Privacy Power Europe

Protecting others by protecting ourselves

Reinder Flaton
0942251
reinderflaton@gmail.com
Leiden University
July 2015
Word count (excluding footnotes and references): 19991
Total word count: 23930

0 Table of contents

1 Introduction

On January 25th 2012, a General Data Protection Regulation (GDPR) was proposed as an extended reform of the currently applicable 1995 Data Protection Directive (DPD). A regulation rather than a directive, the reform will entail enhanced scope for uniform data protection standards as composed by the European Union (EU). Its application, however, is bounded by territorial limitations. EU regulation has direct effect only within the EU itself. Even so, EU regulation does *affect* third countries and foreign commercial enterprises. Data transfers are done on a global scale and are impervious to man-made geographical borders. Attempts to regulate them may therefore lead to jurisdictional overlaps.

This paper focuses on the EU using its power to change standards abroad. This is done in light of the Normative Power Europe (NPE) concept. NPE is a particular perspective on the EU's international role and its influence on affairs beyond its borders. From this perspective, the EU promotes and spreads its norms to third countries or other external entities. When it comes to privacy and data protection standards, the EU seems to be doing exactly this. In what follows it should become clear if this is accurate. The objective is to find out to what extent the EU is a normative power in the area of privacy and data protection.[1]

[1] I want to thank Jan Oster for helpful suggestions; Edward Snowden for giving me the inspiration to write about this topic; and Dennie Oude Nijhuis for convincing me to pursue this Master. I also thank my family, friends and of course my girlfriend simply for being alive.

2 Normative Power Europe

The term *Normative Power Europe* (NPE) was first used by Ian Manners (2002) to distinguish the power the European Union wields on the international stage from that of other – more traditional – great powers of the past and present. Hence, the assumption is that the EU does things differently; differently than, say, the United States, which tends to use a more diverse package of powers, including its military strength. Military strength is something that the EU lacks, forcing it, or 'enabling it', to exert its influence in different ways. Of course, its component parts, the Member States, have various degrees of military capabilities, but, despite the existence of the CSDP, the EU does not have much control over them. What it does have control over, however, is its single market – the largest market in the world. The EU has the power to develop and enforce rules, which participants in the single market are obliged to comply with. This gives the EU a combination of economic power and political power over entities engaged in economic activities inside EU borders. So where its economic power derives from the size and importance of the single market, and its political power from its mandate to enforce agreed upon rules, one may argue that, in the area of foreign policy, there exists a power void left by the EU's military non-power, which could be filled by a kind of normative power.

The concept of NPE is one that conceptualizes the EU as an actor in international relations that has the power to influence others so as to persuade them to change their behavior. It is a way of saying to the rest of the world that 'we' believe in certain things, and that 'they' ought to believe in them too; that we do certain things on the basis of those beliefs, and that they should also be doing those things. It furthermore implies conceptions of the self as adherents to certain norms but also conceptions of others as entities who do not (yet) adhere to those norms. A normative power, then,

should have the ability to stimulate an evolutionary process in external actors that would guide them from point A to point B; from a point of non-adherence to adherence. It should have the ability to make others act in ways they did not before. Others should thus either be persuaded by the universal validity of the norms propagated by the EU and for those reasons start acting in accordance with the norms, or – and this may just as well be – that even when particular others are not ready to accept as valid the norms themselves, the EU has other means of being persuasive when it comes to third parties being prepared to change their behavior.

2.1 The NPE hypothesis

The Union's action on the international scene shall be guided by the principles which have inspired its own creation, development and enlargement, and which it seeks to advance in the wider world: democracy, the rule of law, the universality and indivisibility of ***human rights and fundamental freedoms****, respect for human dignity, the principles of equality and solidarity, and respect for the principles of the United Nations Charter and international law.*[2]

Article 21 TEU above carries the spirit of the NPE hypothesis, and most likely formed the fundamental basis of Ian Manners' (2002) original idea. The debates around the idea of EU normative power have been vivacious from the outset, casting doubt on some of the holy houses in International Relations scholarship. Manners, after all, positions himself opposite to adherents of the realist school in international relations (specifically Hedley Bull) when he discusses: *"…the international role of the European Union (EU) as a promotor of norms which displace the state as the centre of concern."*

[2] Treaty on European Union, article 21

(Manners, 2002: 236) According to Hedley Bull, writing in the 1980s, 'the civilian power of the EC was conditional upon the military power of states.' Manners agrees that this was true for the 1980s, but counters that times have changed since then. The Cold War had fed many of the assumptions underlying the concepts of civilian and military power, but the collapse of the Soviet empire was neither caused by civil diplomacy nor by military force. Rather, Manners argues, it was caused by the power of ideas and norms.

"I argue that by refocusing away from debate over either civilian or military power, it is possible to think of the ideational impact of the EU's international identity/role as representing normative power." (Manners, 2002: 238)

Manners then elaborates further on the NPE concept by discussing the EU's normative difference, the EU's normative basis, and the diffusion of EU norms. The EU's normative difference derives according to Manners from 'its historical context, hybrid polity and political-legal constitution.' These characteristics are what makes the EU different.

"*…in my formulation the central component of normative power Europe is that it exists as being different to pre-existing political forms, and that this particular difference pre-disposes it to act in a normative way.*" (Manners, 2002: 242)

The EU's normative basis derives from five 'core norms' which are implicitly or explicitly represented in the EU's laws and policies, namely: peace, liberty, democracy, the rule of law, and human rights. These core norms are then promoted and spread through a process Manners calls 'norm diffusion'. The six ways in which the norms are supposedly diffused are: contagion, informational diffusion, procedural diffusion, transference, overt diffusion, and cultural filter. Contagion has to do with leading by example – so essentially to be the change one wishes to see in the world. Informational diffusion is about strategically composed communications and proclamations

of intent. Procedural diffusion takes place when relationships with third parties are institutionalized through negotiations and agreements, bilateral or multilateral, and through EU enlargement.[3] Transference refers to a process by which EU norms and standards are either exported or stimulated by means of the carrots and sticks principle.[4] Overt diffusion occurs due to the EU being physically present in a third country. And finally, cultural filter describes the impact of international norms on learning processes in third countries.

Thus, by grace of its structure, its principles, and its means for spreading its norms, the EU could be conceptualized as a normative power.

2.2 Constructive criticism

There are several legitimate criticisms of this first attempt by Manners (2002) to distinguish normative power from other sources of power. Diez (2005) and Sjursen (2006) both recognized that the concept of normativity is burdened by the presupposition that the EU is a force for good. The notion of 'spreading norms' has a somewhat pretentious tone to it. Different peoples have different norms so it really depends on the validity of the norm itself whether spreading that norm is something to be desired.

2.2.1 Cosmopolitanism

Helene Sjursen (2006) emphasized the need to develop criteria that would allow us to evaluate the validity of the norms the EU attempts to spread.

[3] One of the requirements for a candidate country to become an EU member is to accept the Acquis Communautaire in full. This is a clear example of procedural diffusion as defined by Ian Manners (2002). After all, intergovernmental negotiations take place which should result in the third country adopting EU norms.
[4] A rewarding of 'good' behavior, and punishment of 'bad' behavior.

The goal of developing such criteria would be to identify universal norms, in relation to which one may judge the EU's imagined normative activities. Sjursen proposes a kind of **cosmopolitanism** as a legitimate basis for EU normative acts.

"…I have proposed that a focus on strengthening the cosmopolitan dimension to international law would be a strong indicator for a 'normative' or 'civilizing' power. - …a normative power would be one that seeks to overcome power politics through a strengthening of not only international but cosmopolitan law, emphasizing the rights of individuals and not only the rights of states to sovereign equality. It would be a power that is willing to bind itself, and not only others, to common rules." (Sjursen, 2006: 249)

2.2.2 Self-reflexivity

Thomas Diez (2005) also suggested a greater degree of **self-reflexivity** to guide EU external action. Diez explains how *"…the narrative of 'normative power Europe' constructs the EU's identity as well as the identity of the EU's others in ways which allow EU actors to disregard their own shortcomings unless a degree of self-reflexivity is inserted."* Diez uses the condition of self-reflexivity as cure to an unscrutinized belief in one's own 'goodness'. One's own norms are then deemed superior and for that reason deserve to be spread through whatever means, be they normative or forceful. Diez points to the Unites States as an example of a state using forceful means to project its norms. Diez warns against the EU going down this same path. If the EU noticeably aspires more military capabilities and ignores taking a reflexive stance towards itself, this could well be detrimental to its normative credibility. Thus, good intentions are insufficient. Actions should be

normatively congruent as well. 'Hell is full of good meanings, but heaven is full of good works'; so goes the saying, and it applies here too.[5]

2.2.3 Market Power Europe

Chad Damro (2012) found that the EU is perhaps more accurately described as a Market Power (MPE). He highlights the importance of the single market, describing it as the EU's 'core'. According to Damro, the EU's identity may have particular normative characteristics, but it is fundamentally a large market. This market is regulated by the EU, and thus any act which has an influence on external actors implicates the power of the market. The EU has exclusive competence over market-related regulatory policies, and the size and strength of the European market may result in the **externalization** of these policies.[6]

One may categorize the externalization of EU regulatory policies under 'normative impact'. However, such impact is not necessarily a consequence of normative intentions. Damro focuses mainly on intentional externalization, but he recognizes that in some cases externalization may result unintentionally[7]. If the intent is (in part) to externalize internal policies and regulations, and these are constructed in light of a particular norm, then the degree to which they are in fact externalized can be measured to indicate the EU's normative power. EU acts aimed at externalization may include external dialogues and negotiations, but also threats of suspension of bilateral agreements or delaying those being negotiated in the present.

[5] I vow to keep my use of such clichés to a necessary minimum.
[6] Damro defines externalization as follows: *The first stage of externalization occurs when the institutions and actors of the EU attempt to get other actors to adhere to a level of regulation similar to that in effect in the European single market or to behave in a way that generally satisfies or conforms to the EU's market related policies and regulatory measures […] The second stage of externalization requires these non-EU targets actually to adhere to said level of regulation or to behave in said way.* (Damro, 2012: 690)
[7] See also Bradford (2011, 2012, and 2014) for the unintended externalization of EU norms. Chapter 7 deals with this phenomenon.

These can be considered examples of intentional externalization.[8] However, externalization may also occur unintentionally. Instead of the EU actively trying to spread a norm, the spread is then caused by virtue of the EU itself being important for third parties in various respects. As will be explained in chapter 7, the importance of single market access for commercial third parties may give it 'involuntary incentives' to adopt EU standards (Bradford, 2014).

2.3 NPE analytical method

Tuomas Forsberg (2011) distinguished two approaches in studying normative power. The first is to announce the sense in which the term normative power is used prior to evaluation of a specific case, so that the scope of its use is clearly circumscribed. The second option is to say that normative power may be better described as an ideal-type.

