The extraterritorial scope of European data protection law

The changes in extraterritorial scope between the Data Protection Directive and the General Data Protection Regulation.

Candidate number: 586

Submission deadline: 25.11.2017

Words: 17505
# Table of contents

1 INTRODUCTION .................................................................................................................. 1
   1.1 Theme ............................................................................................................................ 1
   1.2 Relevance ...................................................................................................................... 1
   1.3 Research question ......................................................................................................... 2
   1.4 Methodology and clarification ..................................................................................... 2
   1.5 Sources of law ............................................................................................................... 3
   1.6 Terminology .................................................................................................................. 4
   1.7 Outline ........................................................................................................................... 5

2 TERRITORIALITY VS. EXTRATERRITORIALITY ......................................................... 6
   2.1 The territoriality principle ............................................................................................ 6
   2.2 The concept of extraterritoriality ............................................................................... 6

3 DEFINING CONCEPTS NECESSARY FOR THE ANALYSIS ........................................... 8
   3.1 The controller ................................................................................................................. 8
   3.2 The processor ............................................................................................................... 8
   3.3 Personal data ............................................................................................................... 9
   3.4 Processing .................................................................................................................... 9

4 EXTRATERRITORIAL SCOPE OF THE DATA PROTECTION DIRECTIVE ............. 10
   4.1 Introduction to the DPD .............................................................................................. 10
   4.2 The broad scope of the DPD ....................................................................................... 10
   4.3 Article 4 of the DPD .................................................................................................... 10
   4.4 An establishment as a connecting factor ..................................................................... 10
      4.4.1 The country of origin principle .............................................................................. 11
      4.4.2 The SWIFT Opinion ............................................................................................. 12
      4.4.3 Establishment as a concept .................................................................................. 13
      4.4.4 The Weltimmo case .............................................................................................. 14
      4.4.5 The weak connection between stable arrangement and activity ......................... 15
      4.4.6 Human presence .................................................................................................. 15
   4.5 In the context of the activities ..................................................................................... 17
      4.5.1 Interpretation by the WP ....................................................................................... 17
      4.5.2 The Google Spain case ......................................................................................... 17
      4.5.3 Update opinion by the WP ................................................................................... 19
      4.5.4 Ramifications of the Google Spain case and subsequent opinion by the WP .... 19
   4.6 Establishments on the territory of several member states .......................................... 20
4.6.1 Multiple national laws may be applicable .................................................. 21
4.7 The use of equipment ............................................................................. 21
  4.7.1 The concept of making use of equipment ........................................... 22
  4.7.2 Control over equipment ................................................................ 22
  4.7.3 Equipment is a weak connecting factor ........................................... 23
4.8 The problem with the WP’s opinions ..................................................... 24
4.9 Preliminary concluding remarks ............................................................ 24
  4.9.1 Procedure for determining the applicability .................................... 24
  4.9.2 The EU’s territorial or extraterritorial jurisdiction ........................... 25
  4.9.3 Motivation behind the DPD’s extraterritorial application ................... 25

5 EXTRATERRITORIAL SCOPE OF THE GENERAL DATA PROTECTION
   REGULATION ............................................................................................... 27
  5.1 Introduction to the GDPR ................................................................... 27
  5.2 From directive to regulation ................................................................. 27
  5.3 The broad scope of the GDPR ............................................................ 27
  5.4 Article 3 of the GDPR ........................................................................ 28
  5.5 Controller and processor as the subject .............................................. 28
  5.6 An establishment as a connecting factor .............................................. 28
  5.7 In the context of the activities .............................................................. 29
  5.8 The targeting approach ...................................................................... 30
    5.8.1 Targeting ....................................................................................... 30
    5.8.2 The offering of goods and services ................................................ 30
    5.8.3 The monitoring of behaviour ....................................................... 31
  5.9 Abandoning equipment as a connecting factor .................................... 32
  5.10 The effects principle .......................................................................... 33
  5.11 No physical presence on the territory of a member state ..................... 34
  5.12 The subjective- or outcome-based targeting approach ....................... 34
  5.13 Preliminary concluding remarks ......................................................... 36
    5.13.1 Procedure for determining the applicability ................................. 36
    5.13.2 A missed opportunity ................................................................. 36
    5.13.3 Motivation behind the GDPR’s extraterritorial application ............ 36

6 EXTRATERRITORIAL IMPLICATIONS OF THE TRANSFER OF
   PERSONAL DATA TO THIRD COUNTRIES ............................................ 38
  6.1 Domestic measures with extraterritorial implications .......................... 38
  6.2 Transfer of personal data to third countries under the DPD ................. 38
  6.3 Transfer of personal data to third countries under the GDPR .............. 39
  6.4 Extraterritorial implication of the DPD and the GDPR ......................... 40
6.5 Preliminary concluding remarks ............................................................. 41
   6.5.1 Transferring personal data to third countries .................................... 41
   6.5.2 Motivation behind the rules ............................................................. 42

7 CONCLUDING REMARKS ........................................................................... 43

BIBLIOGRAPHY .............................................................................................. 45
1 Introduction

1.1 Theme
The theme for this master thesis is the extraterritorial scope of European data protection law.

1.2 Relevance
The current stage of human development is often referred to as “the information age”. The introduction of the World Wide Web to the masses in the 1990s, marked the beginning of an explosion in the processing of personal data. At the time of writing this master thesis; Facebook has 2 billion monthly active users\(^1\) and Google’s revenue amounts to 89.46 billion dollars\(^2\). Companies like these have made a business model out of the use of personal data, whether it be through targeted advertising, or maintaining and improving their services.

There have been several attempts to regulate personal data. The *DPD* (Directive 95/46/EC, Data Protection Directive) entered the data protection stage in 1995. The instrument was not revolutionary, but some authorities in the field considers it to be one of the most ambitious and comprehensive data privacy regulations ever put to paper.\(^3\) The DPD is set to be replaced by the *GDPR* (Regulation 2016/679, General Data Protection Regulation). The new instrument aspires to clarify and improve on the principles and objectives introduced in the DPD. Both instruments demonstrate the *EU’s* (European Union) desire to adapt its legislation to combat the increasing threat to the personal data of its member states citizens.

The internet transcends traditional territorial borders. A company may have its physical place of business and storage of wares located in the USA, but the internet has allowed the company to offer its wares to the European market. In an increasingly interconnected world, the EU has been faced with the challenge of protecting personal data that is leaving the territorial boundaries of the EU and the *EEA* (European Economic Area). The EU has responded to this challenge by incorporating articles in the instruments that makes their data protection rules applicable outside the territory of the EU/EEA.

\(^1\) Statista, (2017a).
\(^2\) Statista, (2017b).
1.3 Research question
The extraterritorial scope of the DPD has garnered confusion and controversy. The practice of extraterritorial jurisdiction is in itself controversial, but the articles in the DPD that concern its scope are also vague and complex. Attempts have been made to clarify some of the uncertain aspects through case law and opinions by advisory entities, with varying degrees of success. Even now, as the DPD is set to be replaced by the GDPR, its extraterritorial scope remains elusive and contested.

In this master thesis, I attempt to answer the question: what are the changes in extraterritorial scope between the DPD and the GDPR? To answer this research question will require an in-depth analysis of the instruments articles that makes their extraterritorial application possible. Only then can the extraterritorial changes be identified. The main focus of this master thesis is on the changes between the instruments, but attention is also afforded the similarities that remain between them. This ensures a more comprehensive presentation of the extraterritorial scope of the DPD and the GDPR.

1.4 Methodology and clarification
Article 4. (1). (b) of the DPD and article 3. (3) of the GDPR makes their data protection laws applicable to controllers in places where a member state’s law applies by virtue of public international law. Public international law is law that governs the states interaction with each other, e.g. the law applicable to embassies. This falls outside the scope of this master thesis and will not be analysed in further detail.

There is a limited amount of case law dealing directly with the extraterritorial scope of the DPD. Two landmark cases by the Court of Justice of the European Union is afforded considerable analysis in this master thesis. Other case law has argumentative value, but does not concern the DPD or the GDPR directly. Consequently, further guidance on the interpretation of both the DPD and the GDPR must be found in other sources of law, e.g. opinions by the article 29 Working Party.

The GDPR has very recently entered into force. Outside of the text itself, any preparatory work and interpretations by authors of law, there are few sources that deals directly with the GDPR. As a result, my analysis of the extraterritorial application of the GDPR will rely more heavily on my own interpretations and opinions.

The DPD requires its member states to implement its data protection rules. Throughout this master thesis, I refer directly to the DPD and/or its rules, rather than the national laws of the member states. This is done out of a desire to simplify the text for the reader.
My referencing scheme utilizes footnotes. Much of the case law utilized in this master thesis concern multiple parties with elaborate names. The footnotes would become extensive and intricate if the official names of the cases were used. In order to simplify both the text and the sources, case law will be referred to by their official name once, in the text, but subsequently referred to by a shortened popular name in the text and the case number and popular name in the footnotes.

Quotes from case law, opinions, authors of law, etc. are sometimes deliberately shortened at the end, to be more succinct. I have chosen not to signify such editing because of readability.

1.5 Sources of law

The DPD and the GDPR are instruments drafted by the EU. They are directed towards the member states of the EU. The text of the instruments serves as the main source of law and is the basis for the interpretations made by the courts, advisory entities, authors of law and myself. The instruments recitals compliments and aids in the interpretation of concepts, words and phrases in the articles.

Case law by the CIEU (Court of Justice of the European Union) is frequently referenced in the text. The CIEU is the judicial authority of the EU and consists of the Court of Justice and the General Court. The court’s principal task is to “examine the legality of EU measures and ensure the uniform interpretation and application of EU law.” For this reason, the case law of the CIEU serves as an important source for the interpretation of the DPD and GDPR.

Opinions by Advocate Generals are sometimes referenced in the text. They assist the Court and are “responsible for presenting, with complete impartiality and independence, an ‘opinion’ in the cases assigned to them.” These opinions do not enjoy the same weight as the case to which they offer their opinion, but they still carry some argumentative weight. Often times, these opinions are more elaborate on certain aspects of the DPD than the actual judgement.

The WP (Working Party on the Protection of Individuals with regard to the Processing of Personal Data) is referenced frequently in this master thesis. Being an advisory entity, the WP is tasked with, inter alia, examining questions covering the application of the DPD and making recommendations on data protection matters. Their opinions do not carry the same weight as case law, but they often find their way into the opinions of the Advocate Generals on the cas-

4 Curia, (2017).
5 Ibid.
6 DPD. art. 29. (1).
7 DPD. art. 30.
es of the CJEU, which demonstrates their argumentative value. With the relatively limited amount of case law on aspects of the DPD and GDPR, the opinions by the WP often end up being the only interpretative authority on the subject. In these cases, the opinions by the WP must carry additional weight.

Interpretations made by authors of law (authors that write about legal subjects) is sometimes used in the text. The weight of their opinions is limited. The strength of their argument determines whether their opinions can be emphasized. If an argument is relatively balanced, logical and reasoned, there can be some argumentative value in it.

The independent weight of the proposals and reports of the Commission (European Commission) is limited to non-existent. But they can be used to explain how and sometimes why the DPD and GDPR arrived at their final form. They provide a unique insight into the processes and rationales behind the instruments and elaborates on aspects that needs improving or clarification.

