Assessing the Impact of the European Union's Novel Data Protection Legislation on European Transatlantic Competitiveness in the Development of Artificial Intelligence

Nick Ambrosius Akkerman

July 2, 2019

Leiden University

Master's thesis

International Relations, EUS

Thesis supervisor: Dr J.S. Oster

Nick Ambrosius Akkerman

Hoofddorpplein 8-3, 1058PD, Amsterdam

Student number 2389290

+31(0)630987969

n.a.akkerman@umail.leidenuniv.nl

MA International Relations, European Union Studies

Thesis supervisor: Dr J.S. Oster

Second reader: Dr J.Q.T. Rood

Number of pages: 50

Word count (total): 14.842

Submitted July 2, 2019

Table of Contents

List of Frequently Used Abbreviations

AI	Artificial intelligence
CCPA	California Consumer Privacy Act
DL	Deep learning
DPA	Data Protection Authority
DSM	Digital Single Market
EC	European Commission
ECJEU	Court of Justice of the European Union
EDPB	European Data Protection Board
EPR	Regulation on Privacy and Electronic Communications
EU	European Union
GDPR	General Data Protection Regulation
IoT	Internet of Things
ML	Machine-learning
OTT	Over the Top (service providers)
PII	Personally Identifiable Information
QI	Quasi-identifiers
SMEs	Small- to medium enterprises
UK	United Kingdom
US	United States

1. Introduction

Artificial Intelligence (AI) is starting to become part of our daily realities and will only increase its presence with new technological advances. In the coming years, current machine-learning (ML) models will improve tremendously depending on their access to richer datasets. Some examples of AI technologies that are being used today are: autonomous vehicles that constantly gather data to learn and identify traffic patterns; phone apps like Uber that use geodata of its users to identify the busiest spots for drivers; custom-tailored advertisements; autolearning spam filters on your email; smart home devices; and voice recognition learning from speech patterns.

AI technology today is still in a developing phase and several governments have announced to increase investments into AI research.[1] The European Union (EU) has included AI in its Digital Single Market (DSM) strategy and has announced to increase its investments in AI by 70% to €1,5 billion under the research and innovation program Horizon 2020. The EU has underlined the need to have a coordinated approach to the technological, ethical, legal and socio-economic issues it will cause (European Commission 2018).

In the United States (US), the AI landscape is diversified around strong digital eco-systems in Silicon Valley, New York, Seattle and Boston, which bring together research capabilities from leading universities, private investments and industry collaborations. Companies like Microsoft, Amazon, Facebook, Google and IBM have already transformed into the world's leading AI companies. Therefore, the US is the EU's most important competitor in the field of AI (DG Internal Policies 2018).

Historically, AI has been perceived as a futuristic, often even dystopian concept. Tech industry voices stress the beneficial opportunities of AI technology, stating that AI will serve humankind by solving our everyday problems, as well as intricate global problems (Maskey 2018). However, even in the early stages of AI, concerns have been raised regarding the massive amounts of user data that AI systems consume to become increasingly 'smarter'. The European Union has taken the forefront to ensure that there is a legal framework surrounding personal data with its General Data Protection Regulation (GDPR), which was implemented

[1] Hansen, Holger. 2018. "Germany plans 3 billion in AI investment: government paper." *Reuters*, November 13, 2018. https://www.reuters.com/article/usgermanyintelligence/germany-plans-3billion-in-ai-investment-governmentpaperidUSKCN1NI1AP

on May 25, 2018.[2] The GDPR has set a regulatory standard on data protection throughout the entire EU. It sets rules for data saving, data subject rights, consent and decision-making solely on automated processing, including profiling. With the GDPR, EU citizens enjoy a far higher level of privacy protection than citizens in other regions of the world (Hall 2018).

The GDPR entails far-stretching consequences for tech companies in Europe. These companies have to comply with higher levels of privacy norms in their home market than competitors in the US and other parts of the world, which could impede the growth and innovation of European companies in the field of AI. The development and application of AI will become crucial for the development of national economies and will become a strong competitive factor among countries. Since AI delivers its value through massive data processing by high-quality algorithms, stricter regulation on handling and processing of this data will likely inhibit the development of AI and will inevitably increase the development costs (He Li, Lu Yu & Wu He 2019, 3). If the EU's rules do not fit well with the data-driven economy, then it risks destroying the opportunities in that field, where European companies already are lagging behind the Silicon Valley giants. On the other hand, a scenario in which the rest of the world adapts to the higher European privacy standard is also imaginable, through a phenomenon known as the 'Brussels Effect'. This thesis researches which scenario will be more likely to develop.

The topic of AI has been controversial in the last two decades, due to the remarkable advances the technology has made. Recent privacy scandals, implicating companies like Cambridge Analytica and Facebook that have abused personal data to develop their business models, are make the subject extremely relevant today. For many, these privacy scandals have shown the importance of the GDPR retrospectively (DG Internal Policies 2018, 58).

This thesis aims to make a scholarly analysis of the implications and effects of the EU's privacy regulations with regards to the development of AI. Scholarly discourse on the subject is still in development since the GDPR was just recently ratified and has dramatically changed the data protection landscape of the EU. The research question is relevant because AI technologies will increasingly become a bigger part of our digital economy. Therefore, it is valuable to know

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

whether regulation in the EU impedes the competitive position of its Member States with regards to this development.

In chapter 3, the study focusses on the importance of personal data for AI. This is done by combining sources about big data processing and AI. Chapter 4 explores recent changes in the regulatory landscape regarding data privacy in the EU. Chapter 5 focusses on conflicts between the development of AI and data privacy regulation in the EU, especially with regards to the GDPR. This is done in part by analysing the GDPR on a provisional level. From here, some conclusions about the compatibility of AI and the GDPR in the EU can be drawn. Chapter 6 studies the major current developments of AI in the EU, as well as test whether criticisms of industry stakeholders on the GDPR match the findings in chapter 5. Also, the influence of *Brexit* on AI competitiveness is studied. Then, in chapter 6, the study focusses on the phenomenon of the 'Brussels effect', with examples from other sectors where the Brussels effect has been successfully demonstrated and it tests whether this could be applicable to European privacy regulation vis-à-vis the US's. Chapter 7 gives a concise overview of the major differences between privacy regulation in Europe and in the US, as well as the way in which these two jurisdictions have interacted in the past on this area. From the outcomes of these chapters, it can draw a conclusion on the research question; 'What is the impact of the EU's novel data protection legislation on European transatlantic competitiveness in the development of AI?'

2. Research Design and Sub-questions

This thesis aims to deal with the whole of the EU privacy framework that is applicable to personal data protection. It examines the question whether the provisions in the GDPR and the EPR discourage AI development in the EU and thus pose a competitive disadvantage for the EU in relation to the US, both are considered industry leaders in the field of AI research and development.[3]

Furthermore, the thesis studies the scenario of the so-called 'Brussels effect', where the EU exports its regulatory models to the rest of the world by setting international standards. This phenomenon has been studied well, also in an American context (Vogel 1997).[4] With decreasing diplomatic effectiveness and limited territorial reach, the EU found this mechanism to be particularly effective to set standards on a global level (Lavenex and Schimmelfennig, 2009). As of yet, other studies have not yet linked the Brussels effect to recent European personal data protection legislation.[5]

This thesis uses an ex-ante approach to answer the research question based on available literature on the subject. The comparative aspect of privacy law in the US and the EU is of great current interest, due to upcoming technologies, the recent application of the GDPR and the controversies surrounding privacy scandals and the EU-US Privacy Shield. The thesis contains an exploratory literature review that is qualitative in nature. It focusses on secondary sources, such as articles from peer-reviewed journals, news articles, legal texts and expert opinions. The following sub-questions correspond to the chapters in ascending order and support the conclusion of this thesis:

Chapter 3	To what extent does AI need personal data to develop and function?
Chapter 4	How has recent EU legislation changed the (personal) data regulation landscape?

[3] On par with other regions, like China and Russia.
[4] Vogel (1997) has researched a similar mechanism, only pertaining to how California exports its legal norms and standards to other states in the US, known as the "California effect". This will be discussed later in the research.
[5] To my knowledge at the time of writing.

Chapter 5 Which privacy laws could be conflicting with the development and competitiveness of AI in Europe by hindering data collection-, processing and handling?

Chapter 6 What are the developments of AI in the EU that are relevant for ascertaining the current influence of the GDPR as well as the competitive position of AI with regards to AI development?

Chapter 7 To what extent could the 'Brussels effect" give equal opportunities for the development of AI by creating the same legal privacy requirements for EU- and US companies?

Chapter 8 How does US privacy regulation differ from that of the EU and how have they interacted in the past?

Conclusion What is the impact of the EU's novel data protection legislation on European transatlantic competitiveness in the development of AI?

3. AI and How It Uses Personal Data

This chapter gives an introduction to AI and how it uses (or needs) personal data. Hence, it describes the workings of the current forms of AI through ML and deep learning (DL).

3.1 Defining AI

The Encyclopaedia Britannica defines AI as follows: "the ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings.[6] Another, wider definition of AI is the "ability to accomplish complex goals" (Tegmark 2017, 38). Forms of 'narrow AI' have been around for decades and this means AI that can perform one task at the time and can continuously improve that task through ML. For example, in 1997, the 'Deep Blue' program by IBM defeated the then reigning world chess champion, Garry Kasparov. This research, when referring to AI, means the development of AI through ML and DL. 'General' or 'symbolic' AI, meaning human-level problem-identification and problem-solving of a wide range of tasks, is not likely to be developed within the next decades, according to experts (Etzioni 2016).

3.2 Personal Data

Personal data is all data relating to an individual. Examples of most frequently occurring personal data transfers are: a name and surname; a home address; an email address such as name.surname@company.com; an Internet Protocol (IP) address; an identification card number; GPS location data; a cookie ID; and data held by a hospital or doctor, which could be a symbol that uniquely identifies a person (European Commission, n.d.)

The GDPR defines personal data as follows: "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to

[6] Encyclopaedia Britannica. n.d. "Artificial intelligence." Accessed June 4, 2019. https://www.britannica.com/technology/artificial-intelligence

the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."[7]

In principle, there are two gradations of personal data. The first one is Personally Identifiable Information (PII), which uniquely identifies an individual by their name or social service number for instance. The second kind is a Quasi-identifier (QI), like age or gender, which could be attributed to more than one individual. However, once a dataset contains a lot of these QI's, then a data controller can recombine these QI's to identify an individual (Dorschel 2019).

