

However, it is argued that the benefits of these forgiveness laws can be taken away by a simple "Google search", and the only way to prevent the loss of such benefits is to provide individuals the "right to be forgotten".[278]

2.2.2 California Senate Bill 568 ("erasure bill")

In September 2013, California Governor Jerry Brown signed the Senate Bill 568[279] (SB 568), also known as the "eraser bill", [280] or the right to be forgotten, and entered it into force on January 1, 2015.[281] The law allows internet users to remove information that they provided to an operator of

[273] Robert Kirk Walker, *'The Right to Be Forgotten'* 64 Hastings Law Journal (2012), 272 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2017967> accessed 26 January 2018.
[274] Bankruptcy Code 11 U.S.C. § 525(a)
[275] Rafael I. Pardo and Michelle R. Lacey, *'Undue Hardship in the Bankruptcy Courts: An Empirical Assessment of the Discharge of Educational Debt'* 74 University of Cincinnati Law Review (2005) 416 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=706761> accessed 5 March 2018.
[276] Meg Leta Ambrose and Jef Ausloos, *'The Right to Be Forgotten across the Pond'* SSRN Electronic Journal [2012] 9 <https://ssrn.com/abstract=2032325> accessed 2 March 2017.
[277] Bankruptcy Code 11 U.S.C. § 525(b)
[278] Ravi Antani, *'The Resistance Of Memory: Could The European Union's Right To Be Forgotten Exist In The United States'* 30 Berkeley Tech. L.J. (2015), 1196.
[279] S.B. 568, 2013 Leg., 2013-2014 Sess. (Cal.2013) <http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB568> accessed 2 March 2018 (hereinafter California S.B 568).
[280] Ronnie Cohen, *'California Law Allows Kids to Erase Digital Indiscretions'* (*Reuters*, 2013) <https://www.reuters.com/article/net-us-usa-california-internet/california-law-allows-kids-to-erase-digital-indiscretions-idUSBRE98N15M20130924> accessed 2 March 2018.
[281] California S.B. 568, para 22582.

an internet web-site. SB 586 does not provide general removal of information or the right to be forgotten, however, it applies to only minors, individuals who are under 18 years old, and who posted the information themselves.[282]

The Bill has two major provisions. The first provision[283] bars "an operator of an Internet Web site, online service, online application, or mobile application" (hereinafter- internet service provider) from marketing or advertising certain products or services to minors such as electronic cigarettes, handguns, and alcohol etc.[284] (*Since this provision is not the topic of this paper, it will not be further discussed*).

The second provision gives California minors a right to remove content (the right to be forgotten) that they provided to an internet service provider.[285] The law also gives an option to an operator of an internet service provider to decide whether removal is to be done by the minor him or herself, or to be removed by the operator of a web site at the request of the minor.[286] An internet service provider is required to give notice to a minor, who is posting information on the operator's web site, of his or her right to removal of the information.[287] However, the law provides that internet service provider is not required to collect users' age data.[288] This is one of the limitations of the law. An internet service provider can avoid the law by simply not collecting the user's age. Some social networking sites such as Facebook and Twitter provide a function to delete the content after it was posted by a user, and both of them collect the information about user's age: other providers simply may choose not to.

Furthermore, SB 568 provides that the law is applicable when the service provider "has actual knowledge that a minor is using its Internet Web site".[289] The wording, 'actual knowledge' is not defined by the law. In the absence of a requirement to collect the user's age, proving the service provider's actual knowledge will be quite challenging, if not impossible.

[282] ibid, para 22580 (d).
[283] ibid, para 22580.
[284] California S.B. 568, para 22580 (a) (i).
[285] ibid, para 22581 (a) (1).
[286] ibid para 22581 (a) (1).
[287] ibid para 22581 (a) (2).
[288] ibid para 22581 (e).
[289] ibid para 22581 (a).

The law also requires internet service providers to give minors "clear instruction" about the procedure of removing the posted information or, if the provider wishes, the procedure to request the internet service provider to remove the posted content.[290]

There are also several conditions, provided by the law, in which the internet service provider is not obliged to remove or make removal of the content available for a minor:[291]
(1) If retention of the content is required by any other law - federal or state.
(2) If the content is posted to the internet provider's web site by a third party, or the content is reposted by a third party.
(3) In case, the information of minor is anonymized by the internet service provider that identification of the minor is no longer possible.
(4) If the minor does not follow the instructions of removal which is provided by the internet service provider.
(5) In case, there was a compensation for the content that the minor has received.