The text refers to case law from Germany and the USA. These cases do not directly concern the DPD or the GDPR, but they serve to exemplify viable solutions to unclear aspects of the instruments and illuminates problematic consequences of technological innovation. Any argumentative value in the judgements, is dependent on the strength of the argument made by the courts.

1.6 Terminology
In this master thesis, jurisdiction is understood to encompass three abilities. The ability to “make […] law applicable to the activities, relations, or status of persons, or the interest of persons in things”. The ability to “subject persons or things to the process of […] courts or administrative tribunals”. The ability to “induce or compel compliance or punish noncompliance with […] laws or regulations”.8

The term extraterritorial is controversial and may have negative connotations for the reader.9 This master thesis will utilize the term extraterritorial regardless of its detractors. This choice is made on the basis of its prevalence and simplicity, and not on any judgement of extraterritorial jurisdiction’s qualities.

The Court of Justice of the European Union has traditionally been referred to as the ECJ (European Court of Justice). In recent years, the designation has changed to CJEU. To avoid any confusion, CJEU will be used to refer to the court.

The Commission was previously known as the Commission of the European Communities before it became known as the European Commission. In the bibliography, both names will be used as the proposals and reports referenced in the text span over two decades.

Third countries are countries located outside of the EU/EEA. They are not members of the EU and have traditionally been considered to be beyond the reach of the EU’s jurisdiction.

Connecting factors are criteria utilized in the DPD and the GDPR that signifies that a subject has the required connection to the EU/EEA to warrant the application of the instruments.

1.7 Outline
In order to analyse the extraterritorial application of the DPD and the GDPR, the concept of extraterritoriality must be explored. Chapter 2 defines the concept of extraterritoriality and compares it to the more widely accepted territoriality principle. Chapter 3 defines concepts that are utilized by the DPD and the GDPR, which are necessary to understand in the forthcoming analysis. In chapter 4, article 4 of the DPD is analysed in order to extract the extraterritorial scope of the DPD. In chapter 5, article 3 of the GDPR is analysed and compared to article 4 of the DPD. In chapter 6, the extraterritorial implications of rules in both the DPD and GDPR that limits the transfer of personal data to third countries are analysed. The analysis is separated from chapter 4 and 5 because the extraterritoriality is based on territorial rather than extraterritorial jurisdiction. My concluding remarks are presented in chapter 7.
2 Territoriality vs. extraterritoriality

2.1 The territoriality principle

In order to understand what extraterritoriality is, and the ramifications of a legislator imbuing a law with extraterritorial properties, the territoriality principle needs to be explained. Other principles of jurisdiction exist in addition to the territoriality principle, e.g. the protective principle, the universality principle, etc. The principle can be traced back to the seventeenth century, with the emergence of the modern, fully sovereign nation State.\textsuperscript{10} Today, it is recognized as the basic principle of jurisdiction in international law.\textsuperscript{11}

The principle of sovereign equality of states and the principle of non-intervention is the foundation for the territorial principle.\textsuperscript{12} A state has the exclusive right and ability to pass laws and judgement within its own territory. Other states may not interfere with this ability. Lowe and Staker puts it succinctly, “States may impose the entirety of their laws – economic, social, cultural, or whatever – upon everyone within their territories.”\textsuperscript{13} Consequently, territorial jurisdiction extends to people who are present inside the state’s borders, but who are not formal citizens.

2.2 The concept of extraterritoriality

The aim of this chapter is not to give an all-encompassing presentation of extraterritoriality. The scope of the concept is simply too extensive. The goal is to confirm its existence and to provide a basic understanding of it.

The concept of extraterritoriality is the antithesis to the territoriality principle. Extraterritorial jurisdiction is the “ability of a state, via various legal, regulatory and judicial institutions, to exercise its authority over actors and activities outside its own territory.”\textsuperscript{14} Traditionalists may reject any notion of extraterritorial jurisdiction because it collides with the territoriality principle. Some authors of law are embracing this form of jurisdiction. Ryngaert acknowledges the existence of national laws having extraterritorial application.\textsuperscript{15} Svantesson views extraterritorial jurisdiction as a “natural consequence, if not a necessity, where we have cross-border activities.”\textsuperscript{16}

\begin{flushleft}
\textsuperscript{10} Ryngaert, (2008), p. 47.  \\
\textsuperscript{11} Ibid., p. 42.  \\
\textsuperscript{12} Ibid., p. 29.  \\
\textsuperscript{13} Lowe, (2010), p. 320.  \\
\textsuperscript{14} Zerk, (2010), p. 13.  \\
\textsuperscript{15} Ryngaert, (2008), p. 85.  \\
\end{flushleft}
Extraterritorial application of laws is also recognized, though not explicitly, by the CJEU in, inter alia, the *Air Transport Association of America case* (Case C-366/10, Air Transport Association of America and Others v. Secretary of State for Energy and Climate Change). The case concerned a directive that requires planes that arrive at and depart from EU airports to have allowances for greenhouse gas emissions. This was contested on the grounds that many flights largely take place outside the EU, i.e. that the EU had overstepped its jurisdiction. The court seems to reason that, by choosing to operate a commercial air route in the EU, there is a sufficient link with the EU for the planes to be subjected to EU law.\(^\text{17}\) Regardless of the connection between the parties, the EU is regulating conduct that takes place outside its territory.

Legislation that explicitly or through interpretation has extraterritorial application is not the only example of extraterritorial legislation. Zerk has described a form of extraterritoriality which she terms “Domestic measures with extraterritorial implication”. This is practice of influencing “conditions, standards and behaviour in other countries using domestic measures.”\(^\text{18}\) A state who engages in this type of behaviour is not practicing extraterritorial jurisdiction per se, but the effects of its domestic legislation are never the less felt outside its own territory.

These authors and judiciaries that acknowledges, explicitly or more indirectly, that domestic laws can be given extraterritorial application, is indicative of a change in the understanding of jurisdiction. This master thesis will show that the EU is no stranger to extraterritorial application of its data protection laws.

\(^{17}\) C-366/10, the *Air Transport Association of America case*, para. 126 – 127.  
3 Defining concepts necessary for the analysis

The DPD and the GDPR contain several concepts that must be defined in order to comprehend the extraterritorial application of the instruments.

3.1 The controller

The controlle is the subject which may be required to submit to the data protection rules in the DPD and GDPR. The definition of a controller is virtually identical in both instruments. Article 2. (d) of the DPD defines a controller as a someone who “alone or jointly with others determines the purposes and means of the processing of personal data”. Determining the purpose is essentially a question of why the processing is happening. The WP has elaborated on the requirement of “means” by including elements from the original and amended proposal to the DPD. The result is that “means”, in addition to technical ways, also refer to, inter alia: “which personal data are to be processed”, “which third parties shall have access to this data”, etc.19

Multiple subjects can be controllers together. The WP confirms that the assessment is the same as when identifying a single controller, though it points out that the participation of the subjects “may take different forms and does not need to be equally shared.”20 Identifying the controller is usually unproblematic, but corporate structures with multiple branches and subsidiaries located in several states may complicate the process. In some cases, it can be difficult to differentiate between what is a branch and what is a separate legal entity.

3.2 The processor

The definition of processor is virtually identical in both instruments. Article 2. (e) of the DPD defines processor as a someone who “processes personal data on behalf of the controller”. The WP has clarified that the processor must be a “separate legal entity” in relation to the controller.21 A subject needs a mandate from the controller to be considered a processor. It can be difficult to differentiate between a processor and a joint controller. If the processor disobeys the limits of the mandate and starts to determine the purpose and means of the processing, the processor is a joint controller,22 with all the legal ramifications it entails. Some controllers, particularly bigger corporate entities, have the economic muscle to have the processing performed in-house. The processing is still being performed, but there is no subject that fulfils the definition of a processor in the instruments.

---

20 Ibid., p. 19.
21 Ibid., p. 25.
22 Ibid.
3.3  **Personal data**  
Both instruments have a similar definition of *personal data*. Article 2. (a) of the DPD defines personal data as “any information relating to an identified or identifiable natural person”. A typical example would be data which names a specific person, but data that indirectly can be used to identify a person, e.g. a social security number, is also considered personal data. Even data about cultural or social identity is considered personal data if the data is sufficiently specific to a person. Only data about natural persons is considered personal data. Data about, e.g. a business, will not qualify as personal data.

3.4  **Processing**  
Both instruments have a similar definition of *processing*. In article 2. (b) of the DPD “any operation or set of operations which is performed upon personal data” is considered processing. A whole host of different examples is provided, such as “collection”, “adaptation” and “erasure” etc. This means that almost any contact a controller or processor have with personal data is considered processing.
4 Extraterritorial scope of the Data Protection Directive

4.1 Introduction to the DPD
The DPD was finalized in 1995, after two proposals; the original proposal and the amended proposal. In 1999 the DPD was incorporated into the EEA agreement, making it binding for, inter alia, Norway. Being a directive, the DPD relies on the individual member states to pass laws, regulations and administrative provisions necessary to comply with its provision. The Commission has uncovered divergences in the member states national implementation of the rules contained in the DPD.

4.2 The broad scope of the DPD
The broad definition of personal data and processing means that the DPD has a broad scope of application. This is recognized by the Commission and means that the DPD can affect many different activities, by many different actors. This is particularly true on the internet, where the DPD is applicable to almost any operation. The DPD does not discriminate against different industries or activities, save for some exceptions in article 3. (2). The extraterritorial application of the DPD will potentially have consequences for a vast number of third country businesses.

4.3 Article 4 of the DPD
The territorial scope of DPD is regulated in article 4 under the headline “National law applicable”. Article 4 has proven difficult to implement for the member states. In the 2003 report on the implementation of the DPD, the Commission pointed out that several of the fifteen member states being scrutinized, had deficiencies in its national implementation of article 4. Article 4 does not explicitly address extraterritoriality. Any extraterritorial application contained in article 4 must be extracted through interpretation. I find it plausible that this is a result of the controversial nature of practicing extraterritorial jurisdiction.

4.4 An establishment as a connecting factor
The concept of “an establishment” in article 4. (1). (a) plays an important part in assessing the territorial scope of the national data protection laws. The chosen phrasing has far-reaching consequences and was apparently highly criticised during the review process.

23 DPD. art. 32. (1).
25 Ibid., p. 4.
26 Ibid., p. 17.
27 Ibid.
4.4.1 The country of origin principle

The implication of the choice of wording in the DPD article 4. (1). (a) is that the controller can have more than one establishment, effectively negating the country of origin principle. The principle can be observed in the E-commerce Directive (Directive 2000/31/EC), where article 3 requires that member states ensures that service providers established on their territory complies with their national provisions. This means that other states cannot impose their own national laws on the service provider. The country of origin principle only allows for a single place of establishment. This can be deduced from recital 19 of the E-commerce Directive, which stipulates that in situations where the service provider has multiple establishments, the establishment “is the place where the provider has the centre of his activities.”

The country of origin principle essentially means that the law of the country of which the subject originates is applicable, to the detriment of other countries laws. Moerel points out that the country of origin principle was incorporated into various areas of law around the same time as the DPD was adopted. In spite of the choices made in other legal instruments, the DPD goes against the grain. However, this was not always the case. In both the original and the amended proposal for the DPD, the country of origin principle is present.