"Ideal types are thus idealized (but not necessarily normatively idealized) descriptions of the concrete features of things that help to compare otherwise fuzzy phenomena with each other. Ideal types are mental constructs, and in individual cases the features of an ideal type can be 'more or less present'. Ideal types are therefore not true or false: they can only be described as being either helpful or unhelpful as heuristic aids for studying concrete phenomena." (Forsberg, 2011: 1199)

This paper takes the second approach. In approaching normative power as an ideal type, the objective is to define as properly as possible the **features** which would make the EU fit the 'normative power' label in the specified area. If the ideal type 'normative power' is assumed to have all the chosen features, it should be possible to answer the research question by analyzing

[8] I elaborate on such normative action, based on different kinds of conditionality, in chapter 6.

to what extent the EU has these features as well. For each individual feature, the result might be different. This approach may be criticized in at least two ways. Either the wrong features are attributed to the imagined ideal type, or particular features are mistakenly attributed to the EU; or both.

2.4 Privacy Power Europe

The Privacy Power Europe (PPE) hypothesis is aimed at appraising the degree to which the EU is a normative power in the area of **privacy and data protection**. This area can, of the 'five core norms' mentioned earlier, be categorized under human rights. The PPE approach borrows in part from Manners' (2008) 'tripartite analysis', which separates three analytical perspectives on normative power: intent (principles), action and impact.

2.4.1 Normative Intent

Manners (2008) referred to this first section of the tripartite analysis as the section dealing with 'principles'. Manners (2008) included **coherence** and **consistency** as concepts through which to evaluate the principles of an NPE. These concepts narrowly correspond with the main points of criticism discussed in section 2.2.1 and 2.2.2; those of Sjursen (2006) and Diez (2005). As such, cosmopolitanism and self-reflexivity are included repackaged and rephrased, perhaps slightly adjusted and arguably improved, as coherence and consistency.[9]

[9] "Coherence entails ensuring that the EU is not simply promoting its own norms, but that the normative principles that constitute it and its external actions are part of a more universalizable and holistic strategy for world peace." (Manners, 2008: 56)
"Consistency means ensuring that the EU is not hypocritical in promoting norms which it does itself not comply with." (idem)

This paper separates EU **normative intent**, dealing with the EU's goals, norms, and how it aims to promote these; from the **universal validity** of the privacy norm. Evaluating the universal validity in chapter 5 in reference to the normative intent discussed in chapter 4, is meant to discern whether the EU is acting 'coherently'. If the EU is promoting a norm of its own, which has no apparent support extending beyond EU borders – i.e., is not universally valid – then the value and desirability of promoting it can be considered questionable. If the norm promoted, on the other hand, transcends cultural differences and particular strategic and geopolitical interests, then EU attempts at promotion of such a norm can be categorized under **normative action**.

The aim is to first develop an accurate picture of the EU's motivations, predispositions and intentions with regard to privacy and the protection of personal data. This is done in the context of the importance of the privacy norm itself, especially in today's world in which the existing importance of the internet and the increasing adoption of Big Data practices are, though beneficial in most respects, posing a threat to our ability to retain control over our personal data. The EU's recognition of this fact will be considered, as will the acts it is pursuing or has pursued to deal with it.

2.4.2 Normative Action

In chapter 6, the EU's actions are analyzed by looking at their engagements and dialogues with third countries and other external entities, and then especially the United States (US). The adequacy decisions made by the EU on the basis of article 25 of the Data Protection Directive (DPD), give it the means to ban data transfers to third countries due to those countries not providing adequate protection of the personal data of EU citizens when

transferred to said countries. The question then is whether this constitutes acting on the basis of normative intent, and whether the means used to persuade third countries to change policy are 'normative means' underlined by normative power, rather than particular other means underlined by other forms of power.

The ongoing dialogues and negotiations with the US on the topic of data protection, mainly in the context of counter-terrorism, enjoy the most elaborate examination among things discussed in chapter 6. Interdependent allies for the most part, the EU and the US have engaged in heated debates in this area throughout recent years. In this case, the question is whether the EU takes a normative position in these debates; whether the EU shows internal consistency in the norms it propagates and the manner in which it acts; how the EU's position has developed over the years; and how effective it is in its attempts at persuasion.

Two ECJ rulings involving considerations of privacy and data protection are furthermore discussed. The ECJ is an institution with substantial power within the EU. Its decisions are binding and have seemingly aided the cause to promote privacy, internally and abroad. An assessment will be made to what extent the ECJ contributes to making the EU as a whole a normative power in the area of privacy and data protection.

2.4.3 Normative Impact

In chapter 7, the impact of EU action will be weighed by looking at the EU's persuasiveness in their dialogues with third parties, the incentives such third parties have to change their behavior, and the extent to which the EU is actually able to externalize its norms. In the area of privacy and data protection, it thus pays to find out whether the EU's data protection

regulations are in fact being externalized, and if the EU intentionally acts in pursuit of this goal; or if externalization is an unintended or secondary side-effect.

The externalization of norms may be caused by a variety of factors. When the EU acts intentionally to promote privacy, the means used to achieve normative impact should be indicative of the kind of power involved, normative or otherwise. When EU acts have the unintended consequence of achieving normative impact, the incentives of third parties to change policy should also be indicative of the kind of power involved. The impact of EU privacy and data protection norms on individual commercial enterprises will be considered, as well as the impact on third country legislation. The extent to which the EU is, or could potentially be, able to achieve normative impact in this area, should show how effective the EU is as a supposed normative power. Effectiveness should be considered an essential feature of the ideal type PPE. After all, an impotent power is no power at all.

2.4.4 PPE ideal type features

The features attributable to the Privacy Power Europe ideal type are the features which will be more or less present in the EU. These features are the following:

1. PPE should have the intent to defend, promote and spread the privacy norm.[10]
2. PPE should act in accordance with the privacy norm and should show internal consistency in doing so.

[10] The normative value of this feature is of course dependent on privacy being a universally valid norm. The PPE hypothesis is therefore partly dependent on presuming universal validity. Chapter 5 should legitimize this presumption.

3. PPE should elevate concerns about privacy and data protection over strategic concerns.
4. PPE should be effective in achieving the spread of privacy and data protection norms.

This study will proceed as follows. The next chapter discusses the increasing importance and relevance of Big Data and related digital developments. Benefits as well as risks will be recognized. Chapter 4 deals with the EU's principles and intentions with regard to privacy and the protection of personal data in assessing the presence of normative intent. Chapter 5 is meant to establish the validity of the privacy norm and with it the cosmopolitan coherence of the EU acting in promotion of this norm. Chapter 6 evaluates an array of EU actions, engagements, dialogues and decisions based on considerations of privacy and the desire to protect personal data. Chapter 7 provides an analysis of the normative impact the EU is able to achieve, and should show how effective the EU actually is or could potentially be in spreading its privacy and data protection norms. Chapter 8, finally, will conclude with a revaluation of the abovementioned PPE ideal type features, in order to answer to what extent the EU is a normative power in the area of privacy and data protection.

3 Big Data

"There were five exabytes of information created by the entire world between the dawn of civilization and 2003, and now that same amount is created every two days."[11]

Big Data could be defined, quite simply, as 'a lot of data'.[12] Of course, such a definition does not come close to explaining what all the fuss is about. This chapter is intended to ensure a baseline understanding of big data and other contemporary data-related phenomena, as well as to sketch the essential context for the rest of the paper. Developments in big data in recent decades have been an important factor driving the European Union to draft and negotiate updated data protection legislation. It makes sense, therefore, to start with a brief discussion of those developments before moving on to EU actions in this area and to the supposed intentions underlying those actions.

Many are excited about big data's potential. Others are worried about its risks. The EU recognizes both sides, and in abstract terms it intends to capitalize on its potential and to mitigate its risks. As such, in the developing world of big data, there is good news and there is bad news. I will start with the good news.

[11] Quote by Eric Schmidt (Google CEO) at the Techonomy Conference 2010, Lake Tahoe; the numbers he uses are of course contestable, but the point is that people produce and store much more information now than we used to.

[12] Data is defined by Merriam-Webster as *factual information (as measurements or statistics) used as a basis for reasoning, discussion, or calculation*. On many occasion, the terms 'data' and 'information' are virtually synonymous.

3.1 The good news

"Big Data can't tap into our unconscious thought processes directly, of course. But with a vast storehouse of our past decisions to analyze, it could detect patterns of behavior we are not aware of, and those patterns could reveal the unconscious thought processes that drive the behavior. In a very real sense, Big Data could know us better than we know ourselves."[13]

There is much to be excited about when it comes to big data. First, however, one requires a sufficient grasp on the basic concept. Its inner workings are immensely complex, but it is not impossible to visualize big data's primary features, and to construct a reasonably accurate picture of the overall concept. Some have described its development as moving toward the construction of a 'global nervous system'. However interesting, this is a few steps beyond the scope of this paper.

The amount of data that is generated these days is vast.[14] In the current digital age, we are able to generate, store, spread, measure, and utilize massive amounts of information. We need physical sites to store this data, but the amount of space we need to store some amount of data is ever decreasing. For example, even though we still use localized data storage devices to store some amount of data, the advent and commercial success of cloud computing has made remote storage of – and remote access to – data an everyday phenomenon. Providers of cloud computing solutions make use of economies of scale with regard to data storage, and data storage

[13] Quote by Dan Gardner: Smolan (2013: 15), an insight which could also be considered a negative.
[14] The collection of data is important for various kinds of learning. A scientist or an entrepreneur, data can help one achieve one's ends. In either profession, one conducts a variety of experiments in order to find answers to lingering questions. Such experiments may give us valuable insights, allowing us to increase our shared knowledge and to optimize existing processes. Without the ability to gather and store data over time, as well as the ability to conduct proper and logically coherent analyses of said data, we would have to put all our trust in our imperfect senses and in fallible anecdotal evidence. Of course, the scientific method is no novelty. However, the amount of data available for analysis is.

centers are located all over the world.[15] As such, they contribute to cost savings throughout the world economy.

Thus, a growing amount of data is generated every day and we have increasing means to store this data. However, the more data is generated and stored, the more data there is to be analyzed. This is often a rather daunting task. Even CERN is unable to analyze all the data the Large Hadron Collider generates, and for this reason distributes it to its partners where necessary.[16] Analyzing big data remains difficult, but the incentives to make it work are clearly there. The scientists at CERN recognize this, but commercial enterprises are also making increasing use of big data analysis to optimize their management (McAfee and Brynjolfsson, 2012) or to develop new ways of catering to the consumer.

Big data is already being used to make possible the provision of certain services, at least some of which many of us have already encountered before. Many businesses with a large customer base are collecting data about their customers and their behavior. This might be done offline by means of customer cards registering the purchases of returning customers, or online by means of customer accounts and digital tools registering page views, search commands, purchases, and all sorts of other actions. There is an array of software products available to help one analyze the collected data. Such analysis should allow the data collector to make predictions about the individual preferences of customers. In this way Amazon may suggest products to you, YouTube may suggest videos, Facebook may suggest friends, and the suggestions will often be on point.