The second circumstance limits the effectiveness of the removal procedure. If a minor shares content online and said content is later shared by others, he/she will only be able to delete the photo which he/she has posted. The content shared by the others will still be circulating on the internet. It seems that by not requiring the removal of content posted by third party, the legislators tried to make sure that the law does not infringe upon the freedom of speech.[292]

Nowadays, social networking sites have a function to receive complaints on content that is deemed "offensive or defamatory", and after review of flagged content can be taken down if the operator wishes to do so.[293] However, if someone deliberately shares non-offensive photos of a minor to cause harm, there is no remedy provided by the law. Facebook has a social reporting function that allows users to contact to the person who posted the content on Facebook and request to take it down, or in case the user does not wish to make a direct contact with the poster of the content,

[290] ibid para 22581 (a) (3).
[291] ibid para 22581 (b).
[292] Lawrence Siry, *'Forget Me, Forget Me Not: Reconciling Two Different Paradigms of the Right to Be Forgotten'* 103 Kentuky Law Journal (2014) footnote 187.
[293] Ibid, 334.

he/she can do it through someone else, or can block the person who posted the content.[294] Nevertheless, this "remedy" provided by Facebook is not a very effective tool to fully solve this complex issue.

Furthermore, the law does not require internet service providers to erase the data completely or comprehensively[295] and renders that the provider will be "deemed complaint" if the content is made invisible to other internet users and the public, and the operator can keep the content in its servers.[296] This means that the controller can still keep the data forever, as long as it is not made public.

The scope of the law is limited since the text of the law suggests that it covers people only until they are eighteen years old, meaning that the content can be removed only if the minor posted the information online and requested to remove it before he or she reaches the age od 18.[297] A legal scholar, Lawrence Siry, argues that the law may be construed expansively, letting the user above 18 years of age request the removal of the data that was made by the user when he or she was under 18: however, he says, such interpretation would be against the wording of the law.[298]

Last, but not least, SB 568 does not provide a minor the right to bring a lawsuit against the service provider.[299] Nevertheless, a minor can bring "a civil action" that "allows for injunctive relief and civil penalties of up to $2,500" for each violation under California Business and Professions Code § 17200.[300]

---

[294] Facebook Help Centre, *'What Is Social Reporting?*' (*Facebook.com*, 2018) <https://www.facebook.com/help/128548343894719> accessed 6 March 2018.
[295] California S.B. 568, para 22581 (a) (4).
[296] ibid para 22581 (c).
[297] Lawrence Siry, *'Forget Me, Forget Me Not: Reconciling Two Different Paradigms Of The Right To Be Forgotten'* 103 Kentuky Law Journal (2014) 334.
[298] ibid 334.
[299] Thomas R. Burke and others, *'California's "Online Eraser" Law for Minors to Take Effect Jan. 1, 2015'* (*dwt.com*, 2014) <https://www.dwt.com/Californias-Online-Eraser-Law-for-Minors-to-Take-Effect-Jan-1-2015-11-17-2014/> accessed 14 March 2018.
[300] ibid.

2.2.3 Issues of SB 568

While advocates of the law argued that it would guard Californian minors' educational and "professional" reputation,[301] opponents questioned the constitutionality of the law.[302] A major concern of the right to be forgotten is that it may infringe upon free speech. In the United States, the First Amendment of the US Constitution provides strong protection of the freedom of speech. This protection applies to speech and content on the internet, as well. In 2013, the Fourth US Circuit Court of Appeals ruled that "liking" on Facebook is an act of speech, and is therefore protected by the First Amendment.[303] Since "liking" is an expression, it is not clear whether the removal of content which is "liked" by others would amount to the infringement of free speech. The First Amendment protects against government intrusion, nevertheless, when removal is required by a statutory law, it is clear that there is state involvement.[304]

Even if SB 568 passes the free speech test, it also faces another challenge: to pass "the dormant Commerce clause" of the US constitution, otherwise it may be deemed unconstitutional. Provided by Article 1, section 8 of the US constitution, Congress has the power "to regulate commerce … among the several states".[305] Based on this clause, the United States Supreme Court ruled that the Commerce Clause has "a dormant aspect" which bars states from adopting laws that obstruct interstate commerce.[306] Since the origin of online activity derives from beyond the boundaries of states, passing a law to regulate the Internet prompts constitutional restraint.[307] Thus, it was argued that since SB 568 would greatly burden internet service providers outside the borders of the state of California, it infringes upon "the dormant Commerce Clause".[308]