The connecting factor in the Original Proposal is the location of a file. The territorial scope of the original proposal in article 4. (1). (a) is limited to “all files located in its territory”. The country of origin principle can be observed in (b). The law of the member state where the controller is “resident” is applied to the situation where the controller “uses from its territory a file located in a third country”. The use of the word resident does, in my opinion, indicate that the controller needs something more than, e.g. a branch or a subsidiary. The writers have also used the singular form of the word, indicating that there can be only one place of residence. Moerel has pointed out that the wording in the Original Proposal shares many similarities with, inter alia, the wording in the E-commerce Directive, which incorporates the country of origin principle.

In Article 4. (1). (a) of the Amended Proposal, the location of the file is substituted with the establishment of the controller because of the potential difficulties with locating a file or pro-

---

28 Moerel, (2011a), p. 94
29 Ibid.
30 COM(90) 314 final – SYN 287, (p. 52).
32 COM(92) 422 final - SYN 287. The Greek language version is the only version available from EUR-lex. A document containing the Amended Proposal from the University of Pittsburgh’s Archive of European Integration is used, (p. 68).
cessing operation. The law of the member state where the controller “is established” is made applicable to the processing of personal data. The phrasing indicates that there can only be one establishment of the controller. The statements made in the Explanatory Memorandum to the Amended Proposal backs up this interpretation by explaining that the connecting factors were chosen because “the same processing operation might be governed by the laws of more than one country”. A result of abandoning the country of origin principle is that multiple national laws may be applicable.

The country of origin principle is abandoned in the DPD article 4. (1). (a) by the inclusion of “an” before “establishment”. This is further evidenced by the controller’s obligation to ensure that every establishment complies with the national legislation of the establishment’s location in the same paragraph. The DPD accommodates for the country of origin principle if the controller only has one establishment. If the controller has any other establishment, in any other member state, the law of that member state applies. This change was made despite the submissions arguing for a country of origin principle during the review process.

If the DPD utilized the country of origin principle, a controller located in a third country would not have to comply with the DPD. This would be the case, even if the controller had, e.g. a branch in a member state. The connecting factor chosen in the DPD means that any establishment of the controller located in a member state, that fulfils the establishment requirements, can make the DPD applicable. Although the changes in phrasing from the proposals to the DPD are small, these changes lead to the extraterritorial application of the DPD.

4.4.2 The SWIFT Opinion

In 2006, the WP issued the SWIFT Opinion (Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)) which resurrected the country of origin principle. SWIFT offers messaging services for correspondent banking to financial institutions. The United States Treasury issued 64 subpoenas to SWIFT’s operation centre in the US, all of whom SWIFT complied with. In addition to its US based operation centre, SWIFT had another operation centre in the Netherlands and multiple sales offices in other member states. The head office was located in Belgium.

The WP found that Belgian data protection law was applicable to the processing operations of SWIFT. Moerel notes that the WP does not assess whether the processing takes place in the

---

34 Ibid.
36 WP 128, p. 9.
context of activities of the sales offices or the operation centre located in the Netherland. Instead, the WP argues that the “critical decisions” on the processing and transfer of personal data was decided by the head office. This argument bears a striking resemblance to the assessment of potential controllers. If the WP argues that the law of the controller is applicable, they are in reality arguing for the country of origin principle.

In my opinion, the SWIFT Opinion is an anomaly. It goes contrary to the wording of the DPD and later court cases will come to contradictory conclusions. The deliberation by the WP is slim, barely surpassing 2 paragraphs. I question whether the WP gave this issue the consideration that it requires. If this approach is adhered to, controllers could simply move their headquarters outside of the EU, effectively avoiding EU data protection laws.

4.4.3 Establishment as a concept

The DPD does not provide an exhaustive definition of the concept of an establishment, but has elaborated on its content in Recital 19: “establishment […] implies the effective and real exercise of activity through stable arrangements; […] the legal form of such an establishment […] is not the determining factor”. By excluding the legal form as the determining factor, a concrete assessment will have to be made of the potential establishment. This does not mean that the legal form is insignificant. Often times a branch or subsidiary provides a strong clue that the processor’s activities are real and effective through a stable arrangement.

In its opinion on applicable law, the WP made reference to statements made by the CJEU in the Berkholz case (Case 168/84 Gunter Berkholz v Finanzamt Hamburg-Mitte-Altstadt). Although the actual statement is located in paragraph 18, and not paragraph 14 of the text and is paraphrased by the WP, the statement serves to illuminate the concept of an establishment: “A stable establishment requires that “both human and technical resources necessary for the provision of particular services are permanently available”.” The WP is cautiously applying the wording of the CJEU, as it acknowledges that it is unclear whether the court’s interpretation of “freedom of establishment” is applicable to every situation covered by Article 4. In the bid to clarify what an establishment is, both the recital and the WP introduces new words and concepts. In turn, these words and concepts begs additional analysis.

---

38 WP 128, p. 9.
39 See 3.1.
40 WP 179, p. 11.
41 Ibid.
4.4.4 The Weltimmo case

4.4.4.1 Factual background

Weltimmo was a company registered in Slovakia. Through a website, Weltimmo offered the ability to advertise Hungarian properties. For this purpose, Weltimmo processed the personal data of the advertisers. When the first month of free advertisement passed, some advertisers requested that their advertisement and personal data be deleted. Weltimmo did not oblige the advertisers and billed them for its services. When the bills were not paid, Weltimmo forwarded its claims to debt collection agencies. The effected advertisers lodged complaints with the Hungarian data protection authority.

4.4.4.2 Opinion on an establishment

In the Weltimmo case (Case C-230/14, Weltimmo s. r. o. v Nemzeti Adatvédelmi és Információszabadság Hatóság), the court rejects a formalistic approach to the concept of establishment. A controller is not only established in a country where they are registered. Instead, the court utilises statements made by the Advocate General, who interprets recital 19 as providing a “flexible definition of the concept”. This approach means that a decision on whether a controller’s activities qualify as an establishment must be made on a case-by-case basis.

The court elaborates on the assessment that must be made:
“both the degree of stability of the arrangements and the effective exercise of activities […] must be interpreted in the light of the specific nature of the economic activities and the provision of services concerned.”

From the few words that are afforded the actual assessment by the court, and the statement that even a minimal real and effective activity qualifies as an establishment, it becomes apparent that the requirements are not strict.

In similar fashion, the court finds that the requirements for a controller to have a stable arrangement are not strict:
“the presence of only one representative can, in some circumstances, suffice […] if that representative acts with a sufficient degree of stability through the presence of the necessary equipment for provision of the specific services concerned”

---

42 C-230/14, the Weltimmo case, para. 29.
43 Ibid.
44 Ibid., para. 31.
Weltimmo possesses a letterbox, a bank account and a single representative in Hungary. The court found this to be sufficient for Weltimmo to have an establishment.46

4.4.5 The weak connection between stable arrangement and activity
In the Weltimmo case, the real and effective activity is assessed separately from stable arrangement. The person who provided stability, functioned as a representative in “administrative and judicial proceedings”.47 There is nothing in the judgement to indicate that the representative had any function in the business aspect of the company. The lack of required connection between the elements increases the possibility of extraterritorial application of the DPD, as more controllers presumably will fulfil the requirements of an establishment.

I question whether this separation of the elements is prudent. By using the Weltimmo case as an example, the alleged function of the representative could possibly be performed by a lawyer that is not employed by the company. Should the Weltimmo case be interpreted to mean that any stability creating arrangement, regardless of the connection to the activity, is sufficient? If so, the mere hiring of representation in a member state, combined with the necessary activity, would presumably make the DPD applicable. Controllers from third countries could possibly be caught by European data protection laws simply by trying to ascertain whether their activities are covered by the DPD. In my opinion, such an outcome would make the connection required for controllers in third countries seem incidental and weak.

4.4.6 Human presence
The statement made in WP 179 seems to indicate that an establishment requires a minimum of human presence. While the court does not deal with it directly in the Weltimmo case, the statements made about the lone representative indicates that their conclusion is just at precipice of what can be considered an establishment. My research could not uncover any court cases dealing directly with this requirement. Due to the lack of case-law or statements by the WP dealing with the subject, I will try to outline how a court may and should rule when there is no human presence connected with the establishment of the controller.

The German Pipeline case (BFH II R 12/92) concerned a company based in the Netherlands which transported crude oil through underground pipelines located in Germany. The case concerns tax law. Any applicability to data privacy law is not immediately apparent. However, the WP used statements from the Berkholz case to elaborate on the requirement of an establishment. As both the Berkholz case and the German Pipeline case concerns tax law, and

46 Ibid., para. 33
47 Ibid.
both cases interpret the meaning of a fixed establishment, it is my opinion that statements made in the German pipeline case can be used to illuminate the requirement of an establishment in data privacy law.

The federal fiscal court (Bundesfinanzhof) made this statement in relation to whether the pipeline constituted an establishment in Germany: “The use of persons (entrepreneurs, employees, third-party employees, subcontractors) in or at the business establishment is not always required”. A similar statement was made by the Schleswig-Holstein Financial Court (Schleswig-Holsteinisches Finanzgericht) in the Swiss Server case (SHF II 1224/97). A server located in Switzerland was found to be a permanent establishment for a German company, even though no employees of the company had any interaction with the server. If these cases are viewed in conjunction with the WP’s acknowledgement that it is uncertain of the scope of the statements made by the CJEU, it is my opinion that, although human presence is a good indication that a controller has an establishment in a country, it is not an absolute requirement.

My argument has extraterritorial ramifications. By lowering the bar for what constitutes an establishment, more controllers located in third countries will presumably be subject to EU data privacy law. I acknowledge that I am weakening the already weakened requirements of an establishment proposed in the Weltimmo case. Critics can claim that my argument makes an establishment, an illusory connecting factor. Such criticism is not without merit, but a concrete assessment still needs to be made on a case-by-case basis. If the representative in the Weltimmo case is removed from the equation, the question remains whether the letterbox and the bank account possess the required activity and stability.

My argument opens up for the possibility that servers or computers can be establishments. This is seemingly in conflict with statements made by the WP in Opinion 8/2010 that a server or computer “is not likely to qualify as an establishment”. By pairing the Swiss server case with the lack of a definitive rejection by the WP, it is my opinion that servers and computers can be establishments, but that the assessment of stability and activity should be more stringent in these situations.

A requirement of human presence will also run afoul to the objective of the DPD. In an age where increasingly, jobs are being taken over by machines or artificial intelligence, such a

---

48 BFH II R 12/92, the German Pipeline case, para. 13 under “Entscheidungsgründe”. Translated from German. The case has been archived by Simons & Moll-Simons GmbH which archived all German supreme court decisions from 1980 to 2010.

49 SHF II 1224/97, the Swiss Server case, para. 22. The case has been archived by Jurpc.

50 WP 179, p. 12.
requirement seems ill conceived if the DPD is going to fulfil its objective of protecting the right to privacy of natural persons laid down in article 1. (1). A requirement of human presence may also serve as a loophole for controllers actively seeking to circumvent the DPD. By avoiding human presence in their establishments, they can also avoid European data protection law.

It can be argued that the question of human presence is of minor importance, as article 4. (1). (c) may still make the DPD applicable to the controller’s activities if equipment is situated on the territory of a member state. My retort is that the question of human presence is not only of importance to the DPD, no matter how insignificant, but also to the GDPR. 51 The use of equipment as a connecting factor also leads to some unfortunate consequences, 52 which can be avoided if article 4. (1). (a) is used instead.