Before the implementation of the GDPR, in 2016, the European Court of Justice (ECJEU) had expanded the scope of what constitutes personal data in the *Breyer* case.[8] In essence, the ECJEU decided that a piece of information can be considered personal data "whenever additional information can be sought from third parties to identify a data subject" (Debussche et al., 2019). There have to be "means likely reasonable to be used to identify" the individual, so it has to be taken into account whether the data controller has the legal and practical means to identify the individual using additional data, even if this is from a third party (Niemann and Schüßler 2016). This means third-party knowledge needs to be considered to a certain, "reasonable" extent. Personal data that has been de-identified, encrypted or pseudonymised but can be used to re-identify a person remains personal data in the scope of the GDPR (European Commission, n.d.). Consequently, it is sometimes difficult to ascertain whether data can be used to identify a person, especially when taking into account the technical complexities and technological developments that can be used to link an individual to a piece of data. Accordingly, personal data that has been anonymised in an irreversible manner to such a degree that the person is no longer identifiable, is no longer considered personal data. In the context of the GDPR, the uncertainty of whether data is personal or non-personal can be precarious with regards to GDPR compliance.[9]

3.3 Machine-Learning

With ML, systems use algorithms to learn from data. ML is considered a subset of AI and can be understood as empowering a machine with the ability to 'learn' from past- or provided data

[7] Regulation (EU) 2016/679, art 4 (1).
[8] Case C-582/14: *Patrick Breyer v Bundesrepublik Deutschland* (12 May 2016).
[9] The EU's interpretation of personal data in the context of the GDPR will be discussed in more detail in section 4.4.

in order to make accurate decisions. In other words, ML is the current scientific method for building AI. Highlighting the importance of data in the world today to 'fuel' the development and functionality of AI, data has been labelled the "new oil" for the data-driven economy (DG Internal Policies 2019).

There are already a lot of uses of ML that are incorporated into our day-to-day lives, ranging from online shopping; to healthcare; to transportation; and to voice recognition on our phones. Crucial to understand is that all these applications become increasingly smarter with each use from the data that is uploaded.

A useful definition by Carnegie Mellon University professor Tom Mitchell on the process of machine learning is as follows: "A computer program is said to learn from experience E with respect to some task T and some performance measure P, if its performance on T, as measured by P, improves with experience E."[10] The experience (E) is often a result of personal data being consumed by the ML system (e.g. Google using location data from mobile phones for its 'Maps' application) and is crucial for its improvement.

For ML it remains a challenge to not use personally identifiable data. Because anonymization means that data cannot be combined to other data points, it often means that data loses its usefulness for the algorithm. ML systems that use fully anonymized data are possible, but methods to achieve this generally have sub-optimal results. For ML, ensuring anonymity usually requires sacrificing utility (Touw 2017).

3.4 Deep Learning

Deep learning (DL) is the newest innovation in the field of AI. As ML is a subset of AI, DL is a subset of ML. It can be seen as a technique to realise ML or an evolution from ML. Like the human brain, DL systems are taught to identify patterns to classify information, instead of this classification of information having to be uploaded manually, as is the case with ML.

[10] Definition by Tom Mitchell, professor of the Machine Learning department of Carnegie Mellon University (1997).

For example, a deep-learning system can learn the punctuation, grammar and style of a piece of text and can use the model it developed to automatically create entirely new text with the proper spelling, grammar and style, which it learned from the example text. A DL robot can observe human behaviour and then replicate this behaviour (Marr 2018). In other words, deep-learning systems learn by example (see figure 1.).

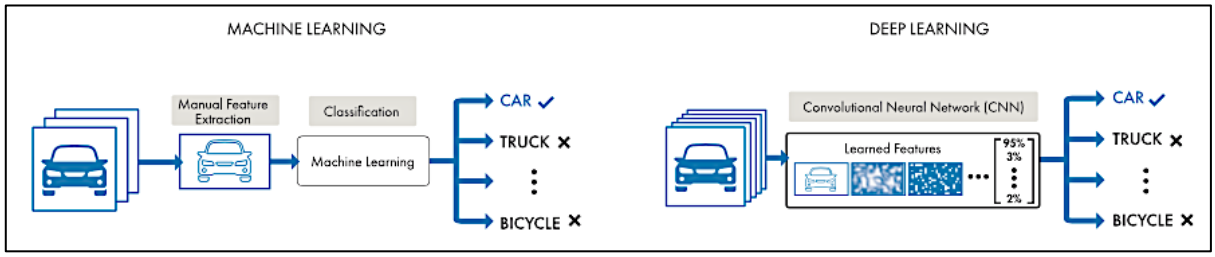

Figure 1. Comparison between ML and DL with the categorizing of a vehicle (source: Mathworks, n.d).

Just like ML, DL has to learn from data, and often personal data. DL requires large amounts of labelled data, text, images or sound. For example, driverless car development requires millions of images and thousands of hours of video. DL networks often continue to improve as the size of your data increases, as figure 1 illustrates, the more data it gets the more "features" it can distinguish while executing its algorithm (MathWorks, n.d).

3.5 De-identification of Data

The inputs that are necessary for ML systems to function often requires personal and sensitive data. This personal data is stored in a particular dataset. To protect people's privacy, machine learning systems have relied on the process of data anonymization. There are a series of techniques in use to disassociate the person in question with its dataset, in order to make sure that the person in question cannot be identified with the use of the dataset (Montjove et al. 2017, 81). Anonymization means that data is processed in a way that the data subject is permanently detached from the dataset, i.e. the data subject is no longer identifiable.

Pseudonymisation is a less thorough method of de-identification of personal data by which personally identifiable data fields are replaced with artificial identifiers or pseudonyms.
This way, personal data can no longer be attributed to a data subject without the use of additional data that could re-identify the subject. For companies, the big advantage of pseudonymization over storing directly identifiable data and full de-identification is that it

permits different records relating to the same individual to be linked (without storing direct identifiers in the data). This could be especially useful in longitudinal studies or for other processes where it is necessary to link different data that has been collected over different times to the same data subjects (Data Protection Commission 2019).

3.6 'Black Box' AI

'Black box' AI refers to an AI algorithm where humans understand the inputs and the outcomes but do not know how the algorithm arrived to that outcome. A black box algorithm, therefore, creates several problems in terms of ethics and compliance. The opposite of black box AI is 'explainable AI'. Explainable AI must have an explanation model and an explanation interface that can be accessed by the data controller and the data subject. In this way, humans could know the rationale behind a decision made by an AI algorithm, which is often desirable and relevant in the scope of privacy regulation in the EU. This is discussed further in the study.

4. GDPR & Other Privacy Legislation in the EU

This chapter summarizes the major changes that the GDPR has made to the existing privacy regulation landscape in Europe. It starts with a short history of privacy regulation in Europe and then moves on to the most substantive changes that the GDPR has brought about.

4.1 Privacy Regulation in the EU

In 1980, the Organisation for Economic Cooperation and Development issued non-binding privacy guidelines. Shortly after, the Council of Europe adopted the first, legally binding piece of privacy legislation; the Convention on Data Protection of 1981. When datafication increased in the early '90s, the EU began the negotiating process of the Data Protection Directive.[11] With this Directive, the European Commission (EC) focussed on the common market aspect of data handling, ensuring the free flow of data throughout the EU, while the European Parliament (EP) aimed to protect the fundamental right to privacy (Bendiek and Römer 2019, 36). As the ECJEU took an increasingly activist stance regarding data protection and privacy, it formulated important EU principles that would later be codified in legislative form, such as the right to be forgotten and the unlawfulness of data retention. In 2016, the ECJEU reformulated the earlier transatlantic Safe Harbour agreement (renaming it 'EU-US Privacy Shield') with the US to ensure sufficient data protection for EU citizens.[12] Later that year, the EU passed the GDPR, repealing and replacing the Data Protection Directive and leaving two-years for companies to implement the new rules before it entered into force in May 2018. The GDPR is a confirmation of the view of the EU that privacy is a fundamental right for all EU citizens (Bendiek and Römer 2019, 37).

4.2 Major changes Personal Data Collection in the GDPR

The GDPR has various rules that have implications for the handling of personal data. From the law text, different facets of data personal data collection are affected by the GDPR. This part of the thesis discusses the most impactful changes from the text of the GDPR.

[11] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data (PII) and on the free movement of such data (Data Protection Directive).
[12] Safe Harbour and Privacy Shield will be discussed in more detail in section 8.1.

4.2.1 Legitimate Interest

Following from article 6 of the text of the GDPR, the controller of the data has to have a "legitimate interest" to store or use the data.[13] This means that the controller has to have a valid reason to store the data and the data subject must have a reasonable expectation, in the time and the context of the collection, that his or her data will be stored. A reasonable expectation and processing can come from: the performance of a contract where the subject is party; for the compliance with a legal obligation; to protect the vital interests of the data subject; for the performance of a task carried out in the public interest; and when the processing is necessary for legitimate interests pursued by the controller or third party, except when those interests are overridden by fundamental rights and freedoms.[14] Reasons that are viewed as being legitimate interest are the prevention of crime and fraud, but also direct marketing purposes.
Also, the subject has the right to not be subject to a decision stemming solely from automated algorithmic processing that has a serious (legal) effect on the data subject, as article 22 states that -in some cases- there has to be human involvement in such a decision.[15]

4.2.2 Consent

To use personal data for commercial or marketing purposes, a data controller must first obtain the consent of the subject and the controller has to be able to demonstrate that consent was indeed given.[16] Also, arising from art. 6 (3), the form of the consent has to be clearly visible and distinguishable from other matters. The withdrawal of consent has to be made possible by the data controller and has the same formal criteria as the giving of the consent.[17] Lastly, the consent has to be made unconditional to the completion of the contract between subject and controller if the consent for the processing of personal data is not strictly necessary for the performance of the contract.[18] Just hours after the GDPR came into effect, companies like Facebook, WhatsApp, Instagram and Google were immediately sued by privacy advocates because their "forced consent" did not comply with the articles relating to consent in the GDPR (He Li, Lu Yu & Wu He, 2019, 3).

---

[13] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), art 6.
[14] Ibidem, art 6 (1).
[15] Ibidem, art 22.
[16] Ibidem, art 7 (2).
[17] Ibidem, art 7 (3).
[18] Ibidem, art 7 (4).