---

[301] James Lee, *'SB 568: Does California's Online Eraser Button Protect the Privacy of Minors'* 48 U.C.D. Law Review (2015) 1173.
[302] Lawrence Siry, *'Forget Me, Forget Me Not: Reconciling Two Different Paradigms Of The Right To Be Forgotten'* 103 Kentuky Law Journal (2014) 334.
[303] Jonathan Stempel, *'Facebook 'Like' Deserves Free Speech Protection: U.S. Court'* (*Reuters.com* 2013) <https://www.reuters.com/article/net-us-usa-speech-facebook/facebook-like-deserves-free-speech-protection-u-s-court-idUSBRE98H0X620130918> accessed 3 March 2018
[304] Lawrence Siry, *'Forget Me, Forget Me Not: Reconciling Two Different Paradigms Of The Right To Be Forgotten'* 103 Kentuky Law Journal (2014) 335.
[305] The U.S. Constitution, art 1, Sec. 8, Cl. 3.
[306] James Lee, *'SB 568: Does California's Online Eraser Button Protect the Privacy of Minors'* 48 U.C.D. Law Review (2015) 1178.
[307] Dan L. Burk, *'Federalism in Cyberspace'* 28 Connecticut Law Review (1996) 1096 <https://ssrn.com/abstract=44433> accessed 3 March 2018.
[308] James Lee, *'SB 568: Does California's Online Eraser Button Protect the Privacy of Minors'* 48 U.C.D. Law Review (2015) 1173.

So far, the constitutionality of the SB 568 has not been challenged. Whether it will pass the constitutionality test or not, we need to wait until such a case appears before the Court of law. However, because "the dormant Commerce Clause" only applies to States, if Congress moves first and enacts a similar law, then the SB 568 will not face a constitutionality challenge.

SUMMARY OF THE RIGHT TO BE FORGOTTEN IN THE EUROPEAN UNION AND THE UNITED STATES

Although allowing an individual's past to be forgotten or the right to oblivion exists both in the EU and the US, this right is broader and more widespread in the EU than in the USA. However, when it comes to the right to be forgotten in the realm of online privacy, the right provided by the GDPR in the EU is much wider in scope and application than the right provided by California's Senate Bill 568.

In the EU, the law applies to personal data of all of the residents of the European Union, whereas in California, the right applies to only the personal data that belongs to those under 18 years old. The GDPR applies to all the companies within and outside of the EU if they process the data of the EU residents. SB 568 applies only to the companies within the United States.

The GDPR provides for the complete removal of personal data upon the data subject's request, whereas the SB 568 does not require companies to erase the data completely: making it invisible to the user and public is enough to be compliant with the law. The law in the EU obliges companies to request the removal of data to prevent the passage of data to a 3rd party. In California, companies have no such obligation. Both the EU and California law requires companies to inform the users about their right to be forgotten.

When it comes to compliance with the law, since the scope and application of the GDPR is wider than that of SB 568, it more complex to comply with right to be forgotten in EU than it is in California. One of the biggest challenges for the companies to comply with right to be forgotten

under the GDPR is that they must weigh the right to be forgotten with other rights, especially with the right to freedom of expression. In California, the legislators made sure that there are no major conflicting issues with freedom of expression, which otherwise would likely have rendered the law unconstitutional. Thus, the right to erasure provided by SB 568 applies only data provided directly by the minor him or herself, and not to content posted by 3rd parties.

CONCLUSION

While the GDPR is the most advanced legal reform regarding online privacy in the world, compliance with the law, especially with its two new rights, the right to data portability and the right to be forgotten, it is also the most challenging compliance issue for companies around the world. The GDPR's right to portability and the right to be forgotten are very broad rights that give data subjects in the European Union control of their personal data.

Compared to the EU, in the US, these two rights are significantly limited in scope and application. The right to data portability or its element, the right to receive, can be found in some sectoral laws in the US, nevertheless, the scope of these laws is quite limited and applies to only certain types of data.

Legal forgiveness, the fundamental basis of the right to be forgotten, exists in the US only for financial wrongdoings. However, California's SB 568, known as the erasure bill, is the first law in the US that provides the right to be forgotten for online service users. Nevertheless, compared to the GDPR, SB 568 is limited in application and scope as it applies only to California minors and not the rest of the general public. These significant differences between the EU law and the law in the US are due to the fundamental structural differences between the two legal systems. In the US, the freedom of expression and the public's right to know has traditionally been stronger than the right to privacy, and any attempt to increase the right to privacy may potentially be interpreted as a restraints on free speech or the right to information.

At the time of writing this paper, the privacy of personal data has gained national attention in the US. It is hard to envisage whether or not the US will adopt new privacy regulation. However, based on the history of the privacy in the US, it is safe to assume that such regulation will not be as broad as the EU's GDPR.