4.5 In the context of the activities

In order for the DPD to apply to a controller, article 4. (1). (a) stipulates that the processing needs to be “carried out in the context of the activities” of an establishment. The DPD does not offer any additional clarification on the wording, which has resulted in a great deal of uncertainty about the requirement.

4.5.1 Interpretation by the WP

The WP entered the stage late with opinion 8/2010 on applicable law. Despite dedicating several pages of the opinion to the requirement, the information that serves to clarify the requirement is sparse, save for a few examples. In order to ascertain whether data is being processed in the context of an establishment, the WP elaborates on three elements that should be taken into account: The first element is the degree of involvement of the establishment(s). The goal is to map which establishment is doing what in order to differentiate between the main establishment of the controller and other establishments. Only then can the appropriate national law be applied. The second element is the nature of the activities. It is crucial to establish whether an activity concerns data processing, and which processing is connected to which activity. The last element is the objectives of the directive. 53

4.5.2 The Google Spain case

The WP failed to demystify the requirement in its opinion. A few years passed before a milestone case in 2014, tackled the requirement.

51 See 5.9.
52 See 4.7.3.
4.5.2.1 Factual Background

A Spanish citizen named González lodged a complaint with the Spanish Data Protection Agency (AEPD) against the daily newspaper La Vanguardia Ediciones SL and Google Spain and Google Inc.. Google Inc. has its seat in the USA. The complaint was founded on the existence of two pages from La Vanguardia Ediciones SL on which González name appears in connection with a real-estate auction linked to attachment proceedings for the recovery of social security debts.

4.5.2.2 Opinion on in the context of the activities

In the Google Spain case (C-131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González), the status of Google Spain is one of the main points of contention. While Google Inc. operates the search engine that display the pages of La Vanguardia Ediciones SL, Google Spain’s function is limited to promotion of advertising space on Google’s website.\(^\text{54}\) The court was tasked with, inter alia, determining whether the processing of personal data was carried out in the context of the activities of Google Spain.

Despite the claims made by Google, the court finds that the wording in article 4. (1). (a) does “not require the processing of personal data […] to be carried out ‘by’ the establishment concerned itself, but only that it be carried out ‘in the context of the activities’ of the establishment.”\(^\text{55}\)

The court also finds that the objectives of the DPD justifies an interpretation of the wording that is not restrictive.\(^\text{56}\)

The court concludes that González’s personal data is processed in the context of Google Spain’s activities. The court provides two rationales for this conclusion. Firstly, Google Inc. and Google Spain are “inextricably linked” as a result of the search engine being economically dependent on the advertising space, and the promotion of advertising space needing the search engine.\(^\text{57}\) Secondly, since the advertising and search results are displayed on the same page, the processing has sufficient context to the commercial advertising activities of Google Spain.\(^\text{58}\)

\(^{54}\) C-131/12, the Google Spain case, para. 43.

\(^{55}\) Ibid., para. 52.

\(^{56}\) Ibid., para. 53.

\(^{57}\) Ibid., para. 56.

\(^{58}\) Ibid., para. 57.
4.5.3 Update opinion by the WP
In response to the inclusion of inextricably linked as a new criterion in the requirement that the processing be carried out in the context of activities of an establishment, the WP saw fit to issue an update on its opinion from 2010. Although the Google Spain case concerned search engines, the WP confirms that the connecting factor utilized by the court is applicable to other business models. The court’s main focus is on the economic aspects of the business’ activities. The WP points out that the revenue gained from the Spanish advertisers was not necessarily used to maintain or improve the Spanish version of the search engine, demonstrating that “the necessary economic link […] may not have to be particularly direct to meet the criteria.”

4.5.4 Ramifications of the Google Spain case and subsequent opinion by the WP
The Google Spain case and its accompanying opinion by the WP had noticeable effect on the extraterritorial application of the DPD. The judgement was also further acknowledged by the CJEU in the Weltimmo case. The Google Spain case means that a processing operation does not need to be performed by an establishment in a member state for the DPD to apply to a controller. The DPD will be applicable to third country controllers who performs the processing outside the EU/EEA, so long as the personal data is processed in the context of an establishment, e.g. a subsidiary. If the processing operation had taken place on the territory of a member state, some may argue that submitting the processing to European data protection law, is the prerogative of the member state resulting from the territoriality principle. In the Google Spain case, the court accepts jurisdictional claims despite the lack of territorial connection. The DPD now regulates conduct that takes place outside the EU/EEA, which represents a significant increase in the extraterritorial scope of the DPD.

The Google Spain case represents a weakening of the connecting factor, but some semblance of connection with the territory is still contained in the requirement that the activities of a local establishment and the data processing activities must be inextricably linked. The connection seems to coincide with what Scott describes as “territorial extension.” This hybrid of the territoriality principle and extraterritoriality is used to describe legislation that depends on a relevant territorial connection, but where the actor that utilizes the law is required to take

59 WP 179 update, p. 5.
60 Ibid.
61 C-230/14, the Weltimmo case, para. 35.
into account conduct or circumstances abroad. Scott argues that this still is an expression of territorial jurisdiction, but also acknowledges that this is not an uncontroversial view.\textsuperscript{63}

I am also sceptical towards Scott’s jurisdictional category. While I will not dismiss it entirely, a category which labels the geographical irrelevance of the processing operation as an expression of territorial jurisdiction, is in my opinion being negligent of the actual consequences for third country controllers. In any case, the relatively weak requirements for entities to be inextricably linked through economic connection, is in my opinion not suitable to warrant an interpretation of the DPD article 4. (1). (a) as an expression of territorial extension, i.e. the territoriality principle. The connection required is simply too weak.

The court also indirectly seems to argue along the lines of the effects principle. The principle’s status and meaning is contested. In the report on extraterritorial jurisdiction by the international Bar association, the effects principle is defined as “the ability of a state to assert jurisdiction over certain conduct committed by foreigners outside its jurisdiction where the conduct has a certain effect within the state.”\textsuperscript{64} The Google Spain case can be read to indicate that the court found Google Inc.’s processing to effect González in such a way as to warrant applying the DPD. This interpretation is supported by the WP.\textsuperscript{65}

The effects principle is sometimes considered to be an extension of the principle of territoriality,\textsuperscript{66} substituting the location of the conduct with the location of the effects of the conduct. I find this argumentation disagreeable. The effects principle has indisputable extraterritorial consequences. Google’s processing operation may have affected González in Spain, but the processing operation itself took place in the USA. I suspect this argument is made because of the controversial nature of extraterritoriality.

\subsection*{4.6 Establishments on the territory of several member states}
Since the country of origin principle was rejected in the DPD, controllers can have multiple establishments in different member states. The DPD article 4. (1). (a) requires that establishments comply with the national data protection laws of the member state in which it is located. Recital 19 of the DPD explains that this addition is motivated by the possibility of circumvention of the data privacy rules. While this reasoning has merit, there are some unfortunate side effects of the requirement which are particularly problematic for controllers located in third countries.

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{63} Ibid., p. 91.
\item \textsuperscript{64} International Bar Association, (2009), p. 12.
\item \textsuperscript{65} WP 179 update, p. 5 – 6.
\item \textsuperscript{66} International Bar Association, (2009), p. 12.
\end{itemize}
\end{footnotesize}
4.6.1 Multiple national laws may be applicable

When each establishment located in a member state must be in compliance with the national data privacy laws of said member state, a controller may have to deal with multiple national laws. The DPD is a directive and leaves it up to the individual member state to implement its rules into national legislation. This has led to a divergence between the data protection rules in the member states. If the rules of the DPD was uniformly implemented across the EU/EEA, it would not matter which member states the controller had establishments in. The same data processing rules would apply to any data processing operation in this scenario.

As this is not the case, controllers located in third countries who wants to establish themselves in several member states are forced to contend with the national legislation of several member states of which it has potentially little to no knowledge of. This can further diminish the controller’s ability to predict its legal standing. The controller may also be forced to spend considerable amounts of time and money to map the data protection rules in each member state where an establishment is located.

As the Google Spain case has shown, the processing operation itself can be conducted in a third country. Situations can be envisaged where a controller is subject to multiple national data protection laws because various parts of a single processing operation are inextricably linked to multiple establishments. An example of this is a controller, who wants to conduct a performance review of its staff in an establishment located in member state A, collecting information about its employees, but storing the information in a server located in another branch in member state B for future use. This contributes to the already challenging task that the third country controller has in trying to predict its legal standing.

4.7 The use of equipment

The previous chapters have shown that by interpreting the various elements that comprise article 4. (1). (a), the DPD can have extraterritorial application. The connecting factors are relatively strong, although efforts by the WP and the CJEU, and my own arguments have weakened them to an extent. Article 4. (1). (c) allows for the application of the DPD with even less of a connection between the controller and a member state. A controller who does not have an establishment in a member state can still be subject to the DPD if equipment, situated on the territory, is used to process personal data. Recital 20 backs this up by asserting that processing perpetrated by a controller located in a third country must not stand in the way of the data protection rules in the DPD. There is an exception to the rule where the equipment is used solely for transit. The concept of equipment is not explained in the DPD. The Com-
mission has acknowledged that the use of equipment is not an easy criterion to operate, and that the criterion was highly criticized during the DPD’s inception.\textsuperscript{67}

4.7.1 The concept of making use of equipment

The lack of explanation of the concept of equipment is unfortunate for controllers located in third countries, particularly because the ability to predict their legal standing is reduced. The situation is further complicated by a change in phrasing from “means” in the amended proposal\textsuperscript{68} to equipment in the DPD. Words with equivalent meaning as means is used in many national laws implementing the DPD. Moerel points out that the drafters of the directive had physical objects in mind when using the word equipment,\textsuperscript{70} which is based on comments made in the Explanatory Memorandum about “terminals, questionnaires etc.”\textsuperscript{71} A purely semantic interpretation would probably yield the same result. This is further backed up by the requirement that the equipment must be “situated on the territory” of a member state. Means appears to encompass more than just physical objects.\textsuperscript{72} This will further muddle the legal standing of controllers located in third countries who may be subject to different national laws with different connecting factors.

The WP did not equate equipment with means until its opinion in 2010 and thus broadening the understanding of the criterion to include, inter alia, human presence.\textsuperscript{73} This broad interpretation makes the DPD applicable to a larger portion of controllers located in third countries, i.e. expanding the DPD’s extraterritorial scope.

4.7.2 Control over equipment

The connecting factor in the DPD article 4. (1). (c) is the equipment itself. The controller needs to “make use of” it. This entails some form of control over the equipment. The DPD is undoubtedly applicable to controllers who fully own the equipment being used to process the personal data. Questions arise where the equipment, e.g. a server, is owned by several entities or where the server is being rented by the controller. If such relations are rejected, this would invite the possibility of controllers actively engaging in co-ownership or leasing of equipment in order to circumvent the DPD. Considering that equipment is a weaker connecting factor than an establishment, it can be argued that the circumvention-argument does not hold the

\textsuperscript{67} COM(2003) 265 final, p. 17.
\textsuperscript{68} COM(92) 422 final - SYN 287, (p. 68).
\textsuperscript{69} Korff, (2002), p. 54.
\textsuperscript{70} Moerel, (2011b), p. 36.
\textsuperscript{71} COM(92) 422 final - SYN 287, Explanatory memorandum, p. 13.
\textsuperscript{72} Korff, (2002), p. 54.
\textsuperscript{73} WP 179, p. 20.
same power. In my opinion, it is less blameworthy to actively attempt to circumvent the DPD where the connection between the controller and the member state is less substantial.