[15] See for example Huawei's cloud storage services: a Chinese cloud computing operator storing the data of CERN, one of Europe's most valuable assets <http://www.huawei.com/ilink/en/success-story/HW_194986>

[16] CERN: What to Record? *The volume of data produced at the Large Hadron Collider (LHC) presents a considerable processing challenge.* <http://home.web.cern.ch/about/computing/processing-what-record>

Knowing what the customer wants allows a supplier to more accurately assess demand and thus to avoid overproduction and waste by managing a more optimized stock. It enables the producer to engage in more data-based decision-making (PWC, 2013).[17] Big data also promises to grant, as far as it does not already, enormous benefits for health care provision. The European Centre for Disease Prevention and Control (ECDC), for example, gathers and analyzes data with the aim of preventing the spread of infectious diseases, while the digitization of medical records will allow health care providers to analyze the data to provide more efficient and targeted care (Groves, 2013).

Furthermore, big data may help enhance energy efficiency through smart meters; it may help improve sport performance through personal quantification tools; it may ease the process of getting from one place to another in the fastest or most efficient manner through navigational tools; it may help financial traders to gain lucrative insights into markets; it may help identify climatic trends; it may even help security and law enforcement agencies to catch criminals or detect potential sources of danger.

In short, big data may give us much. But what might it take from us?

3.2 The bad news

Data, especially in bulk, has become an incredibly valuable asset. And as is true for anything of value; the possibility exists that people with malicious intent aim to get their hands on it. If data can be a means to beneficial ends, it can also be a means to harmful ends. In general, if one is to prevent a valuable asset from falling into the hands of the wrong people, it ought to be protected. The required level of protection will in turn be dependent on the determined value of the asset.

[17] Which is preferable to conventional decision-making in the same way that an educated guess is preferable to a wild guess.

While there are a substantial number of data types which could be beneficial for specific purposes, there is one particular kind of data which poses the most clearly identifiable risk of abuse: personal data. Personal data, or **personally identifiable information** (**PII**), as it is often referred to in legal terms, is particularly sensitive because it concerns people's 'personhood'. It is information linked to the individual itself. Any abuse of such information has an immediate effect on a person; a sentient individual, capable of experiencing abuse first-hand. While information about material objects may well be abused for the selfish purposes of the abuser, it does not compare – as personally perceived consequences are concerned – to abuse of information about people. There exists a clear difference between kinds of data. They are not all the same.

Big data, as previously explained, involves the storage and subsequent analysis of a lot of data. Such data may thus include data of the most sensitive kind: PII, which might for example refer to information contained in medical records. So when one imagines the benefits of medical records being digitized and analyzed with the aim of enhancing medical knowledge and thus of improving the quality of health services, one has not yet considered the fact that medical records are actually private information. It is not enough to say that the purposes of analysis are benign. Anyone can make such claim.

Because private information tends to be sensitive, this information is often protected in one way or another. It is not accessible to everyone. Access has to be provided by those who own the information. Thus, accessibility is based on consent. Because big data involves big amounts of data, the process of acquiring consent from all the data owners is burdensome. And even if consent is acquired for accessing all or most of the data for some particular purpose, the data ought to be handled in such a way that access is

not inadvertently acquired by unauthorized persons. This is often no easy task, but it is certainly costly.

Protection of valuable data indeed comes at a cost. It may also be deemed a distraction from the purpose for which access to the data was acquired in the first place. As such, the incentives do not always balance towards ensuring optimal protection. This puts sensitive PII at a risk, especially when analyzed in bulk. Even more so because the incentives for gaining access to the data might be quite substantial. Intervention by authorities to alter the balance of incentives can be argued to be justified in that case.

When it comes to medical records; those often already enjoy reasonable protection, as ensured by the law. However, consider the amount of PII that is being collected and stored without us necessarily even being aware of it. Countless devices are brought to market that are connected to the internet and are collecting data about us. Such is the advent of the *Internet of Things* (IoT). The 'things' in IoT are often equipped with Radio Frequency Identification (RFID)-tags which make it possible to identify and track the items within a data communication architecture designed for some purpose (Weber, 2010: 23). Tracking items entails collecting data about them. Users of such items do not necessarily know that the items are equipped with the tags as there need not be any visual or audible signal alerting the user of data communication taking place (Weber, 2010: 24; COM, 2014). Therefore, PII might end up stored on some remote storage device without the owner of the information knowing about it.

Data may be collected for both benign and malicious purposes. However, even data collected for benign purposes may be ill-protected and vulnerable for unauthorized access. The more data is being collected by RFID-tagged items and the more commonplace such data collection becomes, the more data is floating around which is at risk of being abused if we pay no attention

to it. Without sufficient protection, PII may easily end up with the wrong people and in the wrong places. And even if the data is sufficiently protected, it could be used for purposes not intended. The fact that data is collected so covertly, makes it difficult for us to keep track of what happens with it, and to decide if we agree with it.

Furthermore, the entities that may access our private information without authorization are not always your regular computer-savvy underground criminals. Our PII is also probably, and perhaps even especially, at risk of being illegitimately accessed by established corporate entities and government agencies; or a combination of both. The revelations of Edward Snowden have brought attention to the global data collection architecture built and operated by the United States' National Security Agency (NSA) and its partners, the proportions of which are almost beyond belief. The NSA is indiscriminately collecting and storing virtually *all* the communications taking place on the global internet (Greenwald, 2014; Harding, 2014). They certainly did not ask for permission.

The data collection activities of the NSA are a perfect example of an entity claiming to have benign intentions, but where the implications of the collection are so severe as to make their supposed intentions meaningless. Even though the NSA is not yet capable of processing and analyzing all the data it collects; there are technological innovations likely on their way that might in the future make it possible for them to do so. The quantum computer might be such an innovation. Once that happens, the risks and consequences, though still unknown, are unsettling. Our PII, which is becoming more and more accessible through the internet, will almost undoubtedly end up in the hands of the NSA or other such agencies. That is, unless we do something about it.

4 Normative Intent

In describing the intentions of the EU underlying its actions in the area of privacy and data protection, this chapter analyzes several EU communications and documents, aiming to find what appear to be proclamations of intent. This seems the only way in which one can ever hope to discover the intentions behind the actions of an institutional construct like the EU. The passages and proclamations are divided into three separate categories:

1. Aimed at attaining economic and/or strategic gain for the EU and its citizens
2. Aimed at attaining increased privacy and data protection for EU citizens
3. Aimed at attaining increased privacy and data protection for people in general

The intentions are ordered from self-interested to more cosmopolitan – or from strategic to normative. Various passages in EU communications and documents are discusses and evaluated, labeling them as belonging to one (or more) of the three categories. It will likely show that each category has its role, though some may hold more weight. The aim is to find whether category 3 holds enough weight for EU intent in the area of privacy and data protection to be qualified as 'normative intent'. For this purpose, one may ask: does the EU have normative intentions in the area of privacy and data protection? This question can be either negated or confirmed by the evidence.

4.1 Data Protection Directive

The 1995 Data Protection Directive[18] was in part built upon recommendations made by the OECD in 1980[19], and the European Council's 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[20].

The OECD recognized: …*that, although national laws and policies may differ, Member countries have a* ***common interest in protecting*** *privacy and individual liberties, and in reconciling fundamental but competing values such as privacy and the free flow of information.* (OECD, 1980)

The Council recognized, per article 1, covering the object and purpose of the convention, that: *The purpose of this convention is to* ***secure*** *in the territory of each Party* ***for every individual, whatever his nationality or residence****, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection").* (European Council, 1981)

Article 1.1 of the Directive, covering the object, reads: *…Member States* ***shall protect*** *the fundamental rights and freedoms of* ***natural persons****, and in particular their right to privacy with respect to the processing of personal data.* (COM, 1995)

These three documents are different in the forcefulness of the language used. This is, of course, largely due to the nature of the separate documents and the regulatory power of the institutions authoring them. Still, each passage can be placed under category 3. For the OECD passage, this is not surprising. After all, the OECD is not merely composed of EU Member States. However, none of the passages seem to discriminate between individuals

[18] …of the European Parliament and of the Council, of 24 October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[19] Guidelines covering the protection of privacy and transborder flows of personal data.
[20] Directive 95/46/EC, article 11 refers to the convention.

that are EU citizens and those that are not. The passage of the convention even explicitly states that nationality and residence are of no concern. On the other hand, it does also mention territorial boundaries. It can be argued, however, that this merely gives respect to the practical limitation of bounded jurisdiction, rather than a lack of cosmopolitan intent.

The OECD guidelines also mention economic motivations for the harmonization of data privacy laws, but the OECD does not aspire economic gain for Europe only. It emphasizes potential gains for all its members, so it cannot belong to category 1. Yet because digital data flows are a global phenomenon, the EU might use the same arguments as the OECD does for harmonizing data privacy laws. Indeed, a Directive in general is aimed at harmonization. While it is true that a Directive is only meant to provide strict guidelines for action on the part of Member States, a Directive does also entail an obligation for Member States to implement measures required for the attainment of the stated purpose of the Directive. As such, the general intent of a directive is to get all Member States to take action in some area.

The specific intent of Directive 95/46/EC was to get Member States to take action in the area of data protection. To an extent, this has happened. However, because individual Member States had an amount of freedom with regard to implementation, EU citizens in some countries remained less protected than EU citizens in other countries. This caused, and still causes, legal uncertainty for commercial enterprises operating in the EU market (Pearce and Platten, 1998). Enterprises doing business in multiple EU Member States had to comply with one set of regulations here and another set of regulations there. This raised the cost of compliance and thus increased incentives for noncompliance. Therefore, aside from the fact that it defeats the normative purpose of the Directive, such result is economically unsound. It is a barrier to trade, because it may defer enterprises from doing business in some countries or from allowing personal data processed

by them to flow freely from one Member State to another. According to provisions 7-9, the Directive was intended to provide remedy for this state of affairs, but it failed to do so in many respects. Such is the economic argument for reform and can thus be grouped under category 1.

All three categories of intent are represented in various provisions and articles of the Directive, as can be seen in table 1. Some provisions belong to more than one category, while some are absent – for example because they deal with possible derogations. One may notice that a fair amount of the provisions are grouped under category 3, which would seem to confirm the presence of normative intent. It has to be said, however, that many of those provisions could also be placed under category 2, for the simple reason that an EU Directive is EU law and not a law governing all people. The division is done in this way because the provisions placed under category 2 specifically stated the territorial limitation, whereas the others did not. For example, provision 12 states that: *Whereas the protection principles must apply to all processing of personal data by any person whose activities **are governed by Community Law**.* In contrast, provision 2 states that: *Whereas data-processing systems are designed to serve **man**; whereas they must, **whatever the nationality or residence of natural persons**, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of **individuals***. The latter clearly has wider scope than the former.

While the provisions seem to balance towards category 3, article 3.2 adds substantial weight to category 2 when it states: *This Directive **shall not apply** to the processing of personal data: - in the course of **an activity which falls outside the scope of community law**…* The same is true for article 4.1a, and even though articles 4.1b and 4.1c describe situations in which territorial limitations are not so clear-cut, article 3.2 renders any further use of language hinting at cosmopolitan intent or general application essentially

meaningless, because the scope had already been narrowed down to EU territory. However, article 25.5 shows that the Commission may attempt to remedy a lack of protection in a third country. This appears to indicate an intention to attain increased privacy and data protection for the people in such third country, thus belonging to category 3. The intent could of course merely be to protect EU citizens' data when crossing certain borders (cat. 2), thus increasing possibilities of trade (cat. 1), but then article 25.6 once again refers to *the protection of the private lives and basic freedoms and rights of* ***individuals***.