4.2.3 The Right to Be Forgotten

Per request of the subject, personal errors in the subject's data have to be corrected. With the withdrawal of consent, the subject can revoke access to their personal data and the controller has to remove it. The collector has to delete personal data in the following cases: the data subject withdraws consent and there is no legal ground for processing; the personal data is no longer necessary for the purposes for which they were collected; the data subject object to personal data used for direct marketing purposes and there is no overriding legitimate ground for processing; the personal data has been unlawfully processed; the personal data has to be erased to comply with the legal obligations of the Member State and if the personal data concerns a minor.[19] However, there are some exceptions to the subjects right to have his or her data removed. This can be the case for reasons of public health and public interest, such as scientific, historical or statistical purposes. The controller, after being notified of the request to erase the data, has to take reasonable steps to ensure that all controllers of the subject's data are informed of this fact.[20]

4.2.4 Anonymization/Pseudonymization

In paragraph 4 of chapter 2, the concept of anonymization and pseudonymization has been examined, as well as the major differences. According to the GDPR, personal data has to either be anonymized or pseudonymized. Pseudonymization is the encryption tool that the GDPR has chosen as becomes evident from the law text. Pseudonymization should give data collectors more flexibility because such data can be de-anonymized later. Pseudonymization is seen as a safeguard to protect individuals privacy and data collectors should aim to apply pseudonymization as soon as possible.[21] Crucially, the principles of data protection in the GDPR do not apply to anonymized data, as this data anonymization should render the subject no longer identifiable, and therefore it does not pose a threat to his or her privacy.[22]

Compared to the previous Data Protection Directive in the EU, the GDPR addresses de-identification in a more nuanced way (Hintze and El Emam 2017, 3). This is because the GDPR

[19] Regulation (EU) 2016/679, art 17 (1).
[20] Ibidem, art 17 (2).
[21] Ibidem, art 6 (4).
[22] Ibidem, recital 21.

recognizes different levels of de-identification, explicitly mentions the possibility of pseudonymization and gives it a different status in the GDPR, along with different requirements than fully anonymized data.

4.2.5 Sharing Externally

When a data collector has received consent to share the personal data with third parties, the data collector has to be able to revoke the access of the third party to this data. This has implications for the transfer of personal data, as companies have to manage this data and assume responsibility for it, even after it has been shared with third parties and deleted from their own database.

4.2.6 'Lex Loci Solutionis'

The 'lex loci solutionis' means the 'law of the place where the relevant performance occurs'. This implies that data processors have to follow the GDPR when European customers' data are processed (Bendiek 2019, 33). This 'extraterritorial scope' was a major innovation under the GDPR. Before, it mattered in what jurisdiction the data was being processed, but under the GDPR, this is no longer relevant. If the organization is targeting EU citizens in the collection of their data, then the GDPR applies.[23] The lex loci solutionis has major implications for the international reach of the GDPR, which are discussed in chapter 5.

4.2.7 New Supervision and Compliance Mechanism

The GDPR created a so-called 'one-stop-shop mechanism', meaning that if an organisation conducts cross-border data processing, the GDPR requires the organisation to work primarily with Data Protection Authorities (DPA's) based in the same Member State as its main establishment (usually the EU headquarters) to achieve compliance.[24] The one-stop-shop mechanism is essentially intended to ensure that organisations and individuals can deal with cross-border privacy-related issues from their home base and that these issues are interpreted uniformly across the EU (Deloitte, n.d.). In cross-border cases where several national DPA's are involved, a single decision will be adopted (European Commission, 2019).

[23] Regulation (EU) 2016/679, recital (36).
[24] Article in the GDPR about one-stop-shop mechanism: Regulation (EU) 2016/679, art 56.

Companies who fail to comply with the standards set by the GDPR can receive large fines from the DPA's. It does not matter whether the failure to comply is inadvertent or on purpose. These fines can be up to 20 million Euros or 4% of the annual turnover of the company, whichever one is higher.[25] This shows the seriousness of the EU's enforcement of the GDPR. Fines under previous EU privacy legislation were capped at around 500.000 euros (Wallace and Castro 2018, 19). The height of these penalties will surely have a deterring effect for companies that otherwise would rather not comply with the privacy norms of the GDPR.

4.3 The Regulation on the Free Flow of Non-personal Data

In 2019, the Regulation on the Free Flow of Non-personal data was implemented throughout the EU.[26] The scope of the Regulation is defined as "the storage or other processing of electronic data other than personal data in the Union which is provided as a service to users residing or having an establishment in the Union", or "carried out by a natural or legal person residing or having an establishment in the Union for its own needs".[27]

The Free Flow Regulation was created to stimulate new digital technologies and developments that use data. The EC aimed to remove barriers to the free flow of non-personal data and allow for easier cross-border sharing of this type of data to promote technological innovation (Science Europe 2019). It specifically mentions AI and ML as upcoming technologies that serve as the focal point of the Regulation. At the time of writing, where the GDPR deals with all personal data, the Free Flow Regulation deals with all data other than personal data in the EU. It aims to create a comprehensive and coherent framework for the free movement of data (European Commission, 2019).

Yet when comparing the scope of the Free Flow Regulation with the GDPR, some issues arise regarding the comprehensiveness and coherence of this data framework. Because of the far-reaching definition of personal data under the GDPR stemming from the *Breyer* principles, many types of data that at first glance seem to be non-personal data still fall within the ambit

[25] Regulation (EU) 2016/679, art 83 (5).
[26] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (Regulation on the Free Flow of Non-personal Data).
[27] Ibidem, art 2 (1).

of the GDPR's definition of personal data.[28] In the Free Flow Regulation, AI and ML are explicitly mentioned as examples where the Regulation could help with processing and transferring of data.[29] This shows the Commission's intention of the Free Flow Regulation being a catalyst for upcoming technologies. However, data could very possibly be re-identified and (re-)combined, particularly in a context of big data analytics, and thus would become personal data (Debussche et al. 2019). In this case, the majority of all data would fall under the GDPR and it would be problematic for companies to determine what kind of data would actually fall under the Free Flow Regulation and not under the GDPR.

4.4 Regulation on Privacy and Electronic Communications ("ePrivacy Regulation")

In addition to the GDPR and the Free Flow Regulation, the Regulation on Privacy and Electronic Communications, or ePrivacy Regulation (hereafter: EPR), has been proposed and was supposed to go into force at the same time as the GDPR. However, the legislation was delayed and is set to be negotiated further in the EP at the end of 2019. The EPR will complement the existing legal framework on privacy regulation. The Regulation is a so-called 'lex specialis' as it deals with a subset of the GDPR (which is a 'lex generalis'), namely confidentiality of electronic communication (Deloitte 2019). The EPR regulates all communications, and not just personal data like the GDPR. Just like the GDPR, the EPR will apply to companies outside Europe with its extra-territorial scope and carries an identical penalty regime for non-compliance.

The EPR covers metadata, which is, "data processed in an electronic communications network for the purposes of transmitting, distributing or exchanging electronic communications content; including data used to trace and identify the source and destination of a communication, data on the location of the device generated in the context of providing electronic communications services, and the date, time, duration and the type of communication as well as their content in transmission".[30] This means it will deal with e.g. cookie-tracking, traffic and location data by telecom providers and will restrict direct marketing through email and other channels. But also, it will apply to machine-to-machine communications, such as the IoT (Internet of Things).

[28] The definition of 'personal data', as has been chosen by the EU, has been described in more detail in section 3.2.
[29] Regulation (EU) 2018/1807, art 6.
[30] Proposal for a Regulation of the European Parliament and Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), art. 4 (3).

At the time of writing, the EPR is being heavily lobbied against by industry stakeholders. The main reason for this is that the EPR will apply to all 'over the top' (OTT) service providers. These are providers that offer communication services via the internet that are "functionally equivalent" to traditional providers (i.e. telephone providers).[31] In essence, the Regulation will cover any website or app that involves a communication component. In these cases, consent has to be given by the user for access to the emails and instant messaging, but also for "any form of advertising, whether written or oral, sent to one or more identified or identifiable end-users of electronic communications services, including the use of automated calling and communication systems with or without human interaction, electronic mail, SMS, etc."[32] Chapter 5 elaborates on the consequences of the EPR in its current form for AI.

[31] Regulation on Privacy and Electronic Communications (proposal), section 1.3.
[32] Regulation (EU) 2016/679, art. 4 (3).

5. Conflicts Between Privacy Regulation and AI in the EU

This chapter analyses possible conflicts between AI and the privacy standards from the GDPR and the EPR, which may slow down or thwart the development of AI technologies in the EU. It describes the rights stemming from the GDPR and argues the negative consequences this could have for the investment in- and development of- AI in the EU.

5.1 Purpose Limitation

Article 6 of the GDPR provides the legal bases for the processing of personal data. For most commercial uses, where data processing is granted through consent or a contract with the data subject, the data controller cannot use the data for other purposes than the purpose that has been consented by or stipulated in the contract (Wallace and Castro 2018, 14). In this case, consent has to be asked or a new contract has to be offered to the data subject. Another option would be to irreversibly anonymize the data.

According to article 6 of the GDPR, reusing data is permissible when the new purposes are interrelated to the old purpose where the consent was given. To determine this, the consequences for the data subject have to be considered and there have to be safeguards, such as pseudonymization. This restricts a data controller from adding new functionality to an AI system with existing data. The repurposing of data means that data controllers have to ask for explicit permission every time a new use for the data is found. This will make it harder to test and innovate with new AI projects and limit their overall potential (Wallace and Castro 2018, 14-15).

The impact of the purpose limitation for ML is not to be underestimated. Individuals will need to give specific permission to allow their data being used for ML, as this data needs to be collected over time and involves large datasets (big data) in order to 'teach' the machines, which goes directly against the GDPR's requirements of not processing personal data for longer than is necessary for the purpose at hand (Cullinan 2018).

5.2 Right to Erasure

The right to erasure (or 'right to be forgotten') as follows from article 17 of the GDPR, means that data subjects have the right "to obtain from the controller the erasure of personal data concerning him or her without undue delay".[33] Some ML systems use existing data to improve themselves by generating new rules for processing future data. If the data on which these rules is based is removed, the effectiveness of the algorithm could be affected negatively or even break completely. The right to erasure also implies that data controllers have to manage all the data that has been added to the algorithm. This will significantly increase labour costs for AI companies. The exceptions to the right to erasure (as have been discussed in the previous chapter) do not apply to most commercial uses of AI, so data subjects can withdraw their consent and demand erasure at any time (Wallace and Castro 2018, 10-11).