The WP confirms in its 2010 opinion on applicable law that the controller does not need to exercise ownership or full control over the equipment. As no concrete requirements are presented, e.g. owner percentage etc., the assessment will have to be made on a case-by-case basis. Once again, the WP’s liberal interpretation gives the DPD wide extraterritorial scope.

4.7.3 Equipment is a weak connecting factor
The connecting factors in the DPD article 4 does not discriminate towards nationality. This is also true for the use of equipment. Situations can be envisaged where a controller, who is located in a third country, processes data of persons who are citizens of a third country and located there, using equipment located in a member state. The controller would then be subject to the DPD, and the persons are protected by the DPD. In this situation, the connection between the controller, persons and a member state is very limited. I find it more difficult to argue for the extraterritorial application of the DPD when the connection to a member state is weak, concomitantly it is presumably more disagreeable for an entity in a third country to submit itself to the law of state of which it has little connection to.

Over the last decade, technology has made major strides. This development has contributed to making equipment a weak connecting factor. An example can be found in the Google Search Warrant case (2:16-mj-01061-TJR) presided over by the District Court for The Eastern District of Pennsylvania. The case concerned whether Google was obligated to obey search warrants that requested copies of the user data from three google accounts stored abroad. Google’s refusal to provide the data was, inter alia, based on its inability to pinpoint the data’s exact location. Google’s files “may be broken into component parts, and different parts of a single file may be stored in different locations (and, accordingly, different countries) at the same time.”

Cloud services offers, inter alia, storage of data which often involves multiple servers located around the world. Cloud service providers may struggle to ascertain where the personal data is stored, or it may not be economically viable to keep track of the data’s location at all times. This can influence the controller’s ability to predict whether its operation is subject to the data privacy rules of the DPD, as the controller may be storing personal data on a server in a member state without its knowledge. The controller may also have multiple national data privacy

74 Ibid.
75 2:16-mj-01061-TJR, the Google Search Warrant case, p. 7.
laws applicable to its processing as parts of the same personal data may be located on servers in multiple member states. The discrepancies in data protection legislation between the different member states makes it difficult for the controller to predict its legal standing in this situation. It will also require the controller to map the data protection laws in each member state where it makes use of equipment, which seems harder to justify when the connecting factor is weak.

4.8 The problem with the WP’s opinions
The WP has been instrumental in interpreting and elaborating on the elements that constitute article 4, which in many cases have expanded the extraterritorial reach of the DPD. While this work should be appreciated by laymen and legal scholars alike, it highlights deficiencies in the DPD. In my opinion, there has been a lack of explanation of fundamental words and concepts in article 4 by the drafters of the DPD. This is, inter alia, apparent from the discrepancies between the member states implementation of article 4. Many of the opinions relevant to article 4 is made late in the lifespan of the DPD. A comprehensive opinion, in WP 179, about article 4 is issued almost 15 years after the DPD was finalized, despite discrepancies in its implementation being identified back in 2003 by the Commission. For controllers established in third countries, this lack of clarification is debilitating when trying to predict whether the DPD applies to them.

I find it questionable that so much of the content of article 4 is left up to the WP to define. While the opinions of the WP are often logical and elaborate, The WP does not have legislative power. The WP has advisory status and its opinions carry less weight than if, e.g. amendments was made to the DPD. The important interpretations made by the WP should, in my opinion, not be relegated to advisory opinions. This practice results in much of the content in article 4 not being located in the DPD itself. Controllers located in third countries who may already be struggling to deal with the DPD, now has an additional source of law that needs to be consulted in order to ascertain whether the DPD is applicable to them.

4.9 Preliminary concluding remarks
4.9.1 Procedure for determining the applicability
By rejecting the country of origin principle, article 4. (1). (a) can lead to the extraterritorial application of the DPD. Advocate General Villalón prescribes a “two-stage examination” in his opinion on the Weltimmo case. The first step is to ascertain whether the controller in

77 Opinion of Advocate General Cruz Villalón, para. 26.
question has an establishment on the territory of a member state. The efforts of CJEU in the Weltimmo case and the WP indicates a liberal understanding of what constitutes an establishment, which in my opinion can be further weakened to encompass establishments without human presence. The second step is to ascertain whether the personal data was processed in the context of the activities of the establishment. The Google Spain case clarified that the processing operation does not need to be performed by the establishment, or even in the member state itself.

If the controller does not have an establishment in a member state, but utilizes equipment situated on the territory of a member state, the DPD may still be applicable to the controller. This connecting factor has been highly criticised and can lead to situations where the DPD is applicable to third country controllers with very limited connection to a member state. The connecting factor has also fallen victim to the vast technological innovation over the last 25 years, making it less suitable in the current technological climate.

4.9.2 The EU’s territorial or extraterritorial jurisdiction
The extraterritorial application of the DPD does not fulfil the textbook example of extraterritoriality, where the legislator legislates outside its jurisdictional boundaries, effectively applying its laws to any third country it desires. The extraterritorial application of the DPD is always dependant on some form of connection between the member state and the controller. This is achieved by the connecting factors present in article 4. These connecting factors vary in terms of what connection is required between the member state and the controller, and how well they have adapted to technological developments.

This middle ground between the textbook example of extraterritoriality and regular territorial jurisdiction have led to some authors of law arguing that article 4 is not an expression of extraterritorial jurisdiction, e.g. territorial extension and the effects principle. Practicing extraterritorial jurisdiction is a controversial subject. It would be convenient to categorise the territorial scope of the DPD as simply an advanced form of territorial jurisdiction, to give the practice a semblance of traditional jurisdictional acceptance. In my opinion, this would be dishonest. In reality, the EU has given itself jurisdiction over people and entities located in third countries. Having an additional establishment in a member state or using equipment located in a member state does not change this fact. My view is not necessarily an endorsement of extraterritorial jurisdiction as a concept, but I struggle to accept these convenient categories as a convincing rejection of the EU’s extraterritorial jurisdictional practice.

4.9.3 Motivation behind the DPD’s extraterritorial application
The extraterritorial application of the DPD has been in the making for over 20 years. Although the DPD has had extraterritorial ramifications from its inception, the developments
over the last 7 years have greatly expanded its extraterritorial application. Some tendencies can be identified as the motivation behind this development, both in the DPD itself and in the opinions of the WP. The objective of the DPD can be observed in article 1 and consists of protecting natural persons right to privacy. Nowhere does it say that this right to privacy is limited to the citizens of a member state. On the contrary, recital 2 states that data processing systems must respect the right to privacy, regardless of nationality or residence. This can be interpreted to call for extraterritorial application of the DPD.

The internet has made the collection and transferal of personal data easy. The lack of physical borders on the internet means that personal data can be collected from anywhere in the world and transmitted to anyone located anywhere. If the data protection rules of the DPD is limited to the territory of its member states, it would be virtually impossible to protect the very people it sets out to protect. These technological developments may have exemplified the necessity for an instrument that can protect the natural persons in the face of new technology that does not adhere to the limitations of territorial boundaries.

The DPD article 1 also make reference to the “fundamental rights and freedoms of natural persons”. This is expanded upon in recital 10 with an acknowledgement of article 8 of the *ECHC* (European Convention on Human Rights). Article 8 contains, inter alia, the right to respect for private life. It is recognized that a right to data privacy is contained in the respect for private life. If the data protection rules of the DPD are viewed as protecting fundamental human rights, it would presumably be easier to argue for their extraterritorial application. The WP seems to argue along these lines in an attempt to justify the extraterritorial effects of the DPD article 4. (1). (c). Such a viewpoint can easily be translated to other parts of article 4 and may have contributed to the expansion of the DPD’s extraterritorial application.

---

78 WP 179, p. 24.
5 Extraterritorial scope of the General Data Protection Regulation

5.1 Introduction to the GDPR
A proposal for a new data protection instrument to succeed the DPD was released in 2012. This proposal was the result of multiple consultations with the interested parties and an impact assessment. In 2016 the GDPR entered into force. It shall apply from the 25th of May 2018.  

5.2 From directive to regulation
In its proposal for the GDPR, the Commission recognized the discrepancies in the implementation of the DPD between the different member states, and the unfortunate consequences this led to. In response to this, the new data protection rules are encoded in a regulation. In contrast to a directive, which leaves it up to each country to fulfil the goals it sets, a regulation is a binding instrument that must be applied in its entirety. This means that there is no room for differences between the member states data protection laws, save for the instances where they are given a margin for manoeuvre.

The diverging data protection laws of the member states under the DPD necessitates that each establishment in a member state complies with the national law of its location, inter alia, to avoid circumvention of the law. This is not a possibility under the GDPR. Third country controllers and processors will have to contend with just one set of rules. This will improve their ability to predict their legal standing. Presumably, there will also be less expenditure and time spent trying to clarify the content of European data protection law.

5.3 The broad scope of the GDPR
Like its predecessor, article 2 gives the GDPR a broad scope. There are some additions to the definitions of the concepts that make up article 2, e.g. genetic identifiers are now considered personal data and structuring is considered processing. While these changes may have impact within their particular fields, they do not substantially change the impact of the data pro-

---

79 GDPR. art. 99.
80 GDPR. recital 171.
83 GDPR. recital 10.
84 GDPR. art. 4. (1).
85 GDPR. art. 4. (2).
tection rules. As the GDPR retains its broad impact, European data protection law continues to effect swathes of different industries and actors.

5.4 Article 3 of the GDPR
Article 3 of the GDPR concerns the instrument’s territorial scope. Article 3 does not use the term extraterritorial, which I think can be attributed to the fact that the controversial nature of extraterritoriality has not changed much since the drafting of the DPD. Regardless of terminology, the following analysis will show that the drafters of the GDPR uses language that more overtly acknowledges the instrument’s extraterritorial application, than what was the case in the DPD.

5.5 Controller and processor as the subject
The controller remains as the subject of which data processing rules may apply. An addition in article 3 is the inclusion of processor’s as subjects that may have data protection rules applicable to them. In many cases, the controller itself, e.g. Google Inc. in the Google Spain case, performs the data processing in-house. If the controller is located in a third country and the processing takes place in a member state, it is often performed by e.g. a branch or subsidiary that fulfils the requirements of an establishment. In these cases, the addition of the processor as a subject has no consequences under the DPD, as the data protection rules would be applicable anyway.

Under the DPD, a situation can be envisaged where the controller hires a third party to perform processing services. As the processor has no organisational affiliation with the controller it is unlikely that it will fulfil the requirements of being an establishment. The controller would presumably not be in control of any equipment the processor uses in its data processing either. Consequently, a controller may circumvent data protection laws by outsourcing the processing operation. The WP considered the possibility that processors can be equipment and found that the broad definition of equipment would justify such an interpretation. The GDPR has abandoned equipment as a connecting factor, which has necessitated the inclusion of processors. By adding processor as a subject in article 3, the drafters have increased the reach of the GDPR and opened up for the possibility that processors located in third countries can have their activities regulated by European data protection law.