BIBLIOGRAPHY

I. Primary Sources

Article 29 Data Protection Working Party, *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González"* C-131/12 (Nov. 26, 2014)

Article 29 Data Protection Working Party, *Guidelines on the right to data portability*, (As last Revised and adopted on 5 April 2017)

Article 29 Data Protection Working Party, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC,* (adopted on 9 April 2014)

Assembly Bill 2643, 2014 Leg., 2013-2014 Sess. (Cal. 2014) <https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140AB2643>accessed 16 March 2018

Bankruptcy Code 11 U.S.C. § 525

California Penal CODE § 647(j) (4) (A)

Case C-131/12 Google Spain SL Google Inc. v Agencia Española de Protección de Datos (AEPD) Mario Costeja González [2013] ECLI: EU: C: 2013:424, Opinion of AG Jääskinen.

Case C-131/12 *Google Spain SL v Agencia Española de Protección de Datos (AEPD) Mario Costeja González* [2014] ECLI: EU: C: 2014:317

Charter of Fundamental Rights of the European Union (2000)

Children's Online Privacy Protection Act (COPPA) of 1998, 15 U.S.C. §§ 6501–6506

Council Directive (EU) 2015/2366 of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC OJ L 337/35 (PSD2)

Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31

Council Regulation (EU) 2016/679 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 [2016] OJ L119/1

Department of Health and Human Services, 45 Code of Federal Regulations § 160.103

Digital Millennium Copyright Act, 17 U.S.C. § 512

Fair and Accurate Credit Transactions Act of 2003, 15 U.S.C. §§ 1681-1681x

Fair Credit Reporting Act, 15 U.S.C. § 1681

Family Educational Rights and Privacy Act (FERPA) of 1974, 20 U.S.C. § 1232g

Gramm–Leach–Bliley Act (GLBA) of 1999, 15 U.S.C. § 6809(4) (A)

Health Information Technology for Economic and Clinical Health Act, 42 U.S.C. § 17935(e) (1) (2009)

Health Insurance Portability and Accountability Act, 42 U.S.C. § § 17921 to 17953 (1996)

Melvin v. Reid, 112 Cal. App. 285 (Cal. Ct. App. 1931)

Senate Bill 568, 2013 Leg., 2013-2014 Sess. (Cal.2013) <http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB568> accessed 2 March 2018

Telecommunications Act, 47 U.S.C. § 251 (b) (2)

The Online Privacy Protection Act of 2003, Cal. Bus. & Prof. Code §§ 22575 - 22579 (Cal. 2003)<https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=8.&chapter=22.&lawCode=BPC> accessed 2 March 2018

The Public Health and Welfare, 42 U.S.C. § 1395x <https://www.gpo.gov/fdsys/pkg/USCODE-2010-title42/pdf/USCODE-2010-title42-chap7-subchapXVIII-partE-sec1395x.pdf> accessed 15 March 2018

The Public Health and Welfare, 42 U.S.C. 300gg-91(a) (2)

Video Privacy Protection Act (VPPA), 18 U.S.C. § 2710 (2012).

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

Von Hannover v. Germany no 59320/00 (ECtHR, 24 June 2004)

II. Secondary Sources

'A - European Data Protection Supervisor' (*European Data Protection Supervisor*, 2018) <https://edps.europa.eu/data-protection/data-protection/glossary/a_en> accessed 11 January 2018

Ambrose M and Ausloos J, *'The Right to Be Forgotten across the Pond'* SSRN Electronic Journal [2012] 1 <https://ssrn.com/abstract=2032325> accessed 2 March 2017

Antani R, *'The Resistance of Memory: Could the European Union's Right to Be Forgotten Exist in the United States?'*30 Berkeley Technology Law Journal (2015) 1173 <http://www.dataprotection.ro/servlet/ViewDocument?id=1080> accessed 22 January 2018

Antani R, *'The Resistance Of Memory: Could The European Union's Right To Be Forgotten Exist In The United States'* 30 Berkeley Tech. L.J. (2015) 1173

Baird S, *'GDPR Matchup: The Health Insurance Portability and Accountability Act'* (*Iapp.org*, 2017)<https://iapp.org/news/a/gdpr-match-up-the-health-insurance-portability-and-accountability-act/> accessed 3 March 2018

Blue Button, *'Blue Button Home'* (*Va.gov*, 2017) <https://www.va.gov/bluebutton/> accessed 3 March 2018

Brock G, *the Right to Be Forgotten: Privacy and the Media in the Digital Age* (I. B. Tauris & Co. Ltd 2016)