TABLE 1	Category 1	Category 2	Category 3
Provision number	3, 4, 5, 6, 7, 8, 9, 43, 56	1, 10, 12, 18, 19, 63, 64	2, 3, 10, 14, 18, 20, 23, 24, 25, 26, 27, 28, 29, 30, 31, 33, 38, 39, 41, 45, 46, 48, 51, 54, 55, 56, 57, 59, 61, 62, 63, 64, 65, 68
Article number	1.2	**3.2**, 4.1a,	4.1b, 4.2c, 25.5, 25.6

In case of Directive 95/46/EC, one may conclude that the territorial limitation inherent to a directive is indicative of EU intent being primarily of the second category, even though different intentional categories could coexist side by side. Provision 2 does suggest that the intent behind using the Directive as a means to an end, is fed by the conviction that privacy is a right which all people should enjoy. Therefore, while category 1 and 2 are

explicitly represented in the Directive, it can be argued that category 3 is implied in some of its phrasing.

4.2 Reform

Rapid technological developments and globalisation have brought new challenges for data protection. With social networking sites, cloud computing, location-based services and smart cards, we leave digital traces with every move we make. In this "brave new data world" we need a robust set of rules. The EU's data protection reform will make sure our rules are future-proof and fit for the digital age. (COM, 2012a)

Apart from the economic argument for reform mentioned earlier, another major argument has to do with the fact that the Directive is already twenty years old. And in this digital age, twenty years is a very long time. The world has changed a lot since 1995. As discussed in chapter 3, technology has changed and is changing in such a way as to pose significant risks to the privacy of individuals and their PII. A reform, therefore, essentially intends to achieve the same as the Directive was supposed to. The EU Factsheet 'Why do we need an EU data protection reform?' (COM, 2012b) states that: *Its basic principles, ensuring a* ***functioning internal market*** *and an* ***effective protection of the fundamental right*** *of individuals to data protection are as valid today as they were 17 years ago.*

As often seen in passages of the Directive, the above phrasing suggests that the EU considers data protection as 'a fundamental right of individuals'. A right cannot in any way be 'fundamental' if it would apply only to EU citizens. Therefore, such phrasing gives the impression that the EU has category 3 intentions (in addition to category 1), yet simply has to work within its practical limitations. Indeed, the EU has since incorporated the

right to data protection into the Charter of Fundamental Rights of the EU (Charter), under article 8. This gives credence to the notion that the EU has normative intentions in this area, regardless of the fact that the EU does not have limitless power to underline its intent.

4.3 General Data Protection Regulation

With data-based technologies increasingly infiltrating our lives, guidelines for instrumental action have to change. As such, a general data protection regulation (GDPR) was proposed in 2012.[21] Because the proposed reform entails a transition from a Directive to a Regulation, guidelines will be replaced by law having direct effect in all Member States. This prevents differences in implementation and should ensure more legal clarity and equal protection under the law for all EU citizens.

Because the GDPR, like the Directive, has limited territorial scope and has the same degree of category 1 intentions underlying it, the focus is on those passages which deal with international engagement; and the possible intention to attain increased privacy and data protection for people in general.

Article 45, for example, deals with the intent and self-ascribed obligation to cooperate internationally to protect personal data. It states that the Commission should: *develop effective international cooperation mechanisms…, provide mutual assistance…, engage relevant stakeholders…, and promote the exchange and documentation* of legislation*… in the enforcement of data protection legislation.* This at the very least shows the intent to get third countries to *adhere to a level of regulation similar to that in effect in the European single market* – a process of attempted

[21] Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

externalization (Damro, 2012: 690), thus stimulating an increase in data protection for people outside the EU (cat. 3). However, it may be argued that such intent merely derives from the aim to protect EU citizens' PII abroad (cat. 2). Indeed, article 41.2a explains that the Commission, when evaluating the adequacy of protection in a third country, should consider, among other things: *…effective and enforceable rights including effective administrative and judicial redress for data subjects,* ***in particular for those data subjects residing in the Union*** *whose personal data are being transferred.* In this, the Commission seems to give priority to the protection of EU citizens, which albeit completely understandable, is perhaps not entirely cosmopolitan.

International engagements with regard to data protection are based on clear category 1 intentions. As the Commission has extensive consultations with relevant private sector entities before drafting and adopting a law, the stakeholders involved have voiced their criticisms of barriers to international data transfers. Such barriers are likely to impede their international business operations. As such, the intent behind the Commission's international engagement is at least in part based on economic considerations. (COM, 2012a: p. 4) The Commission also predicts that companies from countries without data protection standards as high as those in the EU will be at a disadvantage compared to EU companies. Non-EU companies will have to comply with EU rules to gain access to the single market while EU-companies will have a head start when foreign markets start adopting similar standards. (COM, 2012c: p. 3)

The international elements of the GDPR are again a combination of category 1 and 2 intentions, with some of the language hinting at underlying cosmopolitan convictions of the third category. The inclusion of article 8 in the Charter confirms this conviction.

4.4 A global strategy

When the EU acts on the international stage, it intends to achieve something with its acts. The European Data Protection Supervisor (EDPS) has published its strategy for 2015-2019. They call it 'Leading by Example' (EDPS, 2015). The title already reveals a potential for significant category 3 normative intentions. Its vision includes the forging of global partnerships.

Its proposed actions are:

- *Developing an ethical dimension to data protection*
- *Mainstreaming data protection into international agreements*
- *Speaking with a single EU voice in the international arena (p.18-19)*[22]

The internet is fundamentally a global environment, and the EU needs to act with this in mind.[23] The EU commissioner for the Digital Economy has already urged for the UN to create a data protection agency.[24] The EDPS also recognizes the necessity of a global approach and proposes extensive international discussion and collaboration in working towards a common purpose: protecting privacy and personal data in a smart and efficient way.[25] Although the EDPS is an independent entity, it is certainly part of the EU and has explicit normative intentions. And with the EDPS being the EU's appointed authority in the area of data protection, their intentions will presumably be consequential.

[22] Underlined by COM (2012c: p. 84) - *…to improve and streamline the current procedures for international data transfers, including legally binding instruments and 'Binding Corporate Rules' in order to ensure a* ***more uniform and coherent EU approach*** *vis-à-vis third countries and international organizations.*
[23] Underlined by COM (2012c: 88) - *…A global harmonized approach towards data protection is deemed indispensable especially bearing in mind the growing popularity of cloud computing*.
[24] Warden, G., Treanor, J. (2015). UN needs agency for data protection, European commissioner tells Davos. *The Guardian, 22-01-2015*
[25] Underlined by COM (2012c: 87) - *…enhance its cooperation, to this end, with third countries and international organizations, such as the OECD, the Council of Europe, the United Nations, and other regional organizations; - closely follow up the development of international technical standards by standardization organizations such as CEN and ISO…*

4.5 A higher goal

So in conclusion of this chapter, does category 3 hold enough weight for EU intent in the area of privacy and data protection to be qualified as 'normative intent'? Although the Directive and the Regulation are laws which apply only to the EU, its market and its citizens; the language used in these documents as well as various related communications on occasion hint at a higher goal. The fact that data protection was included in the Charter as a fundamental right does indeed suggest that it is deemed applicable to all individuals, no matter their nationality, ethnicity or background. Indeed, the fact that political refugees, for example, may not be sent back to their country of origin if that will likely result in a violation of their human rights according to the Charter, is a clear indication that such human rights are based on shared convictions about 'human beings' and not merely about those residing in the EU. Article 21 of the TEU also states that protecting human rights is one of the principles that should guide the EU when acting internationally. It is fair to conclude, therefore, that the EU has normative intentions in the area of privacy and data protection.

5 The validity of the privacy norm

To be a normative power in the area of privacy and data protection, the EU needs to be engaged in promoting the privacy norm. In fact, any supposed normative power should be engaged in promoting some kind of norm. Sjursen (2006) argued that such a norm should be subject to a degree of scrutiny. Indeed, if a particular norm were not universally valid, the value of being a normative power for said norm would be questionable. Manners (2008) called it the virtue of *coherence*. For the EU's external actions in the area of privacy and data protection to be coherent, they ought to be *part of a more universalizable and holistic strategy for world peace* (Manners, 2008:56). Perhaps in this specific case, it would be more accurate to speak of a strategy for the betterment of the human condition.

This chapter tackles the question whether an increase in privacy and data protection betters the human condition. If the answer is *yes*, then the privacy norm can be considered universally valid and therefore worthy of promotion. The EU being a promotor of this norm, at least supposedly, would thus help to qualify it as a normative power in the area of privacy and data protection. If the answer is *no*, on the other hand, then promotion of the norm would be futile if not unethical, and it would legitimize asking the question why the EU is even engaged in attaining it for its own citizens.

5.1 The value of privacy

Privacy is indispensable to a wide range of human activities. If someone calls a suicide hotline or visits an abortion provider or frequents an online sex website or makes an appointment with a rehabilitation clinic or is treated for a disease, or if a whistle-blower calls a reporter, there are many reasons for keeping such acts private that have no connection to illegality or

wrongdoing. In sum, everyone has something to hide. Reporter Barton Gellman made the point this way: Privacy is relational. It depends on your audience. You don't want your employer to know you're job hunting. You don't spill all about your love life to your mom, or your kids. You don't tell trade secrets to your rivals. […] …Comprehensive transparency is a nightmare… Everyone has something to hide. (Greenwald, 2014: 181-182)

Daniel Solove (2008) has shown that although many scholars agree on the virtue and importance of privacy, the concept of it is one that is 'in disarray'. So while it is imperative to conceptualize privacy, it is and remains a very demanding task. And whereas the importance of privacy almost seems a matter of intuition, such intuitive argument for why privacy is indeed important and should be protected is not philosophically satisfactory (Negley, 1966). The world is changing regardless of how we feel about it, and our ideas about what it is or should be are not the same as in the past, and will presumably change in the future. There is no predicting, at least not with certainty, if future generations will value privacy to the same extent as we did or do now. Nevertheless, the conceptualization and valuation of privacy is an ongoing philosophical conversation with real world applications.

According to Rachels (1975), the ability of individuals to control what others observe and know about them, allows them to maintain different kinds of relationships with different kinds of people. People act differently when they are alone than when around other people; act differently when alone with certain people rather than others; and differently again when in public or engaged in formal affairs. The content of conversations within these different kinds of relationships are thus dependent on the nature of the relationship. Some topics are deemed appropriate for conversation in some relationships but not in others. For that reason, people might stop talking about certain things when the conversation is being observed by one or more outsiders.