If the right to erasure is exercised by the people who share similar characteristics which are crucially important for the performance of an algorithm, then that algorithm becomes less reliable. According to a study by (Malle et al, 2016), real-life scenarios where people that want their data removed that share commonalities are easily conceivable and will undermine important rules in the algorithm and impair its effectiveness for other users. For example, when a credit agency has developed an AI algorithm that decides whether a person is low- or high-risk for a loan, people who have a high-risk profile will be more likely to demand erasure of data to boost their chances of being accepted for future loans.[34] With the withdrawal of the data profiles of these high-risk individuals, the algorithm becomes less adept at judging whether a new applicant for a loan is high- or low-risk since data points containing high-risk profiles on which the algorithm bases its rules have been erased. Companies using these algorithms will be dissuaded from investing AI when the right to erasure negatively affects the reliability of its outcomes (Wallace and Castro 2018, 12).

Lastly, it is extremely difficult to determine at what point it is safe to delete data within an algorithm without changing or even breaking the system. As article 17 states that data has to be deleted without "undue delay", this task will become troublesome for data controllers in charge of the deletion of personal data. Many organizations are already finding the implementation of the right to be forgotten to be one of the most onerous, legal, technical and

[33] Regulation (EU) 2016/679, art 17.
[34] See section 5.5 on "Invoking Rights Under the GDPR".

operational challenges in their efforts to comply with the GDPR, as the locating of all personal data requires detailed data mapping efforts (Hintze and El-Emam 2017, 5).

5.3 Right to Human Review

Pursuant to article 22 of the GDPR, companies have to manually review algorithmic decisions as it confers a right to individuals "to not be subject to a decision based solely on automated processing".[35] This automated processing (or decision-making) is the essence of AI algorithms. It means that these technologies cannot solely produce any legal effect or something that is similarly impacting for a consumer. Examples could be in the cases of a denial of a mortgage application, a rejected job application or the liability for a car accident. There has to be a human review to evaluate the bases on which these decisions have been taken by the AI system. Consequently, the right to human review (or right to explanation) will make the use of ML black boxes against the law, because with these systems, there is no possibility of human control on the algorithms and there is only insight to the actual conclusion of the system's calculation. So, inherently, black boxes would never be in compliance with the GDPR's right to human review.[36]

The level of transparency that is necessary for the right to explanation requires explainable AI; EU citizens and data controllers have to be able to learn why exactly a decision was taken by an AI algorithm. An important reason that the EU has chosen to add this right to the GDPR is to avert discrimination and bias in AI technologies. For example, an AI algorithm decides whether an applicant is eligible for a mortgage and the applicant has a low level of education. The AI algorithm could decide that because of his low level of education, the chances of defaulting on the mortgage are higher since the default-rate is generally higher in this group. Thus, it could make generalist decisions pertaining to an individual case. Critics have objected that there is already a bias with human decision-making and that human bias is worse than algorithmic bias because human bias is often not fact-based.

Still, the right to human review in the GDPR is ambiguous. This is because there are two ways in which the right to human review could be interpreted. One explanation is the functional explanation (about the system), which shows insight into the AI algorithm. A data subject,

[35] Regulation (EU) 2016/679, art 22.
[36] Ibidem, Recital 20.

when invoking its right to explanation, would get a technical answer as to why a certain decision affecting the data subject is made. The second, deeper interpretation is the 'rationale explanation', where the factors that lead to a decision are identifiable and relatively easy to ascertain (Wachter et al 2017, 76). The GDPR does not specifically identify to what extent the right to human review applies (to the system functionality or the rationale behind the decision). In Recital 13-15, it refers to the right to "meaningful information about the logic involved" in automated decisions. Granted, the word "meaningful" points more to the rationale explanation, but Recitals are not legally binding and there is no statutory provision labelled the "right to explanation" in the GDPR. This may raise questions over the protection actually afforded to data subjects and the limitations that the right to explanation pose to AI companies. Most likely, jurisprudence and further legislation will decide in the future what the right to review really entails and define the consequences for AI companies and EU citizens.

The right to human review will, in any case, require companies to employ people that have the competence to review decisions made by AI algorithms and the power to change such a decision. This will incur significant costs to these companies and perhaps even discourage them from using AI technology altogether. The EC, therefore, has put its trust in the development of explainable AI, with an interface that could explain the factors and give meaningful information regarding its decisions. However, explaining a complex algorithmic decision would most likely lead to a trade-off between the representational capacity of the algorithm and the ease with which a human controller can access and understand the data. This is also known as 'the performance vs. explainability dilemma' (Wallace and Castro 2018, 9). The result will be either that algorithms will become less complex so that human controllers can understand them, or companies will decide against the use of AI altogether because of the costs involved.

5.4 De-identification and Compliance

Fully anonymized data is not considered personal data anymore, so when data is irreversibly anonymized, it is no longer privacy sensitive information and not included in the scope of the GDPR.[37] Nonetheless, pseudonymized data is still subject to various provisions in the GDPR. This is because many methods of pseudonymization are readily reversible by a data controller

[37] Regulation (EU) 2016/679, Recital 26.

or the data can be matched with other data that can potentially identify the person. In these cases, the pseudonymization does not meet the standard of article 12 (2) GDPR. There are methods of 'strong' pseudonymization that could meet those standards and companies would need to demonstrate that their form of pseudonymization meets the standard (Hintze and El Emam 2017, 6). The difficulty here lies in at what point pseudonymization is classified as being 'strong', especially when re-identification techniques are improving as well with the development of AI.

GDPR Obligation	Identified	Pseudonymized	Anonymized
1. Provide notice to data subject	Required	Required	Not Required
2. Obtain consent or have another legal basis	Required	Potentially helps	Not Required
3. Give right to erasure / right to be forgotten	Required	Depends on strength	Not Required
4. Other data subject rights (access, portability…)	Required	Depends on strength	Not Required
5. Basis for cross-border transfers	Required	Required	Not Required
6. Data protection by design	Required	Partially met	Not Required
7. Data security	Required	Partially met	Not Required
8. Data breach notification	Likely	Less likely	Not Required
9. Data retention limitations	Required	Required	Not Required
10. Documentation / recordkeeping obligations	Required	Required	Not Required
11. Vendor / sub-processor management	Required	Required	Not Required

Figure 2. GDPR obligations under different stages of de-identification (source: IAPP White Paper 2017).

According to critics, there is a lack of clarity about when de-identified data is in compliance with the GDPR. It is difficult to ascertain whether pseudonymization is strong enough that re-identification is no longer possible. Furthermore, if data is pseudonymized, it is complex (and in some case subjective) which obligations under the GDPR have to be met (see figure 2). A combination of these legal complexities of the GDPR and the mistrust of companies in de-identification methods may lead to companies not taking advantage of the exemptions that the GDPR gives to pseudonymized data. This is because of the potential legal troubles these companies face if the data is not converted properly in compliance with the GDPR. These companies would therefore miss the advantages that pseudonymized data could offer over fully anonymized data for developing AI. Many firms could decide not to take the risk to invest in

AI because of the possibility of inadvertent non-compliance with the complex rules of the GDPR and the high fines that could follow. Especially SMEs will be deterred by the high fines, which are at least 20 million euros (Wallace and Castro 2018, 18).

5.5 Invoking Rights Under the GDPR

The impact of several of these rights under the GDPR for companies that use AI is dependent on the degree to which EU citizens will use these rights and impose their rights onto these companies; the right to review and the right to erasure being two of those rights.

Individuals have the right to contact a company to exercise their rights under the GDPR (rights of access, rectification, erasure, portability, etc.). Any request has to be met, in principle, within a month by the organisation. If a request is denied by an organisation, the organisation has to motivate their decisions and the individual has the right to lodge a complaint with the DPA and seek a judicial remedy. In principle, these requests have to be performed free of charge.[38] Furthermore, the GDPR has specific provisions included for affected individuals of infringement of the GDPR through group litigation for example.

On February 26, 2019, the European Data Protection Board (EDPB), the agency responsible for implementing and monitoring GDPR compliance along with the national DPA's, released a first overview of the GDPR's implementation and the number of cases that were brought to the EDPB by the national DPA's. The total number of cases reported was 203.326. Most of these cases were related to complaints (94.622), others were initiated on the basis of a data breach (64.684), the rest of the cases had to do with various other infringements of the GDPR.[39]

As of May 25th, 2019, one year after the implementation of the GDPR, Eurobarometer (2019) has done a study interviewing 27,524 respondents about their rights under the GDPR. Figure 3 shows the results of this study.

[38] See: European Commission. n.d. "How should requests from individuals exercising their data protection rights be dealt with?" Accessed June 18, 2019. https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/dealing-citizens/how-should-requests-individuals-exercising-their-data-protection-rights-be-dealt_en.

[39] For full report: European Data Protection Board. 2019. "First overview on the implementation of the GDPR and the roles and means of the national supervisory authorities." Accessed June 19, 2019. http://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2019/02-25/9_EDPB_report_EN.pdf

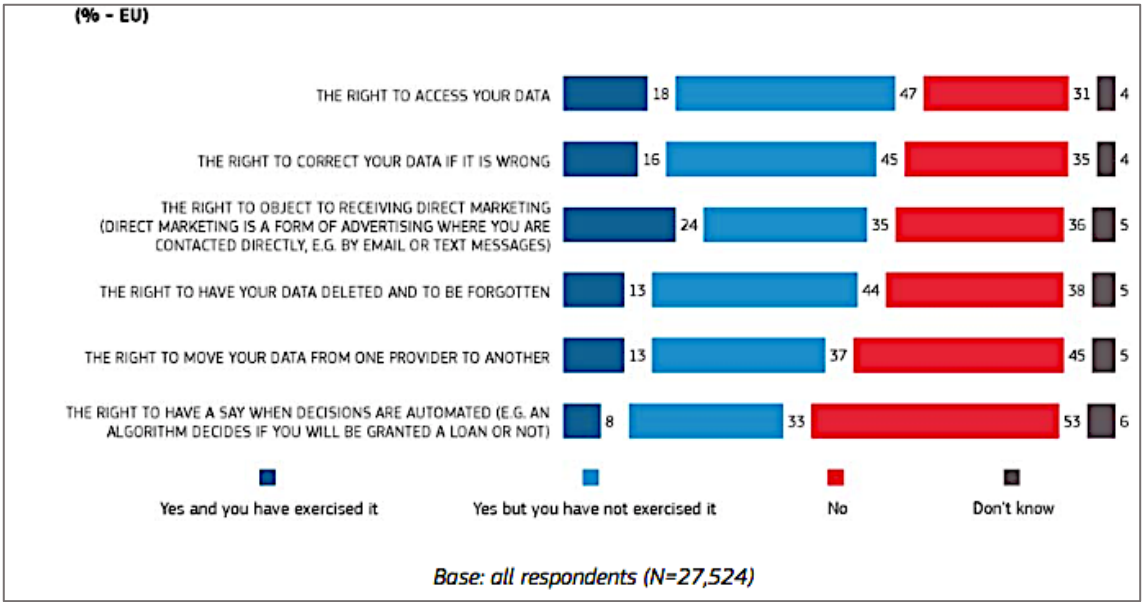

Figure 3. Survey among European Citizens about GDPR rights. Question: "Have you heard of each of the following rights?" (source: Eurobarometer 2019).