Brock G, *the Right to Be Forgotten: Privacy and the Media in the Digital Age* (IBTauris & Co, Ltd 2016)

Burk D, *'Federalism in Cyberspace'* 28 Connecticut Law Review (1996) 1095 <https://ssrn.com/abstract=44433> accessed 3 March 2018

Burke T and others, *'California's "Online Eraser" Law for Minors to Take Effect Jan. 1, 2015'* (*dwt.com*, 2014) <https://www.dwt.com/Californias-Online-Eraser-Law-for-Minors-to-Take-Effect-Jan-1-2015-11-17-2014/> accessed 14 March 2018

Burri M and Schär R, *'The Reform of the EU Data Protection Framework: Outlining Key Changes And Assessing Their Fitness For A Data-Driven Economy'* 6 Journal of Information Policy (2016) 479 <http://www.jstor.org/stable/10.5325/jinfopoli.6.2016.0479> accessed 7 February 2018

'Can I Ask A Company To Delete My Personal Data?' (*European Commission - European Commission*, 2018) <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/can-i-ask-company-delete-my-personal-data_en> accessed 8 February 2018

Cohen R, *'California Law Allows Kids to Erase Digital Indiscretions'* (*Reuters.com*, 2013) <https://www.reuters.com/article/net-us-usa-california-internet/california-law-allows-kids-to-erase-digital-indiscretions-idUSBRE98N15M20130924> accessed 2 March 2018

Connolly K, *'Right to Erasure Protects People's Freedom to Forget the Past, Says Expert'* (*the Guardian*, 2013) <https://www.theguardian.com/technology/2013/apr/04/right-erasure-protects-freedom-forget-past> accessed 23 January 2018

Crabtree T, *'Does California's Amended Online Privacy Law Mean We All Have To Change Our Privacy Policies? | Emedia Law Insider'* (*eMedia Law Insider*, 2013) <https://www.emedialaw.com/does-californias-new-law-mean-we-all-have-to-change-or-privacy-policy/> accessed 2 March 2018

Daniel J. Solove and Woodrow Hartzog, *'The FTC and the New Common Law of Privacy'* Vol. 114, No. 3, Columbia Law Review (2014) 583

'Data Protection in Europe- Academics Are Taking a Position' 29 Elsevier: Computer Law & Security Review (2013) 180 <https://www.sciencedirect.com/science/article/pii/S026736491300037X> accessed 2 February 2018

Elvy S, *'Paying for Privacy and the Personal Data Economy*' 117 Columbia Law Review Association, Inc. (2017) 1369 <http://www.jstor.org/stable/44392955> accessed 7 February 2018

'European Commission, Experts Uneasy over WP29 Data Portability Interpretation | 7Wdata' (*7wData*, 2018) <http://www.7wdata.be/privacy-issues/european-commission-experts-uneasy-over-wp29-data-portability-interpretation/> accessed 15 January 2018

European Union Committee, House of Lords, *'EU Data Protection Law: A 'Right To Be Forgotten'?'* (The Authority of the House of Lords 2014) <https://publications.parliament.uk/pa/ld201415/ldselect/ldeucom/40/40.pdf> accessed 6 February 2018

Facebook Help Centre *'What Is Social Reporting?'* (*Facebook.com*, 2018) <https://www.facebook.com/help/128548343894719> accessed 6 March 2018

Fleischer P, *'Three Years of Striking the Right (To Be Forgotten) Balance'* (*Google*, 2017) <https://www.blog.google/topics/google-europe/three-years-right-to-be-forgotten-balance/> accessed 26 February 2018

Francis L, *'When Patients Interact With EHRs: Problems of Privacy and Confidentiality'* 12 Houston Journal of Health Law & Policy (2012) 171.

Goldman E, *'California's New Law Shows It's Not Easy to Regulate Revenge Porn'* (*Forbes.com*, 2013) <https://www.forbes.com/sites/ericgoldman/2013/10/08/californias-new-law-shows-its-not-easy-to-regulate-revenge-porn/#368a490427bb> accessed 2 March 2018

Google Transparency Report '*Search removals under European privacy law'* (*Transparencyreport.google.com*, 2018) <https://transparencyreport.google.com/eu-privacy/overview> accessed 25 February 2018

H. Jeff Smith, Tamara DinevHeng Xu, *'Information Privacy Research: An Interdisciplinary Review'* Vol. 35, No. 4 Management Information Systems Research Center, University of Minnesota (2011) 989