Rachels (1975) gives the example of two close friends having a private conversation about personal things the content of which is deemed 'not the business' of people *not* considered to be 'close' friends or even friends at all. The conversation may continue so long as it is assumed that others have no access to the content of the conversation. The moment at which an outsider 'joins' the conversation, the personal topics discussed prior to the newcomer's arrival may now be deemed inappropriate to discuss. Now imagine this situation – that of a third person being present in the conversation – to go on indefinitely; a situation in which the two friends might never again be able to truly converse in private. The relationship between the two is bound to change. Unless, of course, they are willing to discuss their personal affairs in the presence of the third person, always.[26]

Above example can be extended to apply to a government surveillance apparatus being indefinitely present to indiscriminately observe everyone's communications. Jeremy Bentham (1787) developed the idea of a Panopticon observing the prisoners day in day out. The prisoners would not know for sure that they were being watched, but the possibility was always there, which would make them wary of discussing things they did not want others, especially the prison wardens, to know about. The ability to have a sense of being alone then disappears, and with it the sense of being free. Now, in a prison, one is not free in the first place. However, when a 'Panopticon-like' system is present on the internet, a medium on which nearly everyone on the planet has some kind of presence, it will affect those who have the right not to be affected. When Big Brother was on TV, one could choose to participate. There is no such choice involved with indiscriminate government surveillance.[27]

[26] It may be assumed, with the reader's permission, that this is rarely the case.
[27] While espionage may be deemed appropriate in situations with proper cause, such proper cause is by definition not established when the espionage is done indiscriminately.

In response to the revelations of Edward Snowden in 2013, the question of why privacy is important has gained global traction. Although the right to privacy is not a particularly novel concept, the importance of protecting it in the digital age certainly seems to be. Such protection is no longer bound to the physical world and is not only necessary in defense of attempted violations by private persons and organizations, but also in defense of government intrusion. The NSA's spying operations affect the entire globe. In a reactionary manner, "the world" seems to have fixated its attention on the protection of data, and especially of PII, against the NSA and similar entities, and against potential intrusions in general. One can be assured, therefore, that the EU is not the only entity engaged in the promotion of privacy and data protection. And when normative goals align, impact is much more likely.

5.2 Privacy around the globe

Privacy is an issue of profound importance around the world.[28]

A wide array of international organizations – political ones as well as NGO's – are actively aiming to promote privacy. On December 18th 2013, the United Nations adopted a resolution on 'the right to privacy in the digital age'[29], reaffirming 'The Universal Declaration of Human Rights' (United Nations, 1948: art. 12) and 'The International Covenant on Civil and Political Rights' (United Nations, 1966: art. 17). The resolution called on all nations to adopt measures to protect privacy and personal data (art. 4). Furthermore, Privacy International, the Electronic Frontier Foundation, Human Rights Watch (Human Rights Watch, 2013), European Digital Rights, the Digital Rights Foundation, etc., with words or with actions, and alone or

[28] Solove, Daniel (2008: 2). Understanding Privacy.
[29] Resolution 68/167

together[30], have all in recent years contributed to the promotion of privacy and data protection rights; while political regions such as the Asia-Pacific (APEC, 2005; Hogan Lovells, 2014), South-America (Bloomberg, 2013; Eustace and Bohn, 2013), South-Africa (Hogan Lovells, 2014b), and even the United States with its proposed USA Freedom Act and the Consumer Bill of Rights, are seemingly following up on the many words spoken about the subject. The conversation is a heated and continuous one, with already the 37th International Data Protection and Privacy Commissioners Conference being held in Amsterdam on October 26th of this year.

It can be said with some certainty, therefore, that the EU is not just promoting its own norms. It is a global issue and a global conversation demanding global solutions. The privacy norm can therefore be regarded as universally valid, and promotion of it can for this reason be considered 'coherent'. However, to be a true normative power in the area of privacy and data protection, normative intentions are not enough. Many others are pushing the issue just as hard, if not harder. What the key thus seems to be, is to be more effective than others in pushing for adequate reform and stimulating positive change. And that's where 'power' comes in.

[30] Human Rights Watch (2015). Joint Statement from Article 19, Human Rights Watch, Privacy International, Digital Rights Foundation, and others on the Prevention of Electronic Crimes Bill 2015 Pakistan. *Human Rights Watch, 19-04-2015*

6 Normative Action

This chapter discusses acts by EU institutions on the basis of legal provisions involving privacy and data protection, as well as statements, negotiations and events wherein these values are at stake. This primarily includes engagements and dialogues with third countries and other external entities, which would constitute intentional attempts at externalization of EU norms. Furthermore, relevant court rulings by the European Court of Justice are also considered.

6.1 Dialogue with third countries

Directive 95/46/EC, article 25(6) of Chapter IV on the transfer of personal data to third countries reads: *The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.* If the Commission (having taken into account the opinions of the Article 29 Working Party and the Article 31 Committee) does indeed find that a third country has adequate safeguards in place to prevent potential abuse of the personal data of EU citizens, it may make an official decision on that basis. Such an **adequacy decision** covers data transfers from all EU Member States, and including the members of the European Economic Area (EEA), to the third country to which the decision applies. Once the decision is made, data transfers from the EU/EEA to the third country may

take place freely and without additional safeguards. Various countries have so far been recognized.[31]

According to Manners (2002), one ought to look at engagement and dialogue when evaluating the ethicality of the normative power involved in some act. As the composition of Directive 95/46/EC was necessarily prior to any negotiations with third countries about the adequacy of their protection, the Directive as a whole has been exerting a normative influence on EU internal entities for quite some time now. After all, law making is an inherently normative activity. However, the normative influence on EU internal entities is not what the NPE hypothesis attempts to explain. The NPE hypothesis is about deliberate attempts to exert normative influence on EU external entities, or at least about normative acts the scope of which reaches beyond the borders of the EU's Member States. Therefore, the most relevant acts regarding adequacy decisions are the negotiations with third countries, referred to in article 25(5). This is the kind of dialogue one would expect a supposed normative power to be engaged in.

It is important to evaluate such dialogues and related activities in light of prior intent and posterior impact. The intent underlying any sort of negotiation is to come to an agreement. Such an agreement would in this case have to be in line with what the Commission deems to ensure adequate protection of the personal data of EU citizens. The intent of the agreement is thus to protect the personal data of EU citizens even when said data is transferred to areas over which the EU has no jurisdiction. It can be said, then, that the intent of the negotiations is simply to protect EU citizens. However, if the Commission negotiates with some third country, and this third country at the start of the negotiations is not yet able to ensure adequate protection, then the intent of the negotiations is also to trigger a

[31] Andorra, Argentina, Canada, Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay, and the Safe Harbour Principles applied to companies in the United States

process of change in the third country. Negotiations ought to guide the third country from data protection standards that are too low to the adoption of standards that are high enough. The intent underlying adequacy decisions is therefore the protection of EU citizens by triggering change in a third country.

The value, or 'appropriateness', of the acts themselves – the adequacy decisions – is measured by the posterior impact being in line with what was intended. So if the impact of an adequacy decision includes a change in the third country and thus an enhancement of protection of EU citizens (of which the latter is difficult to measure, so more likely assumed), then the decision may be judged appropriate. An adequacy decision judged appropriate in this manner, however, will probably also have the effect of enhancing the protection of the inhabitants of the third country. And if it does indeed have this effect, then one may speak of 'normative impact', because the data protection norms will then have changed due to acts undertaken by an EU institution.

To further assess the degree to which the EU is a normative power regarding data protection, one may look at the ethicality of the intent as being part of some cosmopolitan strategy – the extent to which it is 'coherent' (Sjursen, 2006; Manners, 2008). When it comes to adequacy decisions, judging ethicality in this way is very much dependent on how one looks at the matter. As argued in chapter 5, the promotion of privacy and data protection standards may in itself be considered part of a universally fought fight for a fundamental right. On the other hand, the outspoken aim of the Commission's negotiations and subsequent adequacy decisions: the protection of EU citizen's personal data, can be considered a somewhat selfish one, with the resulting improvement of the conditions in the third country being a welcome but unintended consequence. This latter and slightly more skeptical conclusion is of course dependent on the Commission

actually having selfish motivations, while the reasoning might just as well be: 'our citizens benefit, your citizens benefit, thus we all win'.

Other things to look at are the incentives of the third country. The intent of the Commission itself might be one thing or another, but one ought not forget that the third country is the other half of the conversation. If the negotiations result in reforms of the data protection laws in the third country, then the law makers in the third country will somehow have been persuaded to do so. Even if one assumes that the prior intent as well as the posterior impact of the EC initiating negotiations were to externalize EU norms, the validity of the norms themselves will not necessarily have been what persuaded the third country to change.

According to the Commission (2012c: 39), *the Commission's adequacy decisions are perceived by some third countries as a means to promote their strategy for a digital economy and a modern information society. These countries consider that adequacy decisions will allow them to become actively involved in international flows of personal data and they will thus become internationally recognized as offering adequate infrastructure and adequate means for processing personal data received from the rest of the world.* The Commission's adequacy decisions would then serve as a kind of certification. If accurate, however, such incentive for third countries would be best described as strategic, not normative.

The intent of both sides of the dialogue is relevant in determining what kind of power is actually involved in the achievement of normative impact. So while the EU's intentions may be one or the other, if the opposite side – the impacted party – has strategic intentions, this may reveal much more about the kind of power involved than anything else.[32]

[32] Incentives of commercial third parties are also discussed in chapter 7.

6.2 Dialogue with the United States

The dialogues between the EU and the US on the topic of data protection are a long winding and continuing story, and shed a revealing light on the EU's normative intent and (lack of) internal consistency. Data protection has been discussed and negotiated mostly in the context of counter-terrorism. The relevant Common Foreign and Security Policy (CFSP) and Justice and Home Affairs (JHA) prerogatives of the EU are mostly the competency areas of the Council and the Commission. However, it is the European Parliament that has always been the most vocal proponent of enhanced data protection and privacy during negotiations with the US. But despite its intentions and ambitions, the EP often lacked the power to influence the negotiations such that privacy and data protection concerns were addressed to its satisfaction.

6.2.1 Passenger Name Records[33]

The agreements with the US with regard to Passenger Name Records (PNR), for example – records which were to be handed over to US immigration services and intelligence agencies at their command – were not well-received and heavily criticized by the EP and the Article 29 Working Party.[34] However, because the EP lacked any real power in this area – its obligatory involvement under the Consultation Procedure not stretching any further than being allowed to give its opinion – the PNR agreement was established

[33] An EU-based PNR system has recently been approved by the EP, as well as the mandate to start negotiations with the Council: <http://www.europarl.europa.eu/news/en/news-room/content/20150714IPR81601/html/Passenger-Name-Records-MEPs-back-EU-system-with-data-protection-safeguards>

[34] The Commission 'caved' in to US demands on PNR: <http://www.statewatch.org/news/2003/feb/11usdata.htm> while the EP adopted a critical resolution on it: <http://www.statewatch.org/news/2003/mar/uspass91564en.pdf> as well as Article 29 Working Party: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp87_en.pdf>

anyway.[35] Heavy criticism remained with subsequent revised PNR agreements because the EP's concerns were not sufficiently addressed; much to the resentment of various MEP's. As such, the EP's vocal defense of privacy and data protection became at the same time an institutional struggle for power (Pawlak, 2009; Ripoli Servent & Mackenzie, 2011; De Goede, 2012; Romaniello, 2013).