From the Eurobarometer study, between 8% and 24% of respondents have exercised their rights from the GDPR by making requests to data controlling organizations. The right to erasure and the right to portability have been exercised by 13% of the respondents, which are far-stretching and labour-intensive rights to comply with by companies. Since the GDPR at the time of writing has only been in place since little over a year, it is likely that these percentages will only increase due to technological advances involving personal data and more general awareness of the rights under the GDPR. This will result in high costs of compliance for tech companies that deal with European personal data. Many Chinese and American companies are also obligated to comply with the GDPR, but EU companies will be the most affected since they mostly deal with personal data of their own, EU residents (He Li, Lu Yu & Wu He 2019, 4).

5.6 EPR and AI

Where the GDPR leaves legal space for legitimate business interest, the only legal basis that the EPR provides to process data will be by the consent of the end-user (with only a few exceptions where data processing is justified through the scope of transmissions or audience measurements by the provider). This would decrease the amounts of data that tech companies will be able to use without permission and therefore slow down development in data-based technologies.

Furthermore, the EPR forbids companies to withdraw the provision of (free) services to users who do not give their consent for third-party cookies. If a person does not consent to third-party cookies, then a company still has to offer its services to that individual.[40] This will pose a difficult scenario for companies using AI, that base their business model on advertising as their biggest revenue stream in order to offer a service, companies like Facebook, Instagram and Google.

Under the EPR, the web browser application (e.g. Google Chrome, Safari, Mozilla Firefox) are responsible for setting the preference for cookies.[41] Browsers will therefore be given a lot of control and power by the EPR. Being that this market is dominated by companies from the US, European internet companies will be at a major competitive disadvantage (Bielieauskaite 2018).

Apart from dealing with new forms of electronic communications that were not covered before, the EPR also applies to forms of ML. In many cases, for every kind of information that an ML system needs, there has to be explicit consent from the user. If we take the example of an autonomous car, then the user will have to give consent to: share the individual status on route; the car's speed; (un)fastened seat bells; road conditions; etcetera... Then, if other passengers enter the car, each of them has to give individual consent too (Bielieauskaite 2018). This would result in a situation where any individual is given the option to consent on an abundance of different day-to-day applications involving their personal data and could result in 'opt-in fatigue' of the EU citizen, causing them not to grant consent for a lot of these technologies.

Opposing tech companies have stated in the media that the EPR will result in communication services being, "too rigid, disproportionately cumbersome, extremely burdensome and not user-friendly" (Kayali 2019). Especially for SMEs working with data, it will become harder to innovate with the EPR since it will make the collection of data more difficult by demanding consent for almost all data. Big, multinational enterprises could easier test and develop their AI technologies by collecting data from users outside of the EU. If this consent is not given, then ML technologies will not develop properly and especially SMEs will be hurt.

[40] Regulation on Privacy and Electronic Communications (proposal), (22)
[41] Ibidem, (22).

On the other hand, since the EPR is still being debated on a European level and has been delayed, mostly due to fierce resistance from the industry stakeholder, the chances of it being implemented in its current form are slim. It is also not entirely consistent with the GDPR because of its strong emphasis on consent, voiding other legal bases for data processing from the GDPR.

6. Current Developments of AI in Europe

This chapter presents an outline of the current developments of AI in Europe. Furthermore, it surveys whether industry leaders in the EU in the field of AI are opposed to the GDPR and how they view the future of AI in Europe.

6.1 Development of AI in the EU

In recent years, the EU voiced concerns that Europe is losing ground to the US and China in the development of AI. That is why the European Council asked the EC in 2017 to develop a European approach to AI. In 2018, the EC issued a report, "Artificial Intelligence for Europe", where this common approach was mapped out. This report contained three pillars to try to reach this goal: 1) being ahead of technological developments and encouraging uptake by the public and private sectors; 2) preparing for socio-economic changes brought about by AI; and 3) ensuring an appropriate ethical and legal framework. (DG Internal Policies 2018, 6).

The common perception is that the EU is far behind in the development of AI. Per contra, Europe ranks second in AI start-ups and there are multiple examples of solidified, fast-growing European AI companies. The problem is that individual Member States have little weigh in the international arena and there is a large geographical divide in the cities that have a considerable number of AI start-ups, as most come from London, Paris and Berlin (DG Internal Policies 2018, 15).

On the EU-level, the program for AI development has been launched under the Horizon 2020 program, allocating 1.5 billion Euros to AI. With the Public Private Partnership on Big Data and Robotics, another 2.5 billion has been raised. The EU recognizes that AI can cause "far-reaching effects in several sectors and cause disruptive changes in value chains and business models" (DG Internal Policies 2018, 5).

In Europe, there are a number of significant drivers that could be crucial in the development of Aim, such as a highly educated labour force and exceptional research institutions. Despite this, the EU has not been successful in the development of globally scalable AI-related business models and, as a result, is too reliant upon foreign AI technologies (DG Internal Policies 2018, 6).

According to a survey by International Data Cooperation (IDC) (see figure 4), there is a great interest among European firms to utilize AI, but only 20.6% of all firms had actually used a form of AI in their business mid-2018.

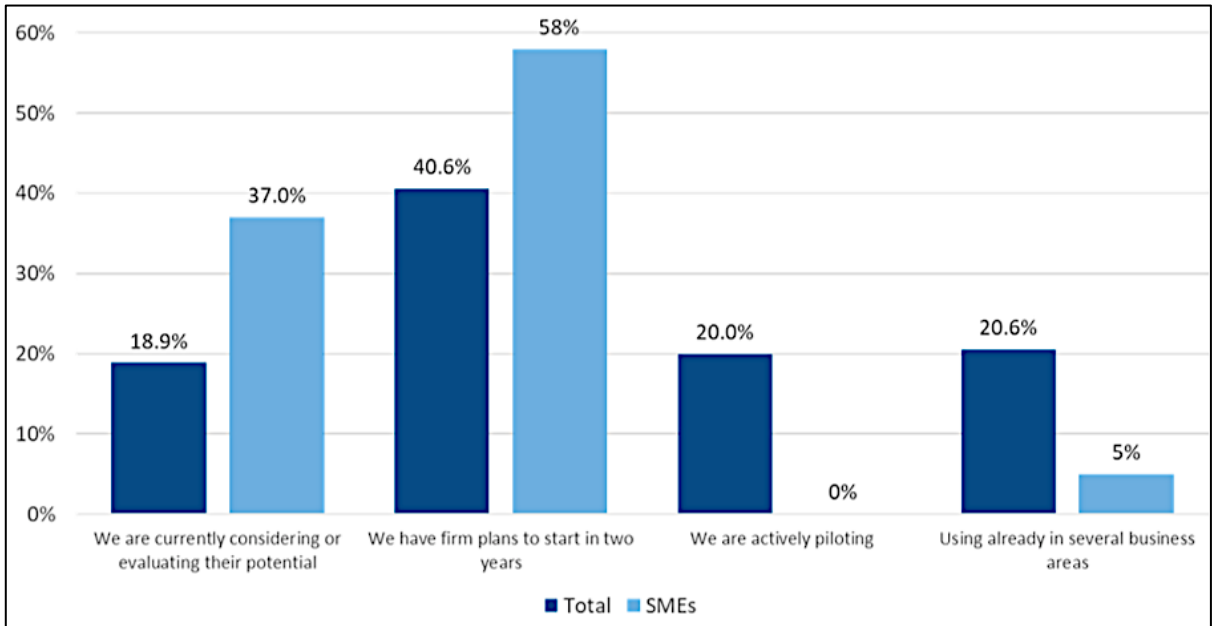

Figure 4. Use of AI solutions or services in Europe (source: IDC's Western Europe AI/Cognitive Solutions Survey, June 2018).

6.2 Critics of GDPR from EU Industry

There are several theoretical and practical barriers that hinder the development of AI in the EU. Figure 5 shows some of these barriers from the viewpoint of companies in Europe working with AI today. Apart from reasons that are inherent to the development of an upcoming and rather contentious upcoming technology like AI (such as perceived immaturity and lack of trust in its potential), 50% of companies deem data compliance a key barrier to using AI, and around 47% lack the necessary skill to manage AI, which also has partly to do with the training of compliance officers and knowledgeable staff to manage the compliance aspect of e.g. ML algorithms. This shows that compliance (with the GDPR) is viewed as a key obstacle to European companies in the development of AI.

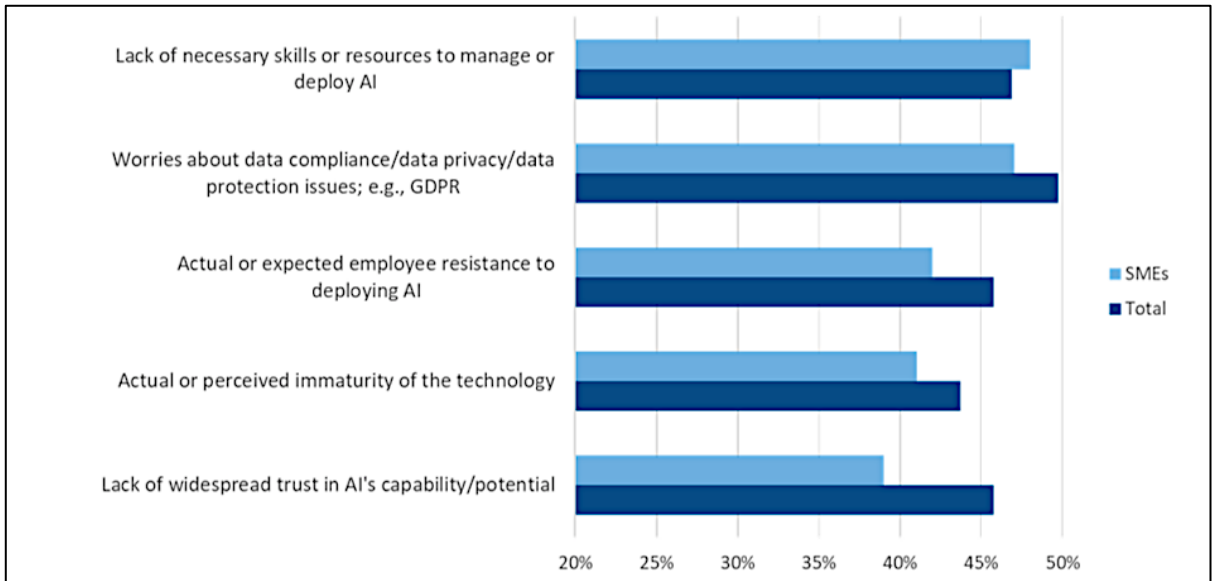

Figure 5. Key barriers inhibiting faster deployment of AI systems in Europe, total vs SME's (source: IDC's Western Europe AI/Cognitive Solutions Survey, June 2018).