Hauser C, *'Cyclist Lost Her Job after Raising Middle Finger at Trump's Motorcade'* (*Nytimes.com*, 2017) <https://www.nytimes.com/2017/11/06/us/middle-finger-trump.html> accessed 24 January 2018

Hern A, *'ECJ To Rule On Whether 'Right To Be Forgotten' Can Stretch Beyond EU*' (*the Guardian*, 2017) <https://www.theguardian.com/technology/2017/jul/20/ecj-ruling-google-right-to-be-forgotten-beyond-eu-france-data-removed> accessed 26 February 2018

Husovec M, *'Should We Centralize The Right To Be Forgotten Clearing House?'* (*Cyberlaw.stanford.edu*, 2014) <http://cyberlaw.stanford.edu/blog/2014/05/should-we-centralize-right-be-forgotten-clearing-house> accessed 7 February 2018

Joel R. Reidenberg, *'Resolving Conflicting International Data Privacy Rules In Cyberspace'* 52 Stanford Law Review (2000) 1315

Keller D, *'The GDPR'S Notice and Takedown Rules: Bad News For Free Expression, But Not beyond Repair'* (*Cyberlaw.stanford.edu*, 2015) <http://cyberlaw.stanford.edu/blog/2015/10/gdpr%E2%80%99s-notice-and-takedown-rules-bad-news-free-expression-not-beyond-repair> accessed 12 February 2018.

Krist A, *'Large-Scale Enforcement of the Fair Credit Reporting Act and the Role of State Attorneys General'* 115 Columbia Law Review (2015) 2311 <http://www.jstor.org/stable/43655764> accessed 20 March 2018

Kropf J, *'Google Spain SL V. Agencia Española De Protección De Datos (AEPD). Case C-131/12'* 108 The American Journal of International Law, (2014) 502 <http://www.jstor.org/stable/10.5305/amerjintelaw.108.3.0502> accessed 6 February 2018

Lee D, 'Europe Google Ruling 'Astonishing' (*BBC News*, 2014) <http://www.bbc.com/news/technology-27407017> accessed 7 February 2018

Lee J, *'SB 568: Does California's Online Eraser Button Protect the Privacy of Minors'* 48 U.C.D. Law Review (2015) 1173

Lynskey O, *The Foundations Of EU Data Protection Law* (Oxford University Press 2015)

Macgillivray A, *'Summary of Comments Received Regarding Data Portability'* (*whitehouse.gov*, 2017) <https://obamawhitehouse.archives.gov/blog/2017/01/10/summary-comments-received-regarding-data-portability> accessed 3 March 2018

Macgillivray A. and Shambaugh J., *'Exploring Data Portability'* (*whitehouse.gov*, 2016) <https://obamawhitehouse.archives.gov/blog/2016/09/30/exploring-data-portability> accessed 17 December 2017

Mayer-Schoenberger V, '*Useful Void: The Art of Forgetting in the Age of Ubiquitous Computing'* (2007) 1 SSRN Electronic Journal <http://ssrn.com/abstract=976541> accessed 23 January 2018

Mayer-Schönberger V, Delete: *The Virtue of Forgetting in the Digital Age* (Princeton University Press 2009)

Mitchell A, *'GDPR: Evolutionary or Revolutionary?'* 17 Journal of Direct, Data and Digital Marketing Practice (2016) 217

Mitrou L and M Karyda, *'EU'S Data Protection Reform and the Right to Be Forgotten - A Legal Response to a Technological Challenge?'* 5th International Conference of Information Law and Ethics 2012 (2012), Corfu-Greece, June 29-30 <https://ssrn.com/abstract=2165245> accessed 26 January 2018

'Nest Learning Thermostat - Install & Explore' (*Nest*, 2018) <https://nest.com/thermostats/nest-learning-thermostat/tech-specs/> accessed 5 March 2018

Pardo R and Lacey M, *'Undue Hardship in the Bankruptcy Courts: An Empirical Assessment of the Discharge of Educational Debt'* 74 University of Cincinnati Law Review (2005) 405 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=706761> accessed 5 March 2018

Paul M. Schwartz and Daniel J. Solove, *'Reconciling Personal Information in the United States and European Union'* Vol. 102 California Law Review (2014) 877 <http://www.jstor.org/stable/23784355> accessed 17 January 2018

Pethokoukis J, *'Washington vs. Big Tech: Should You 'Own' All Your Social Network Data? An AEIdeas Online Symposium'* (*AEIdeas*, 2017) <http://www.aei.org/publication/washington-vs-big-tech-should-you-own-all-your-social-network-data-an-aeideas-online-symposium/> accessed 10 March 2018