5.6 An establishment as a connecting factor
The GDPR retains “an establishment” as the primary connecting factor for controllers and processors in article 3. (1). The drafting of the GDPR would seem a perfect opportunity to

86 WP 179, p. 20.
define the requirement of an establishment more precisely. Instead, the same definition as in the DPD remain.\footnote{GDPR. recital 22.} In light of the clarifications made in the recent Weltimmo case, it is regrettable that this opportunity was not used, although the relatively short period of time between the case and the GDPR entering into force may have played a part in this omission. As there is currently no case law on the GDPR or any elaboration offered in the instrument, my argument about human presence should still be viable. Given the importance of an establishment as a connecting factor, third country controllers and processors would probably welcome further guidance on what constitutes an establishment in the GDPR itself.

The importance of an establishment as a connecting factor is also apparent in its rejection of a country of origin principle. Once again, it is left up to interpretation to extract this point. Some guidance can be found in article 4. (16) where a definition of “main establishment” is provided. If main establishment is used as a separate category, then an establishment must mean any establishment. This simplifies the interpretation, but it is unfortunate for third country controllers and processors with limited knowledge of the GDPR that this is not clearly stated. One could speculate whether the drafters perceived a clear rejection of the country of origin principle as being too blatant about the GDPR’s extraterritorial application.

5.7 **In the context of the activities**

The GDPR retains the processing requirement from the DPD in article 3. (1). The processing only needs to be done “in the context of the activities of an establishment”. As there are no changes in phrasing in the GDPR, the developments made in the Google Spain case and the updated opinion by the WP should be applicable. This is further evidenced by a new addition in the article. The GDPR applies to processing “regardless of whether the processing takes place in the union or not.” The nature of case law means that it can be overturned. By codifying some of the judgement in the Google Spain case, the extraterritorial application of the GDPR is formalised and protected from being overturned by the CJEU. The drafters should be complimented for this addition, which serves to clarify aspects of article 3, to the benefit of third country controllers and processors trying to predict their legal standing. This is one example of the more overtly acknowledgement of extraterritorial application in the GDPR.

I find it surprising that only parts of the Google Spain case were codified in article 3. The case introduced a new criterion where the activities of a local establishment and the data processing activities must be inextricably linked. This seems too important a criterion to be left silently embedded in article 3, particularly when the WP has explicitly recognized it in its updated opinion on applicable law. The gains made from the addition of the insignificance of
the processing operation’s geographical location is somewhat diminished as third country controllers and processors must consult the Google Spain case or the WP’s opinion directly to extract this criterion. The omission of inextricably linked could be understood as intentional by the drafters. In which case, the GDPR will presumably have an even wider extraterritorial scope, considering that the processing activities and the establishment does not need to be inextricably linked. The commission is silent on the issue in its proposal and there is no case law to consult. Barring any rejection of the criterion in future, I am inclined to believe that article 3. (1) maintains the criterion proposed in the Google Spain case.

5.8 The targeting approach
One of the biggest changes in the GDPR comes in the form of article 3. (2), where the data protection rules are applicable to controllers who process personal data in relation to the offering of goods and services or the monitoring of natural persons. The rules are only applicable to controllers and processors “not established in the union”, which solidifies the GDPR’s extraterritorial application.

5.8.1 Targeting
The GDPR utilizes what is known as a targeting approach. Targeting means that a subject directs its activity, whether it is business-related or otherwise, towards other subjects. The targeting approach can be derived from recital 23 of the GDPR where the question of the offering of goods and services is really a question of whether controllers and processors “envisages offering services to data subjects”. This phrasing bears resemblance to statements made in the joined consumer protection cases; the Pammer Alpenhof case (Peter Pammer v Reederei Karl Schlüter GmbH & Co KG (C-585/08), Hotel Alpenhof GesmbH v Oliver Heller (C-144/09)) where the CJEU found that a trader has “directed” its activity towards a member state when it is “envisaging doing business with consumers”. Pammer Alpenhof is widely recognized as having developed the targeting test. Advocate General Jääskinen shares the view that the rules in the GDPR is an expression of the targeting approach in his opinion on the Google Spain case.

5.8.2 The offering of goods and services
Third country controllers and processors who target data subjects in the union through the offering of goods and services will have to obey the GDPR. The offering of goods and services may appear like an overly broad criterion. The internet has made the world its marketplace, with many businesses offering worldwide delivery of goods and services. These tech-

---

88 C-585/08 and C-144/09, the Pammer Alpenhof case, para. 92.
90 Opinion of Advocate General Jääskinen, para. 56.
nological developments will potentially lead to the GDPR being applicable to vast amounts of businesses with a potentially weak connection to the EU/EEA. The drafters have attempted to limit the criterion in recital 23 by exemplifying what is, and is not considered targeting. These exemplifications seem to be mainly aimed at goods and services offered over the internet.

Recital 23 rejects the accessibility of a website, e-mail or other contact details as sufficient to establish that the controller or processor has targeted data subjects in the union. Barring any censorship by the state, websites are accessible from anywhere in the world. If accessibility was sufficient, the GDPR would be applicable to any business operating on the internet through a website. Any extraterritorial application of the GDPR is hard to justify when the connection between a member state and a business is nearly non-existent. A similar argument can be made about the accessibility of e-mails and other contact details. The internet has made connecting with businesses independent of geographical location.

Recital 23 clarifies that businesses cannot avoid the GDPR by utilizing their native tongue in their offering of goods and services, but the use of the language of a member state can be an indication of targeting. The use of member state language as a sign of a proper connection between a member state and a controller or processor can be traced back to the Weltimmo case, where the CJEU seems to have emphasized that Weltimmo’s property websites were written exclusively in Hungarian. Additional elements that may indicate targeting is the use of a member state currency and mentioning customers or users located in the union.

Article 3. (2). (a) is applicable to the offering of goods regardless of whether payment is required. Business on the internet is increasingly being conducted free of charge for the consumer. Facebook is an example of a business that offers its services free of charge and processes vast amounts of personal data. These businesses have found other ways to monetize their offerings through, e.g. ad revenue. Often times, these businesses are responsible for more processing of personal data than businesses requiring payment, i.e. if you are not paying, you are the product. Limiting the applicability of the GDPR to offerings that demands payment would have severely compromised the GDPR’s ability to protect the right to protection of personal data.

5.8.3 The monitoring of behaviour
Article 3. (2). (b) makes the GDPR applicable to controllers and processors who monitor the behaviour of data subjects. In addition to tracking itself, subsequent use of personal data can be considered monitoring. This includes profiling where the goal is to, inter alia, predict per-

---

91 C-230/14, the Weltimmo case, para. 16.
sonal preference, behaviours and attitudes. Facebook proves a good example again, as it allows for advertisers to target people based on demographic, geography, interests and behaviour. The offering requires intimate knowledge of data subjects using Facebook and will presumably be considered profiling. Facebook would be caught by both (a) and (b) in article 3, which illustrates that these alternative connecting factors have the ability to overlap.

The drafters have limited the monitoring alternative to “behaviour that takes place within the union”. I find this limitation surprising. If a person located in Norway use Facebook and his interests are monitored, where does his behaviour take place? Is it in the place where the server that handles traffic for Facebook from Norway is located or is it the place where the computer the person is using is located, i.e. Norway? The Google Search Warrant case demonstrated that geographical location is difficult or even impossible to determine on the internet. If the motivation behind the phrasing was to avoid situations where the data subject is located in third countries, but is still afforded protection by the GDPR, this is already accomplished by the stipulation in article 3. (2) that the GDPR only applies data subjects in the union.

5.9 Abandoning equipment as a connecting factor

The drafters of the GDPR chose not to include equipment as a connecting factor. The criterion was highly criticized and several problems with its application has been identified. Recognizing these deficiencies, the WP argued for the “targeting of individuals” as an additional connecting factor. The decision by the drafters to do away with equipment as a connecting factor completely may be motivated by a belief that article 3. (2) of the GDPR will catch controllers and processors that use equipment in a member state. In most cases, this seems to be true. If a third country cloud service provider uses a server in a member state to store its customers data, the GDPR will presumably apply as its services have been offered to the data subjects in a member state. Situations where the use of equipment is not covered by either alternative in article 3. (2), can possibly be caught by article 3. (1) if my argument concerning human presence in establishments is accepted.

Article 3 of the DPD is nationality neutral, which had the unfortunate effect of making the DPD applicable to a third country controller who processed personal data about a natural person who was not located in a member state. This made equipment a weak connecting factor in some instances. It seems that the drafters have taken the criticism to heart. Article 3. (2) of the

---

92 GDPR. recital 24.
94 See 4.7.3.
95 WP 179, p. 24.
GDPR only applies to data subjects “who are in the union”. This is a rare example of the GDPR having been limited in its extraterritorial application, compared to the DPD.

While this addition has alleviated the connection problem, it may be at odds with the objectives of the GDPR. The protection of fundamental rights and freedoms of natural persons are one of several objectives of both the DPD and the GDPR, and both instruments make mention of ECHR article 8.6697 Elevating the content of the GDPR to fundamental and human rights, but simultaneously limiting the protection afforded to natural persons in the union seems counter intuitive. This reasoning leads to a whole host of other questions about, e.g. the reach of fundamental rights and the universality of human rights, all of which are too extensive to be discussed further in this master thesis. It must be sufficient to point out this logical discrepancy and hope that it is addressed in the future.

5.10 The effects principle
I find attempts to brand the effects principle as an extension of the territoriality principle disagreeable. Regardless of whether the principle is categorized as territorial or extraterritorial, the undeniable extraterritorial effects of the principle make it relevant in an analysis of the GDPR’s extraterritoriality.

I argued that the Google Spain case could be interpreted to usher in the effects principle in European data privacy law. The targeting approach in the GDPR can be construed as an expression of the effects principle. This view is supported by the WP in its updated opinion on applicable law where it is stated that the GDPR relies “more explicitly […] on the ‘effects principle’ to complement the ‘territoriality principle’”.98 The offering of goods and services and the monitoring of behaviour are activities that can impact data subjects in the union. The focus has shifted from the location of the equipment, to the location of the effects of the activities. As a result, the GDPR will apply to controllers and processors when they pursue activities that the drafters deem as having the effect required to justify the application.

The effects principle can also be observed in article 3. (1), though not to the same extent as in (2). By keeping an establishment as a connecting factor, third country controllers or processors are still required to have some form of territorial connection with a member state for the GDPR to apply. Considering that the GDPR has adopted the understanding of processing proposed in the Google Spain case, the connecting factor no longer relies exclusively on a territo-

---

66 DPD. recital 10
67 GDPR. recital 1.
98 WP 179 update, p. 5 – 6.
rial connection. The processing, can take place outside the EU/EEA, but the effects of the processing is felt by data subjects in the EU/EEA.

5.11 No physical presence on the territory of a member state
The DPD operate with connecting factors that establish a physical connection with a member state. If a controller has an establishment or equipment physically located in a member state, the DPD may be applicable. Even with the relatively modest requirements for there to be an establishment introduced in the Weltimmo case, and my argument about human presence, there must be some form of physical presence in the member state. By abandoning equipment as a connecting factor, the GDPR may be applicable to controllers and processors with no physical presence in a member state. This represents a broadening of the extraterritorial scope of the GDPR, which potentially leads to more controllers and processors having to obey European data protection law.