6.3 Impact of *Brexit*

The recent move of the UK to leave the EU, commonly known as *Brexit*, could potentially harm the competitiveness of the EU as a whole in the field of AI. The EU asserts itself as a leading AI entity, but the UK dominates the region in research and development. Presumably, the UK will develop its own data privacy laws to complement the development of AI, which has been a top priority for the UK. The UK plans to balance consumer interests with AI interest to seize the competitive advantage (Humerick 2018, 399). It is unclear in what form *Brexit* will continue and therefore it is hard to assess the impact of *Brexit* on AI development in the EU. What is clear, however, is that where the EU could have used the UK's dominance in the field to consolidate AI projects in the EU, it now has to face another competitor in AI development.

7. The 'Brussels Effect'

This chapter puts forth the theory of the 'Brussels effect' and the theoretical conditions that enable the Brussels effect from taking place with a certain regulatory target. Hereafter, it assesses the Brussels effect as related to the effect of the GDPR on privacy regulation in the US.

7.1 Conditions for the Brussels Effect

The Brussels effect refers to the regulating power of the EU and its impact on the regulatory systems worldwide. This has been referred to as the process of "unilateral regulatory globalization". The theoretical foundation of the Brussels effect "identifies the conditions for and the mechanism through which the externalization or export of the EU regulatory system prevails" (Bradford 2012, 9). The Brussels effect is derived from the 'California effect', a term introduced by Vogel (1997), to describe the way in which California exports its legal norms to the rest of the US in a similar fashion as the Brussels effect. This chapter will discuss the conditions for the Brussels effect and is based on studies by Anu Bradford (2012).

7.1.1 Market Power

One of the conditions that make this export of the regulatory system more likely is the market size of the EU. The EU is the largest economy in the world by Gross Domestic Product (GDP) with a GDP per head of €5,000 and 500 million consumers.[42] For other trading blocs, it becomes in their best interest to convert to the European norms and regulations in order to sell their products on the EU market and gives multinationals an incentive to standardize their production globally and adhere to a single rule, which converts the EU rule into a global rule. This is the Brussels effect (Bradford 2012, 5). According to experts, the Brussels effect is only gaining more prominence across the world over time.[43]

[42] According to the European Commission, see: European Commission. 2019. "EU position in world trade". Accessed June 11, 2019. http://ec.europa.eu/trade/policy/eu-position-in-world-trade/
[43] See for instance: Beatle, Alan. 2017. "Why the Whole World Feels the 'Brussels Effect'." *Financial Times* November 16, 2017. https://www.ft.com/content/7059dbf8-a82a-11e7-ab66-21cc87a2edde

7.1.2 Regulatory Capacity

Market power is not the only factor that enables the EU to impose their norms and regulations on world trade. Regulatory capacity is another factor because not all states with great market power become sources of global standards (Bradford 2012, 12). First off, becoming a regulatory power is a conscious choice pursued by a state. Then, after a state makes this choice, there has to be an institutional and regulatory capacity that is capable of setting sanctions in case of non-compliance (Bradford 2012, 13).

7.1.3 Preference for Strict Rules

Furthermore, there has to be a preference for strict rules. This preference for strict rules is more likely to be found in countries with high income (Bradford 2012, 14). In the EU, this is bolstered by their general sense of risk aversion within their regulation and legislation. The EU has implemented the precautionary principle, which on the onset deems new products unsafe unless proven otherwise. This has the effect of setting a high regulatory bar to the acceptance of new technologies (Beatle 2017). The preference for strict rules ensures that countries (i.e. companies) opt for the higher standard so that they only have to implement one compliance mechanism. This trend of the EU showing risk-averse behaviour has been present in the last decades. This in contrast with the US, that has shown increasingly risk-taking behaviour. The EU tended to adopt the policies of the most risk-averse Members States (Ujj 2016, 87).

7.1.4 Regulating Inelastic Targets

The imposing of global standards to regulate is only possible when other countries cannot circumvent the regulation by moving the targets of the regulation to another jurisdiction. In other words, a 'race to the bottom' where producers seek more lenient regulations in other countries. The EU avoids this by targeting inelastic regulation targets -i.e. the consumer markets- in the areas of product and food safety and privacy. If the EU chose to regulate corporate tax levels and these regulations would have been too strict, companies would flee the EU's jurisdiction. Yet, because the consumers stay in the EU and cannot be moved to an area with a more lenient jurisdiction, producers are forced to comply with EU norms (Bradford 2012, 17).

7.1.5 Nondivisibility of Standards

The section above on regulating inelastic targets means that producers abroad will comply with the EU norms but does not mean yet that the Brussels effect will happen since it does not imply that the producer will export these norms to its home market or to the rest of the world. This only happens when the production or the conduct is nondivisible across different markets or when the benefit of having one standard exceeds the benefit of lower production cost due to economies of scale (Bradford 2012, 17). A single production process or a single standard of the brand can be advantageous in certain markets. There are three primary types of nondivisibility: legal-, economical- and technical nondivisibility.

Legal nondivisibility becomes apparent in global mergers where the most stringent jurisdiction concerning anti-trust law determines the fate of the transaction worldwide. The most famous example of legal nondivisibility blocking the 42-billion-dollar acquisition of Honeywell International by General Electric. The EU blocked this transaction on the basis of European anti-trust laws, whilst the American authorities had already cleared the merger. Because of the legal nondivisibility, it was impossible to allow the merger in one market and disallow it in the other. On that basis, the merger did not go through (Grant 2005, 595).

Economical nondivisibility relates to producers who find it economically disadvantageous to develop different products for markets with different norms and therefore conform their production to the highest standard in order to market one single product. A single production process creates economies of scale and therefore the EU often is able to dictate the global product standards indirectly.

Technical nondivisibility is the difficulty with which computer systems can be partitioned across different markets. Technical nondivisibility is often related to the regulation of privacy laws. For technical reasons, companies handling in big data are often not able to isolate (personal) data from EU countries with the other data and are therefore forced to comply to the most demanding (EU) standard (Bradford 2012, 18). The Brussels effect is already showing in this area after the arrival of the GDPR, as it has spurred changes in data collection and handling practices in tech companies in the United States. Companies like Facebook and Google have made several changes in 2018 in response to the GDPR, as the technical nondivisibility of their systems has made it easier for these companies to adapt to the standards stemming from the

GDPR than to create separate systems. Major US data-brokering company Acxiom is revisiting its online portals where consumers can look into the data that Acxiom has about them and has stated on several media outlets that the GDPR will "set the tone for data protection in the next decade worldwide".[44]

7.2 Brussels Effect on Privacy Regulation in the US (and Beyond)

The technical nondivisibility of standards is a major argument in favour of the view that the GDPR will result in a global privacy standard through the Brussels effect, and thus will provide a 'level playing field' for companies worldwide that are developing AI. With the GDPR, all conditions that have been laid out by Bradford (2018) for the Brussels effect to happen are met. The EU has a consumer market with enough market power to serve as a market for technologies that require personal data processing; the EU has the regulatory capacity through its powerful legal institutions; the GDPR imposes privacy norms that are (generally) stricter than existing norms in other jurisdictions; the focus of the GDPR is on the consumer market and there is a technical nondivisibility in cross-border data-processing systems. The latter is exemplified by multinational corporations that have adjusted their global data handling to reduce compliance costs because data is always free-flowing between borders and very difficult to contain in one jurisdiction. Therefore, these companies have often adopted a single privacy policy modelled after the European one (Bradford 2012, 25-26).

Moreover, European privacy regulation has in the past often spilled over to other jurisdictions in the world. Since the EU's Data Protection Directive of 1998, over 30 countries have adopted the EU standard resulting from this Directive. The US have tried to resist the EU's lead on data protection, but US companies have been affected and have often changed their business practice, also because of pressures of multiple intercontinental lawsuits from EU countries (Bradford 2012, 23).

The GDPR has already influenced data protection legislation outside of Europe. Since the GDPR in principle bans the export of data to third party countries who do not provide an adequate privacy protection level (adequate being up to the standards set by the EU) and has an extraterritorial reach, the consequences of the GDPR for other jurisdiction will be even

[44] See Tiku, Nitasha. 2018. "Europe's New Privacy Law Will Change the Web and More." *Wired*, accessed June 11, 2019. https://www.wired.com/story/europes-new-privacy-law-will-change-the-web-and-more/

greater than past privacy regulations. In 2019, French watchdog Commission Nationale de l'Informatique et des Libertés (CNIL) fined American tech giant Google £44 million for failure to obtain user consent from its European users for the purpose of personalised advertising (Vinocur 2019). This has shown to the world the gravity of the GDPR's extraterritorial scope with its large fines. It also reflects the fact that foreign companies' business activities with the EU will be heavily influenced by GDPR (He Li, Lu Yu & Wu He 2019, 3).

8. Transatlantic Interactions on Privacy Regulation

The question that follows from the previous chapters is; will the GDPR have the effect of levelling the playing field for worldwide development of AI by harmonising norms of data protection, or will the US find that the advantages of a quicker development of AI outweigh the requirement to convert to the EU norms of privacy through the discussed mechanisms of the Brussels effect? In order to assess this, privacy regulation in the US and its ties to the EU in this field is analysed.

8.1 Privacy Regulation in the US

The progression of modern privacy law in the US has taken a very different path than that of the EU. It is not that the right to privacy was not deemed important in the US. On the contrary, in some sectors the US had very strict privacy laws relating to data. Although, any data that was not covered by those sectoral laws was unprotected (Heisenberg 2005, 2). This is because there are no comprehensive, all-encompassing privacy laws in the US (the last one being the Privacy Act of 1974). For the most part, the US have traditionally relied on sectoral (such as FERPA) and state laws, industry self-regulation and privacy-enhancing technologies such as encryption. Often, these legal models are used in a reactive fashion, after a problem emerges.