6.2.2 The SWIFT Affair

This struggle continued in the dialogues surrounding the SWIFT affair. SWIFT, the Society for Worldwide Interbank Financial Telecommunication, is an important globally operating enterprise facilitating international bank transfers. Hence, they deal with the exchange of financial data, which includes the PII of many European citizens. SWIFT's headquarters are in Belgium, and it used to also have a branch in Virginia.

After, and in response to, the terrorist attacks on September 11th 2001, the US government developed and set-up the Terrorist Finance Tracking Program (TFTP). In secret. In the context of this program, SWIFT was to be involved in investigations on many occasion. Such involvement entailed demands for financial data of EU citizens. Therefore, the Data Protection Directive applied. Having branches both in Belgium and in Virginia, however, SWIFT was bound by two vastly different jurisdictions when it comes to the protection of personal data. Hence, SWIFT was caught in a kind of Catch-22:

[35] See Commission decision of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers to the United States' Bureau of Customs and Border Protection, C(2004) 1914: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32004D0535&from=EN>
See also Council decision of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection, 2004/496/EC: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32004D0496&from=EN>
It eventually resulted in an agreement with the US on 28 May 2004 < http://ec.europa.eu/justice/policies/privacy/docs/adequacy/pnr/2004-05-28-agreement_en.pdf>

obeying US government demands would imply violating EU and Belgian law, while noncompliance with the US would be illegal from an American perspective.

When the TFTP program was revealed by the American press[36], the EP reacted vigilantly.[37] Of course, the Article 29 Working Party and the EDPS also strongly condemned the affair.[38] After a new temporary EU-US compromise due to the concerns raised, SWIFT announced their plans for a 'system re-architecture'.[39] This restructuring ensured that SWIFT would have its data stored solely in Europe. The United States thus no longer had the legal power to force SWIFT to hand over data, which created a major incentive for the US to renegotiate an agreement. The EP was kept in the dark about these negotiations; and when the EP found out, MEP Sophie in 't Veld (LIBE) requested access to the relevant documents. Yet EP demands were basically ignored and the interim agreement was signed without the EP's involvement exactly one day before the Treaty of Lisbon entered into force (De Goede, 2012; Romaniello, 2013). Art. 218 of the revised Lisbon TFEU would have required the EP to consent to such international agreements. The agreement was signed before this rule could be called upon (Ripoli Servent & Mackenzie, 2011).

[36] See Lichtblau, Eric & Risen, James (2006, June 23). Bank Data Is Sifted by U.S. in Secret to Block Terror. *The New York Times* <http://www.nytimes.com/2006/06/23/washington/23intel.html?pagewanted=all&_r=0> and Simpson, Glenn R. (2006, June 23). Treasury Tracks Financial Data In Secret Program. *The Wall Street Journal* <http://www.wsj.com/articles/SB115101988281688182>

[37] Public Hearing of the EP on the interception of bank transfer data from the SWIFT system by the US secret services: <http://www.europarl.europa.eu/hearings/20061004/libe/programme_en.pdf>

[38] Press Release on the SWIFT Case following the adoption of the Article 29 Working Party opinion on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT): <http://ec.europa.eu/justice/policies/privacy/news/docs/PR_Swift_Affair_23_11_06_en.pdf> and the Opinion of the European Data Protection Supervisor – Proposal for a Council Decision on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program (TFTP II)
<https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2010/10-06-22_Opinion_TFTP_EN.pdf>

[39] SWIFT (2007, June 15). SWIFT announces plans for system re-architecture.
<http://www.swift.com/about_swift/legal/swift_announces_plans_for_system_re_architect>

It is fair to say that the EP was treated rather badly here, and this treatment would indeed have its consequences. The first new SWIFT agreement was rejected by the EP, despite substantial lobbying efforts by United States officials (Monar, 2010; Ripoli Servent & Mackenzie, 2011; Romaniello, 2013). From that moment it was clear that the EP's concerns needed to be seriously addressed if an agreement was ever going to be reached. When new negotiations for a long-term agreement were called upon, it gave the EP the opportunity to use its newly gained power to influence the outcome of the negotiations. They had to approve of agreements made, and because of this, intensive cooperation was needed from the initial stages of negotiation (Cremona, 2011). After all, the agreement needed to be drafted in a way that would have the EP likely approve it (Romaniello, 2013).

The EP always seemed more concerned about data protection than the Commission and the Council. The EP's normative intent in the area of privacy and data protection can thus be considered higher. As an institutional component, the EP is perhaps the best example of a normative power within the EU as a whole. It is a normative power which used to lack the instruments to have its intentions and positions translate into actual impact. They simply lacked the necessary power. However, this changed when the Lisbon Treaty took effect. The increased institutional power should then have allowed the EP to have its intent translate into more impact.

The SWIFT case shows the EU internal inconsistencies on privacy and data protection. Hence, the shift in the institutional balance should have made the EU has a whole more of a normative power in the area of data protection than it was before. The normative intent in the area of data protection was always present in the EU, but the power underlying the intent was less present before the Lisbon Treaty than it was after. The increase in the underlying power has made the potential for impact higher. Its actions

should show whether the EP is making sufficient use of its extra powers, and the actual impact on third countries should show whether they are effective.

In that regard, Ripoli Servent & Mackenzie (2011) argued that as soon as it gained its new powers, the EP moderated its positions and became more prone to concessions to the security concerns raised by the Commission and the Council, and also the United States. *Under consultation – with only the power to give its opinion – the EP grew to be a clear data protection champion. However, this absolute position might be starting to erode. With the gain in decision-making powers, the EP has abandoned its policy preferences and acquired a taste for consensus and more moderate views* (Ripoli Servent & Mackenzie, 2011: 401). It appears that more political power and responsibility makes it less likely for an entity to take a strong position. An NGO, for example, lacks political power and does not have to compromise, and can therefore remain fully true to its convictions. A political institution with an ability to negotiate and actually influence policy-making, on the other hand, will often have to compromise with other political institutions. This is true for the EP, but also for the EU as a whole.[40]

In the SWIFT negotiations (at least in part a normative dialogue), the only EU institution taking a 'persuading' stance in the area of privacy and data protection is the EP, while the Commission and the Council were seemingly quite willing to concede to US demands, or perhaps even agreed with them. If a normative power is supposed to *shape* norms in external entities, the position of the Commission and the Council is not exactly fitting. The EP definitely appears most deserving of the title 'normative power'.[41] On the other hand, if it is true that the EP is moderating its positions now that they have more influence, this does not bode well for the prospect of the EU as a whole positioning itself as a normative power in this area. And even if the

[40] The same is true for opposition parties versus government parties in national parliaments.
[41] Aided of course by the EU's privacy watchdogs – the Article 29 Working Party and the EDPS.

EP, with its increased power at the negotiating table, is able to achieve some normative impact on US policies, the incentives for the US to change its behavior are unlikely to be based on the universal validity of the EP's privacy arguments. The fact that the US has only changed course when its own interests were at stake, shows clear strategic motivations for US action in this area.

Still, the fact that a company like SWIFT can decide to operate solely in the EU, putting the EU in a relatively dominant position in the negotiations involving the PII of European citizens, thus giving the EU nonviolent means to achieve normative impact where the means would otherwise be absent – and subsequently achieving such normative impact; this seems illustrative of the EU being a normative power. The EU is not using any force, certainly not military force, to achieve in the negotiations what it wants to achieve. If it wants to achieve normative impact and is in fact able to achieve it, to whatever extent, this indicates a kind of power. Though this power is probably political rather than normative[42], it does point to a willingness on the part of the EU to put strategic interests aside for the sake of a human right. And although the EU may not be internally consistent, the increased powers of the EP have made the EU at the very least more of a normative power in the area of privacy and data protection than it was before.

6.2.3 Safe Harbor

According to the Commission Decision on Safe Harbor (Com, 2010), the previously discussed adequacy decisions are to be extended to individual processors based in the United Sates. The adequacy decisions generally only apply to entire countries but the Commission has made an exception for individual data processors in the US, under certain conditions. Safe Harbor

[42] The arguments for the value of privacy were certainly not what persuaded the US to compromise.

(SH) is an opt-in program. However, access to the EU single market is conditional upon meeting the SH requirements, and due to the importance of the single market for many big US data processors, they really have no choice but to comply.

This is a clear example of the EU using economic leverage to induce change in an external actor; in this case US data processors desiring access to the single market. This economic power ensures a degree of normative impact on those US enterprises. The fact that the EU does not benefit economically from raising the requirements for access to its market, which actually creates additional barriers to trade with the US, seems to indicate an elevation of privacy concerns over economic concerns. This could be considered characteristic of a normative power.

However, it could also be looked at the other way around. According to Boehm (2014), if data of EU citizens is transferred to the US under SH, it is not possible to protect this data from then being subject to US law; and since US privacy law applies only to US citizens, EU data is not sufficiently protected. Even if the company protects its data to the satisfaction of the EU, it cannot guarantee that the US government has no jurisdiction over them. So even though it may create incentives for private organizations to improve their data protection policies; it may effectively weaken the data protection of EU citizens by lowering requirements and not taking into account US jurisdiction over companies under SH. It may be then be argued the EU has actually prioritized the economic benefit of removing barriers to trade over strict adherence to its own privacy and data protection standards; a strategic decision. It is a compromise which entails less data protection – at least from this perspective – of EU citizens, and may thus be considered not to be characteristic of a normative power in this area.

6.2.4 N.S.A.

In hindsight, the normative impact that the EU was able to achieve in the negotiations with the US is rather questionable. Edward Snowden leaked classified documents in 2013 which revealed that the US did not keep their side of the deal (to put it mildly) in the agreement with the EU.[43] The agreement with the EU entailed that, in the context of counter-terrorism, the US could attain (bulk) access to files possibly containing the PII of EU citizens, under certain conditions. Such conditions included sufficient regard for the privacy of EU citizens and their PII. That was what the whole controversy was about in the first place. Now, all of a sudden, it becomes known that the US were accessing the PII of EU citizens in even more ways than imagined in the agreements. And it was all done in secret; thus making the prior EU-US negotiations on this topic appear somewhat meaningless.

In March 2014, Snowden testified to the EP by video conference, and answered some of the many questions that ensued after his revelations[44]. His revelations brought to light that the NSA was even specifically targeting the EU in its spying activities[45]. The EU, and especially the EP, were infuriated by what they came to know. Although the debate had always been one with heated opinions on two distinctly opposite sides, the negotiations

[43] See Haase, Nina (2014, January 9). EU report reveals massive scope of secret NSA surveillance. *Deutche Welle*: <http://www.dw.de/eu-report-reveals-massive-scope-of-secret-nsa-surveillance/a-17352243> and the Draft Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs, 2013/2199 (INI): <http://www.statewatch.org/news/2014/jan/ep-draft-nsa-surveillance-report.pdf>

[44] Snowden testified before the EP by making an introuctory statements after which MEP's asked a variety of pointed questions: http://www.europarl.europa.eu/document/activities/cont/201403/20140307ATT80674/20140307ATT80674EN.pdf>

[45] See for example Poitras, Laura et al. (2013, June 29). Attacks from America: NSA Spied on European Union Offices. *Spiegel Online International*: <http://www.spiegel.de/international/europe/nsa-spied-on-european-union-offices-a-908590.html> and Poitras, Laura et al. (2013, August 26). Codename 'Apalachee': How America Spies on Europe and the UN. *Spiegel Online International* <http://www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625.html> and Fidler, Stephen et al. (2013, June 30). NSA Accused of Spying on EU. *The Wall Street Journal* <http://www.wsj.com/articles/SB10001424127887323936404578577053539567198>

were, and had to be, based on a degree of mutual trust. This trust has been befouled by secrecy and disreputable behavior. Moreover, this broken trust has had some major consequences.