It can be argued that physical presence on the territory of a member state is an antiquated way of assessing the strength of the connection to a controller or processor. The internet has allowed businesses to process personal data of people located almost anywhere in the world. Some businesses operate exclusively through the internet without any physical place of business. This type business brings into question whether it possible to fulfil the objectives contained in article 1 of the GDPR if the connection is required to have physical manifestations in a member state. The effects principle which permeates the targeting approach may appease some concern about connection when, in lieu of a physical connection, the activities of the controller or processor must affect the data subjects in the EU/EEA. Technological advances have allowed personal data to be processed without a physical connection to a territory. The connecting factors in article 3. (2). (a) and (b) of the GDPR may be better suited for the future, as they do not rely on a physical connection to the EU/EEA.

5.12 The subjective- or outcome-based targeting approach
The litmus test when assessing potential targeting, is whether the controller or processor “envisages” offering services to data subjects.99 The definition of envisage is to “contemplate or conceive of as a possibility or a desirable future event”.100 This means that controllers and processors must, as a bare minimum, be consciously aware that they are offering services to data subjects in a member state. The subjective nature is further emphasised by the use of “intention” in recital 23. The definition of intention is “a thing intended; an aim or plan”.101 This would require the controller or processor to make a concerted effort to target data subjects in a

99 See 5.8.1.
member state. The discrepancy between the words leads to a discrepancy in the concept of targeting. A cloud service provider can be aware that their services are available to data subjects in a member state, without have singled out the market with the intention to offer their services.

Svantesson has criticized the subjective nature of the targeting approach, which he sees as requiring a “conscious decision” from the controller or processor. He argues that the targeting approach should abandon the subjective elements and instead focus on the “outcome” of activities of a controller or processor.\(^\text{102}\) By focusing on subjective aspects, situations can occur where data subjects are being deprived of their protection under the GDPR, but are still having their personal data processed. The consequences for the data subjects remains the same, but the controller or processor has avoided the restrictions of the GDPR owing to its ignorance or lack of intention. This can incentivise circumvention through deliberate unawareness. If Svantesson’s outcome argument is applied, the GDPR would be applicable where the data subjects have been targeted, regardless of knowledge or intention.

I share Svantesson’s opinion that an outcome-based targeting approach is a better solution than a subjective-based targeting approach. The GDPR’s recital seems at odds with this approach. In my opinion, article 3. (2) can be interpreted to allow for an outcome-based approach through the effects principle. The principle is intended to be used as the basis for jurisdictional claims and requires there to be a certain effect within a territory that justifies the exertion of jurisdiction over third country subjects. If a controller, regardless of intention, e.g. processes personal data in connection with the sale of goods to a data subject in a member state, there is a tangible effect in the territory. The jurisdictional claim is justified. If the controller does not sell any goods to data subjects in the territory, no data processing takes place. A jurisdictional claim cannot be justified. The effects principle necessitates that the third country subject’s activities have the required effect, i.e. the outcome approach goes hand in hand with the effects principle.

Regardless of which approach is taken towards targeting or whether they can coexist, it is evident that this area needs clarification. The uncertainties about the terminology in recital 23 and the subjective elements as a whole, makes it difficult for third country controllers and processors to predict their legal standing. Considering the central role the targeting approach plays in the extraterritorial scope of the GDPR, it is unfortunate that third country controllers or processors potentially will have to consult secondary sources for this clarification.

---

5.13 Preliminary concluding remarks

5.13.1 Procedure for determining the applicability
The GDPR retains the two-stage examination of the DPD. It must be ascertained whether the controller or processor has an establishment on the territory of a member state, and whether the personal data was processed in the context of the activities of the establishment. The second step has accommodated the Google Spain case in its phrasing, which means that the GDPR is applicable even if the processing itself takes place outside the EU/EEA. The abandonment of the connecting factor equipment represents the biggest change from the DPD. In its place, the targeting approach has been implemented. If a controller or processor offers goods or services, or monitors data subjects in the union, the GDPR may be applicable to their activities.

5.13.2 A missed opportunity
The drafters of the GDPR has implemented some of the interpretations and lessons that has been made during the life of the DPD. The irrelevance of the geographical location of a processing operation is codified in the text, though the accompanying requirement that the activities of the controller and its establishment must be inextricably linked is inexplicably missing. Equipment has been abandoned as a connecting factor because of modern technology making it unsuitable, and the unsatisfactory consequences it can result in. My analysis has also uncovered that there are multiple concepts that need further clarification. Opinions by the WP and the Weltimmo case have both clarified aspects of what constitutes an establishment, yet the GDPR retains the same definition as the DPD. Recital 23 of the GDPR uses terminology that makes it unclear what type of subjective elements are relevant when determining if a controller or processor has engaged in targeting.

I am cautious to criticize the choices made by the drafters, as we do not know how the GDPR will function in practice, but I feel that there are some missed opportunities to clarify important aspects of the instrument. The importance that the territorial scope has for the legal standing of third country controllers and processors, who have little or no knowledge of the jurisprudence of the EU, should justify an approach that elaborates on the concepts of article 3 as much as possible. If third country controllers and processors are forced to conduct extensive and costly research into legal sources outside the text of the GDPR, the willingness to engage with the EU, business related or otherwise, may be diminished.

5.13.3 Motivation behind the GDPR’s extraterritorial application
The motivation behind the continued extraterritorial application of European data protection law under the GDPR seems to still be rooted in the desire to protect the fundamental right of protection of personal data. Article 1 of the GDPR has retained the objectives of the DPD. In
its explanatory memorandum, the Commission identifies the rapid technological developments as being responsible for new challenges for the protection of personal data.\textsuperscript{103} The targeting approach, which incorporates new connecting factors that are better suited for the present and potentially future technological situation, can be seen as a response to these challenges.

The Commission also recognises the importance of trust in the online environment and the economic and innovative consequences lack of trust has.\textsuperscript{104} The internet transcends state borders, and many businesses utilize the internet to sell their wares or services. If data subjects cannot rely on third country businesses to adequately protect their data, this may lead to the undesirable consequences identified by the Commission. The targeting approach seems to be designed to catch business conducted over the internet. The EU has traditionally focused on the well-being of the internal market in its legislation. The GDPR is no exception.\textsuperscript{105} I believe that the Commission’s rationales and resulting extraterritorial application of the GDPR represents an acknowledgement of the fact that the European economy does not function in a vacuum. Consequently, the EU’s internal market has motivated the drafters to expand upon the extraterritorial application of the GDPR.

\textsuperscript{104} Ibid., p. 1 – 2.
\textsuperscript{105} GDPR. recital 13.
6 Extraterritorial implications of the transfer of personal data to third countries

6.1 Domestic measures with extraterritorial implications

The previous chapters have demonstrated that the EU is practicing extraterritorial jurisdiction through its data protection instruments. Article 4 of the DPD and article 3 of the GDPR are not the only examples of the extraterritorial application of European data protection law. Laws can be territorial in nature, i.e. providing rights and obligations for subjects within its territory, but still have effect outside the territory of the state.106

6.2 Transfer of personal data to third countries under the DPD

Article 25. (1) of the DPD requires third countries to “ensure an adequate level of protection” if they are to receive personal data from a member state. Article 25. (2) prescribes an extensive adequacy evaluation where “all the circumstances surrounding the data processing” shall be assessed. If a third country does not have an adequate level of protection, transfer of personal data is prohibited.107 Article 26 allows for derogation from article 25 in several instances, e.g. where the data subject has given consent, the transfer is necessary to protect the data subject’s vital interest or where the controller in the third country provides appropriate safeguards.

In the context of territorial laws with extraterritorial implication, the level of protection required to be adequate is of greater interest than the rules themselves. The level of adequacy impacts the level of extraterritorial implication. If a third country is required to have rules with an identical degree of protection as the DPD, the EU would indirectly be giving the DPD extraterritorial application. If a third country is allowed to have a diverging degree of protection, but still being allowed to receive personal data from the EU, the rules would be more akin to recommendations, with far less extraterritorial impact.

In its Working Document on articles 25 and 26, the WP introduces “minimum requirements” for protection to be considered adequate. The minimum requirements consists of basic data protection principles, but does not encompass the DPD in its entirety.108 This can be interpreted to allow third countries some leeway in their data protection rules. Recital 60 of the DPD is seemingly contradictory to the WP’s opinion, by requiring that third countries must be in “full

---

106 See 2.2.
107 DPD. recital 57.
108 WP 12, p. 5 – 7.
compliance” with the data protection laws of the member states for any transfer to take place. These conflicting sources makes it difficult to determine the level of protection required.

The SHA (Safe Harbour agreement) was brokered with the USA in response to article 25 and 26 and is considered to ensure an adequate level of protection for the transfer of personal data.\textsuperscript{109} Bygrave has pointed out that the data protection principles of the SHA are less stringent than their DPD counterparts.\textsuperscript{110} This indicates that an identical protection to the DPD is not required for the protection to be adequate. I am more cautious about emphasising this divergence, as an estimated 120 billion dollars in trade was at stake if no agreement could be made.\textsuperscript{111} Additionally, the USA is a global superpower, which presumably gave it a stronger bargaining position to influence the level of protection in the agreement. Heisenberg further confirms my scepticism by commenting that the parties “wanted to give the appearance of protecting Europeans’ privacy, but whether or not it was actually fully protected was relatively unimportant to both.”\textsuperscript{112}

In 2015, the CJEU declared the SHA invalid in the \textit{Schrems case} (Case C-362/14 Maximillian Schrems v Data Protection Commissioner (joined by Digital Rights Ireland Ltd)). The case concerned Facebooks transferral of personal data from an EU citizen to the USA. The plaintiff claimed that the USA did not offer sufficient protection against surveillance by public authorities. The CJEU interpreted what could be considered adequate in relation to article 25 of the DPD.

“the term ‘adequate level of protection’ must be understood as requiring the third country in fact to ensure [...] a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union”.\textsuperscript{113}

The CJEU does not elaborate further on what can be considered essentially equivalent protection, but it seems far removed from the minimum requirements proposed by the WP. From a purely semantical interpretation, it is my opinion that essentially equivalent means that the third country legislation does not have to mirror the DPD exactly, but it must contain the same level of protection.

\textbf{6.3 Transfer of personal data to third countries under the GDPR}

The GDPR retains the requirement that third countries must have an adequate level of protection in article 45. (1). Personal data can be transferred where an “adequacy decision” has been

\textsuperscript{109} Commission Decision 2000/520/EC, art. 1.
\textsuperscript{111} Heisenberg, (2005), p. 78.
\textsuperscript{112} Ibid., p. 160.
\textsuperscript{113} C-362/14, the Schrems Case, para. 73.
made by the Commission. There are multiple examples of elements that are particularly important when assessing the adequacy of third country legislation in article 45. (2). a – c. The GDPR contains more elaborate rules on the transfer of personal data where appropriate safeguards, e.g. binding corporate rules,\textsuperscript{114} are provided by the controller,\textsuperscript{115} than the DPD. There are also multiple derogations from the adequacy requirement.\textsuperscript{116} The GDPR elaborates on the rules in the DPD and introduces some new elements, but the most important question, in relation to the extraterritorial implication, remains what level of protection is adequate.