In contrast with the EU, privacy is being viewed in the US as a commodity rather than a fundamental right. This becomes obvious when, in the US conflicts arise over who owns the personal data obtained from internet sources (Hall 2018, 37). The transatlantic differences become especially noticeable in the way that the opt-in system works in the US. The default is the opt-out (businesses may use the personal data unless explicitly told not to), where European privacy laws have chosen consent, or opt-in, as the desirable method for companies to use personal data (Heisenberg 2005, 2).

Privacy regulation in the US in the last two decades has also been influenced by the aftermath of the terrorist attacks on the World Trade Centre in 2001. As a direct result of these attacks, for example, the US passed a law that mandated that the identities of all plane passengers be placed in a database of the Department of Homeland Security, the Passenger Name Record (PNR). Not surprisingly, this sparked another privacy-related, transatlantic conflict

(Heisenberg 2005, 2). Also, the surveillance capabilities of intelligence agencies were increased with privacy-intruding legislation like the 'Patriot Act'.

8.2 Safe Harbour Agreement

The Safe Harbour agreement of 1998 was in first instance seen as a victory for US companies since it allowed for a lot of room for US companies to 'self-certify' to be able to meet the Safe Harbour principles that allowed them to store and process data of European citizens. But complying with the Safe Harbour framework could be expensive for companies. They had to set up systems that notified the data subject about the usage of their data and offer opt-out mechanisms. That is why companies such as Amazon and Yahoo decided to establish websites that had their data separated from Europe and the US (Hall 2018, 140).

By agreeing with Safe Harbour, the aim of the US was to establish a norm of self-regulation with regards to privacy legislation and create a flood of companies that would sign up for the Safe Harbour-status. It did not, however, and the EU was able to export its privacy standards to most other countries around the world. Even some states in the US have taken over some norms and standards that resemble the EU-model. The agreement can be seen as "a costly ceasefire during which most other countries (as well as some US states) allied with the Europeans (Heisenberg 2005, 2). Safe Harbour was invalidated by the ECJEU on October 2015, after Edward Snowden revealed the espionage conducted by the U.S. government.[45]

8.3 EU-US Privacy Shield

In addition, the EU has been finalizing trade agreements recently that have GDPR principles enshrined in them (Bendiek and Römer 2019, 33). Safe Harbour's successor, the 'EU-US Privacy Shield' was created in 2016. The Privacy Shield contains seven legal principles being: notice; choice; accountability for onwards transfer; data integrity and purpose limitation; access and recourse, enforcement and liability.[46] With the enforcement of these principles by the US (with regards to personal data from EU citizens as well as from the American citizens),

[45] See: Klint, Finley. 2015. "Thank (Or Blame) Snowden for Europe's Big Privacy Ruling." Accessed June 28, 2019. https://www.wired.com/2015/10/tech-companies-can-blame-snowden- data-privacy-decision/
[46] For further explanation of these principles, see Impact Advisors. 2019. "7 Principles of the EU-U.S. Privacy Shield Framework." Accessed June 13, 2019. https://www.impact-advisors.com/security/eu-us-privacy-shield-framework/

the US is qualified as having adequate privacy laws in the scope of the GDPR. With regards to Safe Harbour, several technical requirements have become more stringent. However, the Privacy Shield principles are not as far-reaching for the US as some of the GDPR principles are for EU countries, in particular principles such as the right to review and the right to erasure.

Shortly after his inauguration in 2017, US President Donald Trump signed an executive order regarding immigration law that also included a provision on privacy; "Agencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information."[47] It was debated on European level whether this section of the order negated Privacy Shield. Legal analysts concluded that Privacy Shield was still viable, in spite of the executive order (Hall 2018, 156). Then, on 5 July 2018, the EP submitted a resolution suspending the Privacy Shield, as it does not effectively procure adequate personal data protection for EU citizens according to the EP (Loyens & Loeff 2018). After the scandal surrounding Cambridge Analytica, that had been signed up to self-certify its 'compliance' along with several privacy complaints directed against Privacy Shield that will be heard by the ECJEU in the short-term from individuals and privacy groups, Privacy Shield is under a lot of pressure (Lomas 2019). These controversies have demonstrated the fragility of Privacy Shield and there is a significant chance of Privacy Shield being repealed in the near future.

8.4 California Consumer Privacy Act

Due to the extraterritorial scope of the GDPR, there has been pressure on the US to implement their own comprehensive privacy legislation framework. In June 2018, the first state to pass an updated privacy act is California, which is traditionally the front-runner in the US when it comes to legislative innovation.[48] The California Consumer Privacy Act (CCPA) is set to go into effect in January 2020. It echoes some of the provisions in the GDPR and this legislation has been influenced greatly by the GDPR (and has even been deemed "GDPR Lite").[49] There are some striking resemblances in the proposed legislation, such as notice; right to be forgotten

[47] Executive order no. 13768, 82 FR 8799 (2017).
[48] Based on the conclusions of research by legal experts on the subject, e.g. Vogel (1995) and Perkins and Neumayer (2012).
[49] See for example: Slefo, George. 2018. "Marketeers and Tech Companies Confront California's Version of GDPR". https://adage.com/article/digital/california-passed-version-gdpr/314079

and access and portability, but also major areas where the CCAP offers less protection to consumers and more freedom for companies, such as the right to human review, the application of the Act and the fining mechanism. To sum up, the CCAP is similar to the GDPR in scope, but more lenient than the GDPR in some crucial areas. Important to note is that the Act is being heavily lobbied against and the California legislature anticipates amending and clarifying the Act before it will be implemented (Erns & Young 2018). At the time of writing, it is therefore not yet clear what the ultimate implications of the CCAP will be.

9. Conclusions

This research has found that AI technologies need personal data to become 'smarter'. Where ML often needs linkable data (QI's) to keep its utility, DL requires large amounts of personal data to be used as an example to learn from. Complete anonymization of this personal data often sacrifices its utility. Pseudonymization is the preferred tool that is highlighted in the GDPR as a compromise between full anonymization and identifiable data, keeping the data subject protected without sacrificing its utility for data processers. However, companies have to determine if the pseudonymized can reasonably be used by third parties to reidentify the data subject, in which case the data is still personal, meaning full compliance with the GDPR in that area.

In addition to the GDPR, the Free Flow Regulation applies to all non-personal data since its implementation in 2019. This Regulation was brought into existence especially with the promotion of technological innovation in mind. It allows for easier cross-border sharing of non-personal data, which would improve the free movement of data in the EU. However, because of the far-reaching definition of personal data stemming from the *Breyer* case, ambiguity arises on the usefulness of this Regulation in that regard. Because of the possibility of re-identification in the context of big data analytics, it would become problematic to determine what kind of data would fall under the Free Flow Regulation, as most data would, in fact, fall under the GDPR. Because of this, companies will likely qualify almost all data as 'personal', since there is a risk of inadvertent non-compliance when data is re-combined and re-identified. This will deter AI companies from using de-identified data.

AI companies handling data will, therefore, most likely have to deal with the GDPR and its limitations on data collection-, processing and handling. The EU recognizes the importance of becoming a world leader in AI through an early development. The EU has got significant drivers that it could use to realize early development of AI. Europe ranks second in AI start-ups and has a strong base of solidified AI companies. However, more than half of the European companies considering using AI in their business, deem GDPR-compliance to be a strong obstacle to using AI in their business. This fact is consistent with this study about conflicts between the legal obligation from the GDPR and AI development.

These limitations stem from multiple articles in the GDPR, the most impactful being the following. The purpose limitation stemming from article 6, means that data controllers cannot use personal data for other purposes than the purpose for which consent is given. This restricts data controllers from adding new functionality to an AI system; consent has to be given every time data needs to be repurposed. If a user does not give this consent (which is likely because there would be no incentive for users to give further consent), than the data cannot be used for AI technologies.

Article 12 and 22 gives data subjects the right that algorithmic decisions regarding them must be reviewable and explainable by humans. Whether or not EU citizens will actually exercise these rights, as has been explored in section 5.5, does not matter in the context of the development of ML and DL through algorithms. Because all algorithms have to be explainable, there will be a trade-off between the sophistication of an algorithm and its transparency. By placing the right to explanation in a recital, it shows that the EU did not grant this idea the same legal status as other rights in the GDPR. Further legislation or jurisprudence will be critical in the overall impact of this article on the development of AI in the EU.

Another conflict arising from the GDPR is article 17, which provides the right to erasure without undue delay. The overall effects of the right of erasure on AI development are largely dependent on the frequency that such a request is placed. In section 5.5, data indicates that 13 per cent of EU citizens have already exercised the right to erasure. This is a considerable amount, which is only likely to go up giving the novelty and increasing general awareness of the GDPR.

Apart from the Free Flow Regulation and the GDPR, the EPR is being negotiated on the EP-level. At the time of writing, the EPR is still under negotiation in the EP and it is unclear if and in what form the EPR would eventually materialize. The EPR, if to be implemented in the way it is proposed now, would severely limit the ways in which companies can collect data and AI companies would be negatively affected in this regard. Another event in the near future that could decide the competitiveness of the EU in the near-future is *Brexit*. The UK is the EU's leading Member States when it comes to AI research and development. With *Brexit*, the AI industry in the EU will likely suffer from the loss of their greatest innovator in that field.

The main conclusion that can be drawn from this study is that it is highly likely that the US in the medium-term will conform to the GDPR model of personal data protection through the Brussels effect. There is precedent in the field of privacy regulation flowing from Europe to different parts of the world. The US will likely succumb to the standards of the GDPR, due to (among other factors) technical nondivisibility of AI systems between the EU and the US, the extraterritorial scope of the GDPR and because of the focus of AI technologies on the European consumer market. The imminent cessation of the EU-US Privacy Shield will likely be a catalyst for another transatlantic agreement that respects the principles of the GDPR. In fact, the CCAP, which is set to be implemented in 2020, already echoes some of the key provisions of the GDPR. The CCAP (as it is proposed in its current form) in general has less strict regulations for companies using data, this means that to comply with the GDPR, in most cases, is to comply with the CCAP. That is why it would be likely that tech companies would choose one compliance model, instead of having to create a 'patchwork' of compliance models. Because of the way that California is often the front-runner of nationwide legislation (also known as the 'California effect') and because of the Californian technological hubs around Silicon Valley, it is likely that the CCAP will set the norms nationwide in the US. On the other hand, it is still unclear in what form the CCAP will be ultimately implemented. Future research will be needed in that regard.