The EP called, for example, for the suspension of the SWIFT agreement[46], while the upcoming negotiations about the Transatlantic Trade and Investment Partnership (TTIP) were called into question[47]. In an EU-US joint statement on March 26 2014, the importance of privacy and data protection within TTIP was reaffirmed[48]. Coming from the US, this statement is rather suspect, but they might have been happy to include it for reasons of PR. After all, the joint statement was a press release – a media effort. However, it seems unlikely for the US to actually make major alterations to its legal framework on privacy, which has long been judged inadequate according to EU standards. Therefore, negotiations that should involve privacy and data protection safeguards are always going to be difficult. An EU that is unwilling to compromise in the area of privacy, is an EU that will have a hard time coming to agreements with the US, but is also an EU that shows a willingness to stand strong on privacy in the face of opposition. A TTIP can have substantial economic benefits for the EU (Francois, 2013), but if it is

[46] European Parliament resolution of 23 October 2013 on the suspension of the TFTP agreement as a result of US National Security Agency surveillance, 2013/2831(RSP): <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P7-TA-2013-0449+0+DOC+PDF+V0//EN> See also Stearns, Jonathan (2013, October 23). EU Parliament Urges Freeze of Terror-Finance Pact With U.S. *Bloomberg:* <http://www.bloomberg.com/news/articles/2013-10-23/eu-parliament-urges-freeze-of-terror-finance-pact-with-u-s-1-> and Traynor, Ian (2013, November 26). NSA surveillance: Europe threatens to freeze US data-sharing arrangements. *The Guardian*: < http://www.theguardian.com/world/2013/nov/26/nsa-surveillance-europe-threatens-freeze-us-data-sharing>

[47] Directorate-General for External Policies, Policy Department's In-Depth Analysis of Civil society's concerns about the Transatlantic Trade and Investment Partnership. Page 16: <http://www.europarl.europa.eu/RegData/etudes/IDAN/2014/536404/EXPO_IDA(2014)536404_EN.pdf> See also BBC (2013, July 1). Hollande: Bugging allegations threaten EU-US trade pact. *BBC News:* < http://www.bbc.co.uk/news/world-us-canada-23125451> and < http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fTEXT%2bWQ%2bE-2013-008851%2b0%2bDOC%2bXML%2bV0%2f%2fEN&language=EN> which shows that some EU Member States suggest the TTIP negotiations should be suspended.

[48] EU-US Joint Statement of March 26 2014: <http://europa.eu/rapid/press-release_STATEMENT-14-84_en.htm> to *"reaffirm our strong partnership*".

willing to jeopardize those benefits for the sake of a fundamental right such as privacy, this is certainly characteristic of a normative power.

Especially the EP has taken a strong and clearly normative position in the TTIP negotiations: *…to negotiate provisions which touch upon the flow of personal data only if the full application of data protection rules on both sides of the Atlantic is guaranteed and respected to cooperate with the United States* ***in order to encourage third countries to adopt similar high data protection standards around the world***.[49] The EP even recommended making the approval of the TTIP conditional on the US dismantling their mass surveillance activities.[50] It remains to be seen what will actually happen, but with the EP having to consent to this international agreement, it holds the key to ensuring US concessions on data protection. It holds the key to achieving normative impact.

The NSA scandal also enticed the EP to call for the suspension of Safe Harbor[51], while conclusions from the Commission about the adequacy of the SH agreement include a recognition that the NSA scandal is cause for 'serious concern'.[52] There is no doubt that the Commission is less outspoken about the issue. The recommendations following its conclusions are a mere repetition of conditions that were already known to the US before the NSA scandal. However, Commissioner Viviane Reding has said that*: Safe Harbour*

[49] Report containing the European Parliament's recommendations to the European Commission on the negotiations for the Transatlantic Trade and Investment Partnership (TTIP), 2014/2228(INI): <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A8-2015-0175+0+DOC+PDF+V0//EN>

[50] EU-US negotiations on TTIP: A survey of current issues. In-Depth Analysis by the EPRS: <http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/559502/EPRS_IDA(2015)559502_EN.pdf>

[51] See LIBE Committee Inquiry: Electronic Mass Surveillance of EU Citizens. Protecting fundamental rights in a digital age: Proceedings, Outcome and Background Documents: <http://www.statewatch.org/news/2014/may/ep-LIBE-Inquiry-NSA-Surveillance.pdf> and EP Press Release: US NSA: stop mass surveillance now or face consequences. *12-03-2014:* < http://www.europarl.europa.eu/news/en/news-room/content/20140307IPR38203/html/US-NSA-stop-mass-surveillance-now-or-face-consequences-MEPs-say>

[52] Communication from the Commission to the European Parliament and the Council on the functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, COM(2013) 847 final: <http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf

is not safe at all – that is why we have put 13 recommendations to our American counterparts – these are non-negotiable. Safe Harbour is a European Commission decision to implement, in order to make it easier for EU-U.S companies to exchange data. We are discussing these 13 points; so far 12 have been answered in a positive way – the 13th point not yet. And for me it is very clear: I have made it clear to my counterparts that the 13th point must be clarified for the European Commission to finally say that Safe Harbour is "safe".[53]

This was reiterated by Commissioner Véra Jourová, who claimed that she had made it very clear that the EU was going to be strict about how the rules of Safe Harbour were applied by the US. On the 13th point that Reding had already spoken of was, however, still no agreement. This 13th point unsurprisingly had to do with National Security derogations. Nevertheless, Jourová intended to finalize talks in May 2015.[54] On June 3, Jourová said the following in a speech: *On Safe Harbour, with the Department of Commerce, we have achieved solid commitments on the commercial aspects. However, work still needs to continue as far as national security exemptions are concerned. Discussions will continue, with the aim of achieving a robust revision of the Safe Harbour framework in the near future*.[55] In other words, the negotiations are still stuck at point 13.

So even though the initial statement by Viviane Reding was powerful – the recommendation being *non-negotiable* – the fact that talks with the US have been going on for a while, without apparent progress, seems indicative of a lack of persuasive means; a lack of power perhaps. However, the

[53] Justice Council press conference by Viviane Reding, 06-06-2014: < http://europa.eu/rapid/press-release_SPEECH-14-431_nl.htm>
[54] Vincenti, Daniela (2015, March 13). Věra Jourová: We will be strict with the US on Safe Harbour. Euractiv: <http://www.euractiv.com/sections/infosociety/vera-jourova-we-will-be-strict-us-safe-harbour-312856>
[55] Press speaking points of Commissioner Jourová at the EU-US Justice and Home Affairs Ministerial Meeting in Riga, 03-06-2015. *European Commission Press Release Database*: <http://europa.eu/rapid/press-release_SPEECH-15-5112_en.htm>

negotiations are also stuck because the EU itself does not want to compromise on data protection any longer. The negotiations have two parties, and both are resistant to compromise; hence no progress is made. The EU's position in the negotiations is based on its intention to protect privacy and personal data; and that can be considered characteristic of a normative power in this area. Dependent on the EU's power in relation to the US, it remains to be seen how much normative impact can be achieved through these negotiations.

The NSA scandal has shown that the US initially may not have taken the EU's calls for more privacy safeguards in their bilateral agreements very seriously. The US were never actually persuaded. They just pretended to be by signing the agreement and then secretly not doing what they said they would. However, now that the truth is out, and with public opinion mostly siding with the privacy proponents, the US is to an extent forced to submit to public demands, which happen to largely align with EU demands, at least in principle. The continuous fight for more stringent privacy safeguards on the part of the US, also in its foreign relations, may then finally have some results. The current zeitgeist, more than in the past, lends itself for increased normative impact to be achieved in the area of privacy and data protection.[56]

6.3 Court rulings

Another important independent actor within the EU is the European Court of Justice (ECJ). The ECJ has shown in recent years to be willing to make consequential decisions in the area of privacy and data protection. Since the

[56] In fact, some changes are already being made in the US with, for example, the USA Freedom Act being approved by the US Senate and signed by Barack Obama. See Zengerle, Patricia (2015, June 2). Obama's signature on the Freedom Act reverses security policy that's been in place since 9/11. *Business* Insider: <http://www.businessinsider.com/obamas-signature-on-the-freedom-act-reverses-security-policy-thats-been-in-place-since-911-2015-6>

Charter of Fundamental Rights became binding with the ratification of the Treaty of Lisbon, the number of ECJ rulings which referred to it saw a significant increase (Búrca, 2013). When the Lisbon Treaty took effect, the ECJ was suddenly tasked to rule on issues it had little experience with, unlike, for example, the European Court of Human Rights. However, as Búrca (2013) has shown, the ECJ has been interpreting Charter provisions largely in isolation. It has not made much use of external 'input' by human rights organizations and prior human rights jurisprudence. Búrca fears that this could make present and future ECJ case law that involve such issues 'insufficiently informed'. Búrca argues that the ECJ should be *more open to the jurisprudence of other human rights bodies and courts, and to hearing argument from those with relevant expertise on the human rights issues arising before it* (2013: 179).

Nonetheless, the insufficiently informed ECJ has ruled largely in favor of privacy and data protection. While particular cases involving considerations of privacy perhaps did not sufficiently take into account other fundamental rights or used seemingly simple and one-sided reasoning where comprehensive discussion would be justified; their outcomes gave the impression of ECJ judges elevating privacy concerns over other concerns. This paper will make no judgment on the desirability of the ECJ ruling in this manner generally, but will rather take these court decisions as given, and analyze them in light of their impact and possible contributory role in making the EU a normative power in the area of privacy and data protection.

6.3.1 Data Retention Directive

Directive 2006/24/EC, or the Data Retention Directive (DRD), was adopted on March 15, 2006.[57] It was one more example of privacy-infringing legislation being adopted in the context of a *heightened alert of imminent terrorist attacks*.[58] It gave Member States guidelines on how long to retain stored data of various kinds.[59] The purpose of the directive was to give authorities responsible for criminal investigations the necessary means to effectively fight crime. Data being retained for a certain amount of time would give such authorities the option of accessing this data on request, whenever deemed necessary for resolving a particular criminal case. The Commission has provided evidence for the necessity of data retention legislation with reference to empirical data and specific cases in which the absence of the retained data used in those cases would supposedly have made it impossible to solve them.[60] The DRD was considered an essential element of European cooperation in combatting borderless crime.