By keeping the rather vague requirement of an adequate level of protection in the GDPR, uncertainties for third country controllers and processors will presumably remain. Recital 104 adopts the interpretation made by the CJEU in the Schrems case that the third country protection needs to be essentially equivalent to the protection in the EU/EEA. The interpretation that I have offered means that mostly semantical and structural differences between the protection laws is accepted. It seems like a missed opportunity that the drafters did not elaborate on this requirement in the GDPR. The lack of a concrete evaluation of the data protection laws of the USA in the Schrems case means that the meaning of essentially equivalent remains somewhat elusive in the GDPR. Hopefully, a thorough assessment will be conducted in a future case that illuminates the requirement.

6.4 Extraterritorial implication of the DPD and the GDPR

Article 25 and 26 of the DPD has been the subject of considerable controversy in some third countries, particularly in the USA.\textsuperscript{117} This controversy will probably remain with the rules in the GDPR. The SHA highlights the extraterritorial implications of the rules. Regardless of the actual level of protection the SHA provides compared to the DPD, it demonstrates that European data protection laws and principles can influence law in a third country. The consequences of these rules are comparable to the consequences of article 4 of the DPD and article 3 of GDPR.

The difference from practicing extraterritorial jurisdiction is the apparent voluntary adoption by the USA, but how voluntary is this adoption? When billions of dollars are at stake, even a superpower like the USA will feel the consequences of a ban on the transfer of personal data. Smaller third countries with a weaker bargaining position will probably feel even more pressure to adopt adequate data protection rules. If the adoption is not voluntary, the rules in the

\textsuperscript{114} GDPR. art. 47.
\textsuperscript{115} GDPR. art. 46.
\textsuperscript{116} GDPR. art. 49.
\textsuperscript{117} Bygrave (2014) p. 194.
DPD and the GDPR share more similarities with extraterritorial rather than territorial legislation.

After the Schrems case and its adoption by the GDPR, a third country needs to have data protection laws that are essentially equivalent to the laws in the EU/EEA. If my interpretation corresponds with the CJEU and GDPR’s drafters, a third country needs to implement the GDPR in its entirety. If the requirement of adequacy only entailed that third countries fulfilled the minimum requirements proposed by the WP, the extraterritorial implication of the DPD and GDPR would be subdued. By giving a third country an all or nothing ultimatum, the rules more closely resemble an expression of extraterritorial jurisdiction.

The Google Search Warrant case has shown that the exact location of data can be problematic to pinpoint.\footnote{118 See 4.7.3.} It may be difficult for a controller or processor to know where personal data is headed. If a server is operated by a branch of a third country controller in a member state, will data being transferred to this server qualify as transfer to a third country? The third country controller may be uncertain about the exact location itself, as data may be split up and stored in multiple locations. This illustrates once again that using the location of personal data as the foundation for rights and obligations in data privacy law, may not be the best or most accurate criteria.

By limiting the transfer of personal data to third countries, the EU is in essence giving its data protection laws extraterritorial application without having to practice extraterritorial jurisdiction. This backdoor into extraterritoriality is less controversial than the extraterritoriality observed in, e.g. article 3 of the GDPR, as the EU is formally practicing territorial jurisdiction. This combination of territorial and extraterritorial application of law is dependent on a position of power. If the third country stands to lose income or other benefits, there is an incentive to adopt the legislation. It can be argued that this practice resembles extortion.

\section*{6.5 Preliminary concluding remarks}

\subsection*{6.5.1 Transferring personal data to third countries}

The extraterritoriality of the DPD and GDPR is not limited to situations where the EU is practicing extraterritorial jurisdiction. The transfer of personal data to a third country is reliant on their data protection law being adequate, i.e. being essentially equivalent to the EU’s laws. This is a domestic measure with extraterritorial implications. The EU is a powerful conglomerate of nations that incentivises adoption of the legislation. Articles 44 – 49 in the GDPR
provides some additions, but is fundamentally a more elaborate continuation of the rules in the DPD. The extraterritorial implications these rules have had can be observed in, inter alia, the SHA. With the introduction of the SHA’s successor, the “Privacy Shield”, in 2016, the rules will presumably continue to play a key role in the extraterritoriality of European data protection law.

6.5.2 Motivation behind the rules

It seems likely that the motivation behind the rules in the DPD and the GDPR is the protection of the data subjects in the EU/EEA. The EU has enacted the most ambitious data privacy laws in the field, which means that any transfer of personal data to third countries represents a risk to the data subjects. By limiting the possibility to transfer personal data, the EU ensures that the data subjects are afforded protection outside their own territory. The status of data protection law as a fundamental right can be a justification for the protection of data subjects outside the EU/EEA.

Technological developments, like the internet, has simplified the transfer of personal data, regardless of state borders. Business being conducted on the internet almost invariably involves the transfer of personal data. The economic importance of the flow of personal data to third countries is recognized in recital 56 of the DPD and recital 101 of the GDPR. Despite the financial gains, the drafters favour the protection of data subjects. When technology allows for personal data to be effortlessly transferred across state borders, the limitations on transferral seems more easily justified.
7 Concluding remarks

This master thesis has shown that the DPD and the GDPR can be applicable outside the territory of the EU/EEA. Neither instrument acknowledges its extraterritorial application explicitly, but the GDPR uses terminology that is more overtly extraterritorial. This exemplifies the controversial nature of extraterritoriality. Attempts have been made to designate principles that have undisputable extraterritorial effects as extensions of the territorial principle. I find these arguments unconvincing. Courts and authors of law have more recently accepted the existence, and in some cases encouraged the use, of extraterritorial jurisdiction. By covering the extraterritorial scope of the GDPR in a veil of territoriality, third country controllers and processors have a needlessly challenging task trying to predict their legal standing.

Both the DPD and GDPR have a broad scope, with some additions in the GDPR, e.g. genetic identifiers, serving to increase its scope slightly. The extraterritorial application of the instruments means that a vast number of different industries and actors that comes into contact with European personal data are caught by the instruments. The scope of the GDPR is also increased through the addition of processors as subjects that can be caught by its data protection rules. This addition discourages circumvention of its rules by controllers who outsource their processing operation.

The DPD has been plagued with diverging implementation of its rules in the member states. This has compromised third country controllers ability to predict their legal standing, as knowledge about a multitude of deviating laws is required. Further complication arises for controllers who have multiple establishments in different member states, as each establishment needs to comply with the legislation of its location. Being a regulation, the GDPR leaves little room for divergence in its implementation. Consequently, third country controllers and processors only need to contend with one set of rules.

Both the DPD and the GDPR utilize the two-stage examination. The connecting factor of an establishment rejects the country of origin principle, which is the basis for the extraterritorial application the instruments. The interpretations made in the Weltimmo case have resulted in an understanding of what is considered an establishment in the context of the DPD that is not strict. I have proposed a further weakening of the connecting factor by rejecting a requirement of human presence in the DPD. This argument will solve situations in the GDPR where the use of equipment is not covered by any of the alternatives under the targeting approach.

The GDPR differs from the DPD by making the geographical location of the processing operation irrelevant. This addition stems from the Google Spain case which concerned the DPD, but the judgement fell late in the instrument’s lifespan and will presumably have a bigger im-
pact by being codified in the GDPR. By implementing this clarification directly into the text of the GDPR, third country controllers and processors can assess their legal standing without having to consult case law or the opinions of advisory entities that are less accessible.

The GDPR has abandoned equipment as a connecting factor and substituted it with the targeting approach. The GDPR is applicable controllers and processors who offers goods and services in the union or monitors the behaviour of data subjects in the union. The extraterritorial ramifications of this change are massive, considering the amount of business being conducted over the internet. The change in connecting factors is indicative of a new reliance on the effects principle to justify extraterritorial application of European data protection law.

The GDPR has abandoned equipment as a connecting factor and substituted it with the targeting approach. The GDPR is applicable controllers and processors who offers goods and services in the union or monitors the behaviour of data subjects in the union. The extraterritorial ramifications of this change are massive, considering the amount of business being conducted over the internet. The change in connecting factors is indicative of a new reliance on the effects principle to justify extraterritorial application of European data protection law.

The data protection rules of the instruments are also effecting countries outside the EU/EEA through limitations on the transfer of personal data to third countries with an inadequate protection level. The rules in the GDPR is a more elaborate continuation of the rules in the DPD, with some new additions. This continuation means that the European data protection law continues to influence third countries without the EU having to engage in extraterritorial jurisdiction. This backdoor into extraterritoriality may become more popular in data protection law and other fields of law, if extraterritorial jurisdiction remains controversial and disputed.

The changes in the extraterritorial application from the DPD to the GDPR is characterized by the weakening of the connecting factors. The irrelevance of the geographical location of the processing operation and the applicability of the GDPR to controllers and processors, despite having no physical presence in the EU/EEA, are examples of this weakening. This has made it easier for controllers and processors to be caught by the data protection rules of the GDPR. Consequently, the extraterritorial scope of the European data protection law has increased. To which degree these changes will affect third country controllers and processors in practice remains to be seen, but businesses who conducts their business over the internet appears to be the ones most heavily affected.

The motivation behind these changes seems to be rooted in a desire to protect the data subjects against the technological developments that have facilitated an explosion in the processing of personal data. In order to increase the extraterritorial scope of data protection law, the Commission, the CJEU and the WP all justify their opinions and interpretations by arguing that data protection is part of the fundamental rights and freedoms of natural persons. The protective motivation is commendable, but it raises question about where to draw the line for extraterritorial jurisdiction. I believe that the EU will continue to expand the scope of its data protection laws in response to technological innovations that facilitates data processing, and other threats towards personal data. In doing so, the EU will remain the leading provider of data protection law and principles for other states to imitate or adopt.
Bibliography

Literature:


<table>
<thead>
<tr>
<th>Author</th>
<th>Year</th>
<th>Source</th>
</tr>
</thead>
</table>
### Laws, opinions, reports, proposals and decisions:

<table>
<thead>
<tr>
<th>Reference</th>
<th>Description</th>
<th>Publication Date</th>
<th>Access URL</th>
</tr>
</thead>
</table>


<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
</table>


Case law:

C-366/10, the Air Transport Association of America case

Case 168/84, the Berkholz case

BFH II R 12/92, the German Pipeline case
Bundesfinanzhof. BFH II R 12/92, 1996. 

2:16-mj-01061-TJR, the Google Search Warrant case

C-131/12, the Google Spain case
Court of Justice of the European Union. C-131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, ECLI:EU:C:2014:317. 

C-585/08 and C-144/09, the Pammer Alpenhof case
Court of Justice of the European Union. Joined cases: (C-585/08) and (C-144/09)1, Peter Pammer v Reederei Karl Schlüter GmbH & Co. KG and and Hotel Alpenhof GesmbH v Oliver Heller, ECLI:EU:C:2010:740. 
http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30d6f68cc34b9c8447799f3ce14d7192d8dd.e34KaxiLe3qMb40Rch0SaxyMch10?text=&docid=83437&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=755421 [cited 24.11.2017].
C-362/14, the Schrems Case

Court of Justice of the European Union. C-362/14, Maximillian Schrems v Data Protection Commissioner (joined by Digital Rights Ireland Ltd), ECLI:EU:C:2015:650.


SHF II 1224/97, the Swiss Server case


C-230/14, the Weltimmo case

Court of Justice of the European Union. C-230/14, Weltimmo s. r. o. v Nemzeti Adatvédelmi és Információszabadság Hatóság, ECLI:EU:C:2015:639.