How DPA's and the EDPB are able to force compliance with the GDPR in the future will be a decisive factor on the impact of the GDPR on AI. Moreover, the future of AI development in the EU is dependent on the way that the ambiguities in the GDPR will be interpreted and acted upon in the future. The ECJEU will likely play a major role in deciding the ultimate implications of the GDPR for AI development. The ECJEU, which have traditionally taken an activist stance on the subject of privacy protection, will have to strike the right balance between guaranteeing privacy protection for EU citizens and creating a beneficial climate for AI innovation in Europe.

Bibliography

- Beatle, Alan. 2017. "Why the Whole World Feels the 'Brussels Effect'." *Financial Times,* November 16, 2017. https://www.ft.com/content/7059dbf8-a82a-11e7-ab66-21cc87a2edde
- Bendiek, Annegret and Römer, Magnus. 2019. "Externalizing Europe: the global effects of European data protection." *Digital Policy, Regulation and Governance* 21 (1): 32 – 43.
- Bielieauskaite, Justina. 2018. "ePrivacy – a new EU law that scares digital businesses?" Accessed June 26, 2019. https://www.digitalsme.eu/eprivacy-new-eu-law-scares-digital-businesses/
- Bradford, Anu. 2012. "The Brussels Effect". *Colombia Law School Scholarship Archive*. Accessed June 11, 2019. hps://scholarship.law.columbia.edu/faculty_scholarship/271
- Coseraru, R. 2017. "Facial Recognition Systems and their Data Protection Risks Under the GDPR." *MA Thesis*, Tilburg University.
- Cullinan, Fiona. 2018. "Machine learning in a world of GDPR and new e-Privacy Regulation." Accessed June 26, 2019. https://firehead.net/2018/08/machine-learning-gdpr-epr-privacy-regulation/
- Data Protection Commission. 2019. "Anonymisation and pseudonymization." Accessed June 18, 2019. https://www.dataprotection.ie/en/guidance-landing/anonymisation-and-pseudonymisation
- Debussche, Julien, César, Jasmien and De Moortel, Isis. 2019. "Big Data & Issues & Opportunities: Free Flow of Data." Accessed June 20, 2019. https://www.twobirds.com/en/news/articles/2019/global/big-data-issues-and-opportunites-free-flow-of-data
- Deloitte. n.d. "The Impact of the One Stop Shop Mechanism." Accessed June 20, 2019. https://www2.deloitte.com/ch/en/pages/risk/articles/gdpr-one-stop-shop.html
- Deloitte. 2019. "Next step after the GDPR: the ePrivacy Regulation." Accessed June 26, 2019. https://www2.deloitte.com/nl/nl/pages/risk/articles/next-step-after-the-gdp-the-eprivacy-regulation.html
- Directorate-General for Internal Policies. 2018. "European Artificial Intelligence (AI) leadership, the path for an integrated vision." Accessed June 27, 2019. http://www.europarl.europa.eu/RegData/etudes/STUD/2018/626074/IPOL_STU(2018)626074_EN.pdf

- Ernst & Young. 2018. "The California Consumer Privacy Act: Overview and Comparison to the GDPR." Accessed June 28, 2019. https://consulting.ey.com/wp-content/uploads/sites/3/2018/11/The-California-Consumer-Privacy-Act_Overview-and-comparison-to-the-EU-GDPR-ilovepdf-compressed-4.pdf
- Etzioni, Oren. 2016. "No, the Experts Don't Think Super intelligent AI is a Threat to Humanity." *MIT Technology Review*, September 20, 2016. https://www.technologyreview.com/s/602410/no-the-experts-dontthinksuperintelligent-ai-is-a-threat-to-humanity/
- Eurobarometer. 2019. "Report Special Eurobarometer 487a – March 2019: The General Data Protection Regulation." Accessed June 18, 2019. http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/86886
- European Commission. 2018. "Artificial Intelligence for Europe." *Communication from the European Council*. Accessed 20 December, 2018. https://eurlex.europa.eu/legalcontent/EN/TXT/?uri=COM%3A2018%3A2373AFIN
- European Commission. 2019. "Building a European Data Economy." *Communication from the Commission to the European Parliament,* Accessed June 20, 2019.
- European Commission. n.d. "What is personal data?" Accessed June 20, 2019. https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en
- European Data Protection Board. 2019. "First overview on the implementation of the GDPR and the roles and means of the national supervisory authorities." Accessed June 19, 2019. http://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2019/02-25/9_EDPB_report_EN.pdf
- Grant, Jeremy and Neven, Damien. 2010. "The Attempted Merger Between General Electric and Honeywell: A Case Study of Transatlantic Conflict." *Journal of Competition Law & Economics* 1, no. 3: 595 – 633.
- Hall, Holly. 2018. "Restoring Dignity and Harmony to United States- European Union Data Protection Regulation**."** *Communication Law and Policy* 23 (2): 125-157.
- Hall, Holly Kathleen. 2018. "Restoring Dignity and Harmony to United States- European Union Data Protection Regulation." *Communication Law & Policy* 23 (2): 125-157.
- He Li, Lu Yu & Wu He. 2019. "The Impact of GDPR on Global Technology Development" *Journal of Global Information Technology Management* 22 (1): 1-6.

- Heisenberg, Dorothee. 2005. *Negotiating Privacy: The European Union, the United States, and Personal Data Protection*. Boulder: Lynne Rienner Publishers.
- Hintze, Mike and El Emam, Khaled. 2017. "Comparing the Bene ts of Pseudonymization and Anonymization Under the GDPR**."** *IAPP White Paper*, Accessed June 18, 2019. https://iapp.org/media/pdf/resource_center/PA_WP2-Anonymous-pseudonymous-comparison.pdf
- Humerick, Matthew. 2018. "Taking AI Personally: How the E.U. Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence". *Santa Clara High Tech* 39 (3): 393 – 418.
- Kayali, Laura. 2010. "Inside Facebook's fight against European regulation." *Politico,* January 23, 2019. https://www.politico.eu/article/inside-story-facebook-fight-against-european-regulation/
- Klint, Finley. 2015. "Thank (Or Blame) Snowden for Europe's Big Privacy Ruling." Accessed June 28, 2019. https://www.wired.com/2015/10/tech-companies-can-blame-snowden- data-privacy-decision/.
- Lavenex, Sandra. and Schimmelfennig, Frand. 2009. "EU rules beyond EU borders: theorizing external governance in European politics." *Journal of European Public Policy* 16 (6): 791-812
- Lomas, Natasha. 2019. "EU-US Privacy Shield complaint to be heard by Europe's top court in July." Accessed June 27, 2019. https://techcrunch.com/2019/05/28/eu-us-privacy-shield-complaint-to-be-heard-by-europes-top-court-in-july/
- Loyens & Loeff. 2018. "EU-US Privacy Shield on the chopping block?" Accessed June 27, 2019. https://www.loyensloeff.com/en-us/news-events/news/eu-us-privacy-shield-on-the-chopping-block
- Malle, Bernd et al. 2016. "Right to be Forgotten: Towards Machine Learning on Perturbed Knowledge Bases." Accessed June 10, 2019. https://hal.inria.fr/hal01635002/document
- Marelli, Luca. 2018. "Scrutinizing the EU General Data Protection Regulation." *Science* 360 (1): 496 – 498.
- Maskey, Sameer. 2018. "AI For Humanity: Using AI To Make A Positive Impact In Developing Countries." *Forbes*, August 23, 2018 https://www.forbes.com/sites/forbestechcouncil/2018/08/23/ai-for-humanityusing-ai-to-make-a-positive-impact-in-developing-countries-2/#7eae9c521b08

- Meyer, David. 2018. “AI Has a Big Privacy Problem and Europe's New Data Protection Law Is About to Expose It” *Fortune, May 25, 2018*. *http://fortune.com/2018/05/25/aimachine-learning-privacy-gdpr/*
- Montjoye, Yves-Alexandre, Farzanehfar, Ali, Hendrickx, Julien and Rocher, Luc. 2017. “Solving Artificial Intelligence’s Privacy Problem.” *Field Actions Science Reports* 17 (1): 80 – 83.
- Moreno, Antonio and Téofilo Redondo. 2016.“Text Analytics: the convergence of Big Data and Artificial Intelligence.” *International Journal of Interactive Multimedia and Artificial Intelligence* 3 (6): 58 - 64.
- Murray, James. 1884. *Oxford English Dictionary*. Oxford: Oxford University Press.
- Niemann, Fabian and Schüßler, Lennart. 2016. “CJEU decision on dynamic IP addresses touches fundamental DP law questions.” Accessed June 20, 2019. https://www.twobirds.com/en/news/articles/2016/global/cjeu-decision-on-dynamic-ip-addresses-touches-fundamental-dp-law-questions
- Perkins, Richard and Neumayer, Eric. 2012. “Does the ‘California effect’ operate across borders? Trading- and investing-up in automobile emission standards.” *Journal of European Public Policy* 19 (2): 217 – 237.
- Science Europe. 2019. “Regulation on the Free Flow of Non-personal Data.” Accessed June 19, 2019. https://www.scienceeurope.org/legislation/activities/free-flow-of-non-personal-data/
- Tegmark, Max. 2017. *Life 3.0*. New York: Penguin.
- Tiku, Nitasha. 2018. “Europe’s New Privacy Law Will Change the Web and More.” *Wired,* accessed June 11, 2019. https://www.wired.com/story/europes-new-privacy-law-will-change-the-web-and-more/
- Torra, Vicenc and Guillermo Navarro. 2016. “Big Data Privacy and Anonymization.” *Privacy and Identity Management* 11 (2): 15 – 26.
- Touw, Steve. 2017. " Anonymization and the Future of Data Science.” Accessed June 21, 2019.
- Ujj, Orsolya. 2016. “European and American views on Genetically Modified Foods.” *New Atlantis: A Journal of Technology and Society* 49 (1): 77-92.
- Vinocur, Nicholas. 2019. “Google fine launches new era in privacy enforcement.” *Politico,* January 21, 2019. https://www.politico.eu/article/google-fine-privacy-enforcement-france-gdpr/

- Vogel, David. 1997. *Trading up: Consumer and Environmental Regulation in a Global Economy*. Cambridge: Harvard University Press.
- Wachter, Sandra, Mittelstadt, Brent and Floridi, Luciano. 2017. "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation." *International Data Privacy Law* 7 (2): 76-99.
- Wallace, Nick and Castro, Daniel. 2018. "The Impact of the EU's New Data Protection Regulation on AI.". *Centre for Data Innovation*. Accessed December 20, 2018.