Post R, *'Data Privacy and Dignitary Privacy: Google Spain, The Right to Be Forgotten, And the Construction of the Public Sphere'* SSRN Electronic Journal (2017) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2953468> accessed 29 January 2018

Prosser W, 'Privacy' 48 California Law Review (1960) 383

'Review of the Midata Voluntary Programme' (*Gov.uk*, 2014) <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/327845/bis-14-941-review-of-the-midata-voluntary-programme-revision-1.pdf> accessed 2 December 2017

Rivero Á, *'Right to Be Forgotten In The European Court Of Justice Google Spain Case: The Right Balance Of Privacy Rights, Procedure, And Extraterritoriality'* European Union Law Working Paper, Stanford-Vienna Transatlantic Technology Law Forum (2017) <https://law.stanford.edu/publications/right-to-be-forgotten-in-the-european-court-of-justice-google-spain-case-the-right-balance-of-privacy-rights-procedure-and-extraterritoriality/> accessed 22 January 2017

Rosen J, *'The Right to Be Forgotten'* 64 Stanford Law Review (2012), 88 <https://review.law.stanford.edu/wp-content/uploads/sites/3/2012/02/64-SLRO-88.pdf> accessed 26 January 2018

Seamans R, *'Data Portability and Competition between Technology Platforms*' (*Forbes.com*, 2018)<https://www.forbes.com/sites/washingtonbytes/2018/03/06/data-portability-and-competition-between-technology-platforms/2/#7422db82658d> accessed 8 March 2018

Sengupta S, *'Sharing, With A Safety Net'* (*Nytimes.com*, 2013) <http://www.nytimes.com/2013/09/20/technology/bill-provides-reset-button-for-youngsters-online-posts.html> accessed 2 March 2018

Shah R. and Kesan J. P.*'Lost in Translation: Interoperability Issues for Open Standards'* I/S: Journal of Law and Policy for the Information Society (2018) 113 <http://papers.ssrn.com/abstract= 1201708> accessed 19 January 2018

Siry L, *'Forget Me, Forget Me Not: Reconciling Two Different Paradigms of the Right to Be Forgotten'* 103 Kentuky Law Journal (2014) 311

Smith J, Dinev T and Xu H *'Information Privacy Research: An Interdisciplinary Review'* Vol. 35, No. 4 Management Information Systems Research Center, University of Minnesota (2011) 989

Solomon L, *'LSD as Therapy? Write about It, Get Barred from US | The Tyee'* (*The Tyee*, 2007) <https://thetyee.ca/News/2007/04/23/Feldmar/> accessed 24 January 2018

Stempel J, *'Facebook 'Like' Deserves Free Speech Protection: U.S. Court'* (*Reuters.com* 2013) <https://www.reuters.com/article/net-us-usa-speech-facebook/facebook-like-deserves-free-speech-protection-u-s-court-idUSBRE98H0X620130918> accessed 3 March 2018

Swire P and Lagos Y, *'Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique'* (Maryland Law Review 2013) 335

The Harvard Law Review Association *'Internet Law — Protection Of Personal Data — Court Of Justice Of The European Unioncreates Presumption That Google Must Remove Links To Personal Data Upon Request. —Case C-131/12, Google Spain SL V. Agencia Española De Protección De Datos'* 128 Harvard Law Review (2014), 735 <http://www.jstor.org/stable/24644058> accessed 25 January 2018

Urquhart L, N Sailaja and D McAuley, *'Realising the Right to Data Portability for the Internet of Things'* SSRN Electronic Journal [2017] 1 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2933448> accessed 15 December 2017

Van Alsenoy B and Koekkoek M, *'Internet and Jurisdiction after Google Spain: The Extraterritorial Reach of the 'Right to Be Delisted'* 5 International Data Privacy Law (2015), 105.

Van Calster G, *'Regulating the Internet. Prescriptive and Jurisdictional Boundaries to the EU's 'Right to Be Forgotten'* SSRN Electronic Journal (2015) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2686111> accessed 2 February 2018.

Walker R, *'The Right to be Forgotten'* 64 Hastings Law Journal (2012) 257 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2017967> accessed 26 January 2018

Warren SL Brandeis, *'The Right to Privacy'* 4 Harvard Law Review (1890) 193 <http://links.jstor.org/sici?sici=0017-811X%2818901215%294%3A5%3C193%3ATRTP%3E2.0.CO%3B2-C> accessed 10 January 2018

Zingales L. and Rolnik G., *'A Way to Own Your Social-Media Data'* (*Nytimes.com*, 2017) <https://www.nytimes.com/2017/06/30/opinion/social-data-google-facebook-europe.html> accessed 3 March 2018

Zivanovic N, *'Medical Information as A Hot Commodity: The Need for Stronger Protection of Patient Health Information'* 19 Intellectual Property Law Bulletin (2015) 183

ABSTRACT

In the digital-age, many companies offer useful and greatly beneficial free online services to customers. In reality, however, these services are not 'free': in return for the services the users give their own personal data to the companies, and the latter make profit from these data. Personal information usage by the companies raises concerns over protection of personal data. Therefore, protection of personal data has been one of the key policy areas for lawmakers around the world, especially in developed countries.

In 2016, the lawmakers of the European Union has adopted General Data Protection Regulation, known with its abbreviation GDPR. The GDPR intended to provide maximum protection to the personal data of the EU residence. The GDPR provides, *inter alia*, two new rights: the right to data portability and the right to be forgotten. These two new rights give the users the power of control over their personal information. However, debates around the GDPR, especially regarding these two rights, do not have unitary discourse. While some of privacy scholars call them great advancement in the field, others raise concerns that the new rights give way to excessive over-regulation.

Nowadays, online privacy is also one of hot topics in the United States. However, legal tradition regarding the protection of personal data is much different from that of the EU. As of today, there is no comprehensive information privacy law in the United States. When it comes to information privacy, the country relies on sectoral laws which were adopted only in response to specific problems and to offer narrow protection to privacy. While the right to data portability can be found in some of the sectoral laws in the US, there is no sectoral law at the federal level that provides the right to be forgotten for online services. However, for the first time in the US, the state of California adopted SB 568: a state law that provides for the right to be forgotten.

This research is intended to discuss the characteristics of the right to be forgotten and the right to data portability in the EU and the US laws, as well as to assess the intricacies of these two rights in both legal systems.

ABSTRACT

Im digitalen Zeitalter bieten viele Unternehmen ihren Kunden praktische, vorteilhafte und kostenlose Online-Dienste an. Jedoch sind diese Dienste in der Realität oft nicht "kostenlos": Als Gegenleistung für diese erhalten die Unternehmen die Daten der Nutzer und profitieren in weiterer Folge davon. Die Verwendung der personenbezogenen Daten durch die Unternehmen ist hinsichtlich des Schutzes der personenbezogenen Daten durchaus bedenklich. Somit stellt der Schutz personenbezogener Daten einen der wichtigsten Politikbereiche für die Gesetzgeber weltweit dar, insbesondere in den Industrieländern.

Im Jahr 2016 wurde vom Europäische Parlament und vom Rat die Datenschutz-Grundverordnung kundgemacht, welche unter der Abkürzung DSGVO bekannt ist. Die DSGVO legt hohe Standards für den Umgang mit personenbezogenen Daten innerhalb der EU fest. Vor allem beinhaltet die Verordnung zwei neue Rechte: das Recht auf Datenübertragbarkeit und das Recht auf Vergessenwerden, welche den Nutzern weitgehende Kontrolle über ihre personenbezogenen Daten ermöglichen. In der Diskussion um die DSGVO spalten sich die Meinungen insbesondere hinsichtlich dieser beiden Neuerungen. Während ein Teil der Lehre im Datenschutzrecht diese als großen Fortschritt anerkennt äußern andere Bedenken, zumal das Vorliegen einer Überregulierung kritisiert wird.

Online-Datenschutz ist in den USA ein aktuelles Thema. Die Rechtstradition in Bezug auf den Schutz personenbezogener Daten unterscheidet sich jedoch stark von jener der EU. Bis heute existiert in den USA kein umfassendes Datenschutzgesetz. Im Bereich des Datenschutzes stützen sich die Rechtsanwender in den USA im Wesentlichen auf einzelne Gesetze, welche aufgrund spezifischer Anlässe verabschiedet wurden und der Privatsphäre des Einzelnen wenig Schutz zukommen lassen. Das Recht auf Datenübertragbarkeit ist in einzelnen Gesetzen in den USA geregelt, wohingegen das Recht auf Vergessenwerden für Online-Dienste auf Bundesebene nicht vorgesehen ist. Jedenfalls wurde vom Bundesstaat Kalifornien (SB 568) zum ersten Mal ein staatliches Gesetz verabschiedet, das das Recht auf Vergessenheit vorsieht.

Diese Forschungsarbeit behandelt die Merkmale des Rechtes auf Vergessenwerden und des

Rechtes auf Datenübertragbarkeit innerhalb des Rechtssystems der EU und der USA und setzt sich mit der Komplexität dieser beiden Rechte auseinander.