A Commission evaluation, released on April 18 2011, concluded in favor of the DRD and its stated aims.[61] It did, however, also give brief consideration of its detrimental effects on privacy and data protection of EU citizens, protected under article 7 and 8 of the Charter. Data retention constitutes an interference with these two fundamental rights, and is therefore required under article 52(1) of the Charter to be necessary and proportional. It may be argued, in line with the Commission's reasoning and supporting evidence,

[57] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF>
[58] Report from the Commission to the Council and the European Parliament – Evaluation report on the Data Retention Directive (Directive 2006/24/EC): <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:en:PDF>
[59] A minimum of six months and a maximum of twenty-four months.
[60] European Commission – Evidence for necessity of data retention in the EU: <http://ec.europa.eu/dgs/home-affairs/pdf/policies/police_cooperation/evidence_en.pdf>
[61] See note 53

that data retention is necessary for public safety and crime prevention; maybe even for national security. The question then remains whether it is also proportionate.

The DRD had already received strong criticism from by means of, for example, a letter collectively signed by stakeholders to Commissioner Malmström.[62] More letters were sent to Malmström after this and increased in their elaboration.[63] They found the Directive to be incompatible with the Charter, unnecessary in achieving its objective and not proportional to what it aimed to achieve; and they provided plausible evidence to support their case. Their arguments underlined the harm done by mass surveillance and blanket data retention, and the importance of minimizing any potential infringement on the right to privacy and the protection of personal data.

As such, there were two sides in the debate about the DRD: the proponents, such as the Commission, on the one side; and the opponents, which mostly included civil and human rights organizations, on the other. The EP, shown to be a privacy proponent in other areas, was claimed by some to have 'sold out' with regard to the DRD (Peers, 2005). According to Ripoli Servent & Mackenzie (2011:393) the DRD is the most evident example of the EP moderating its position after gaining more power; something they supposedly also did with regard to the SWIFT agreement. However, when the civil and human rights organizations started vocalizing their discontent, the EP also began to demand reforms and improvements to the DRD.[64]

[62] Letter to Cecilia Malmström: <https://www.privacyinternational.org/sites/privacyinternational.org/files/dr_final.pdf>
[63] See for example the letter signed on September 3 2010: <http://www.statewatch.org/news/2010/dec/eu-mandatory-data-retention-civil-society-letter-10.pdf> and the one sent on September 26 2011: <http://www.aedh.eu/plugins/fckeditor/userfiles/file/Actualit%C3%A9s%20des%20ligues%20membres/EDRI%20letter%20to%20Commissioner%20Malmstr%C3%B6m%2026_09_2011.pdf>
[64] European Parliament News. MEPs cast doubt on controversial rules for keeping data on phone and internet use. Newsroom: <http://www.europarl.europa.eu/news/en/news-room/content/20121019STO53997/html/MEPs-cast-doubt-on-controversial-rules-to-keep-data-on-phone-and-internet-use>

All the while in 2012, the ECJ received requests for preliminary rulings on cases C-293/12 and C-594/12 concerning the validity of the DRD, which became all the more relevant in light of the NSA scandal a year later. On April 8 2014, the ECJ ruled the DRD to be invalid.[65] The DRD *entails a wide-ranging and particularly serious interference with the fundamental rights to respect for private life and to the protection of personal data, without that interference being limited to what is strictly necessary*.[66] The ECJ acknowledged that the retention of data under DRD may be appropriate in light of its objective, but that the Directive in its current form did not constitute an appropriate means to its ends, due to it being an excessive infringement on privacy and data protection.[67]

The ECJ coming to the conclusion it did is an example of the ECJ elevating privacy concerns over potential other concerns. Whether or not one agrees with the ECJ's verdict, it cannot be denied that the ECJ acknowledges the value of privacy and data protection and of the Charter articles protecting these values. It effectively accomplished what various NGO's already wanted to achieve.[68] There is still uncertainty about what the decision will mean for data retention legislation in individual member states.[69] On the whole, however, the ECJ holds substantial power within the EU. Its decisions are binding. Therefore, an ECJ ruling in favor of privacy and data protection is an

[65] Court of Justice of the European Union. Press Release No 54/14 on the Judgment in Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others. *April 8* 2014: <http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf>
[66] *Idem*
[67] Although the ECJ nowhere specifically referred to the communications of the civil and human rights organizations, its reasoning is remarkably similar. So while it is difficult to tell whether the arguments made by the NGO's directly influenced the eventual verdict, it is also unlikely that the ECJ judges were totally unaware of them. Therefore, where Búrca (2013) fears an insufficiently informed ECJ, in this case it could be argued that it was sufficiently informed for them to come to the same conclusions.
[68] The ECJ can thus be said to act in a normatively coherent manner.
[69] This question was already vocalized by Sophie in 't Veld in a letter to Commissioner Malmström after the ECJ ruling: <http://ec.europa.eu/carol/index.cfm?fuseaction=download&documentId=090166e59724b7c6&title=29.04.2014_Letter to Commissioner Malmström on judgment data retention directive - signed.pdf> Her question gains legitimacy in light of recent events in Belgium < https://edri.org/belgian-constitutional-court-rules-against-dataretention/>, Germany <https://edri.org/data-retention-german-government-tries-again/>, and the Netherlands <http://blogs.wsj.com/digits/2015/03/11/dutch-court-strikes-down-countrys-data-retention-law/>

ECJ that makes the EU more of normative power than would otherwise be the case.

6.3.2 The Right to be Forgotten

Since the beginning of time, for us humans, forgetting has been the norm and remembering the exception. Because of digital technology and global networks, however, this balance has shifted. Today, with the help of widespread technology, forgetting has become the exception, and remembering the default.[70]

Our tendency to retain rather than discard information has increased corollary to the decrease in the cost of retention (Mayer-Schönberger, 2007). Our enhanced ability to analyze data for various purposes makes data more valuable, and the retention of said data fruitful and worthwhile. The internet has proven an immense and ever-expanding repository of stored data, which tends to remain stored for unspecified periods of time. At the same time, access to such data has been made relatively easy by the advent of search engines such as Google. The data stored on the internet, retrievable through search engines, also includes personal data. Hence, access to personal data has been made easier as well. And this has had some significant implications.

In 2010, Consteja González filed a complaint against a Spanish newspaper and Google Spain. In this he was supported by the Spanish national data protection agency (AEPD). González complained about the fact that when one would search for his name on Google, the search results would include references to his past which reflected negatively on him. They referenced his former home being repossessed and put up for auction. At the time, he was

[70] Mayer-Schönberger (2011: 2).

in debt and was unable to fulfil his financial obligations. These issues were eventually resolved, but references to them still appeared on Google. González and the AEPD found this to infringe on his right to privacy.

González' case was not the only one of its kind. Of course, not all of them ended up in a court room, but there are plenty of situations imaginable wherein people are negatively affected by publically accessible information related to them that lingers on the internet.[71] Dark chapters of one's past are a mouse-click away from resurfacing. The internet remembers what is perhaps better forgotten. To provide mitigation for such problems, a so-called 'right to be forgotten' was proposed and widely debated. According to Xanthoulis (2013: 98), this right is a 'specific expression of a multidimensional right to privacy'. It entails an opportunity for individuals to have information relating to them, which is inaccurate or no longer relevant, deleted from its source. This ought to give people more control over their personal data on the internet.

While the debate around the right to be forgotten mostly revolved around the value of the right to privacy as compared to other rights and freedoms[72], and about its potential detrimental effects on those other rights and freedoms; most would agree that a right to be forgotten does enhance one's privacy and protects one's personal data. Wanting to create such a right can therefore justly be considered part of normative intent, albeit only in the area of privacy and data protection.

[71] There is the often cited example of Stacy Snyder, an aspiring teacher who, despite having excellent qualifications, was denied certification. A Myspace picture of her dressed as a pirate and holding a plastic cup, titled 'drunken pirate', supposedly disqualified her as a role model for kids (Mayer-Schönberger, 2011:1). While the initial posting could be deleted, copies of the picture could not, and were still a mere search command away from being found. Another striking example was given in a comment on a Guardian article by user *Owakahnige*.[71] His 10 year old son's mother was murdered when he was a baby. News reports of this past tragedy are still traceable to his name when searching for it on Google.

[72] Rosen, Jeffrey (2012, February 13). The Right to be Forgotten. *Stanford Law Review*: <http://www.stanfordlawreview.org/online/privacy-paradox/right-to-be-forgotten?em_x=22>

In a 2010 press release, Commissioner Viviane Reding first mentioned the idea of a right to be forgotten in the context of protecting data in the online single market and fully supported it.[73] A conditional right to 'erasure' was already implied in article 12 of Directive 95/46 but it was more literally codified in the Commission's draft proposal for a GDPR under article 17. The Commission being the initiator of reform, at least on the political level, and Commissioner Reding being so outspoken about the inclusion of a right to be forgotten; it seems that the Commission for once led the EU in acting on its supposed normative intentions.

In 2014, the aforementioned Consteja González case ended up developing into the ECJ court case that came to be associated with the right to be forgotten. Initially, the matter was to be resolved in the Spanish court, but this court referred the following questions to the ECJ for preliminary ruling:

1 Does the 1995 data protection directive apply to search engines like Google?
2 Does EU law apply to Google Spain, since its servers are in the US?
3 Do individuals have the right to request information be removed under the right to be forgotten?

On May 13 2014, the ECJ essentially answered 'yes' to all three of these questions, thus 'establishing' the right to be forgotten.[74] However, despite the fact that Case C131/12 came to be known as the 'right to be forgotten' case, the ECJ did not actually invent anything new. It only interpreted an

[73] Speech/10/327 by Viviane Reding on Building Trust in Europe's Online Single Market. *22-06-2010*: <http://europa.eu/rapid/press-release_SPEECH-10-327_en.htm> [73] In a speech that same year, she said the following: *Personal data can easily be stored and then even more easily multiplied on the Web. But it is not easy to wipe it out. As somebody once said: "God forgives and forgets but the Web never does!" This is why "the right to be forgotten" is so important for me. With more and more private data floating around the Web – especially on social networking sites – people should have the right to have their data completely removed."* Speech/10/700 by Viviane Reding on Privacy Matters – Why the EU needs new personal data protection rules. *30-11-2010: <http*://europa.eu/rapid/press-release_SPEECH-10-700_en.htm>

[74] Judgment of the Court (Grand Chamber) in Case C-131/12. Request for a preliminary ruling under Article 267 TFEU from the Audencia Nacional (Spain): <http://curia.europa.eu/juris/celex.jsf?celex=62012CJ0131&lang1=en&type=TXT&ancre=>

already existing right to erasure codified in Directive 95/46 (Bunn, 2015). The case was, on the other hand, undoubtedly consequential and its effects immediately visible. After all, the case specifically applied to Google, one of the largest and most influential companies in the world, and ruled to be a data processor according to the ECJ's interpretation of article 2(b) and 2(d) of Directive 95/46. The new right to be forgotten implied a new 'obligation to forget' for Google.[75] Google has already processed over a quarter million requests for the deletion of over a million URLs; a little over 40% have so far been granted.[76] The proven impact of the ruling exemplifies the power of the EU judiciary branch.

The ruling in Case C-131/12 is another example of the ECJ ruling in favor of privacy. In fact, it seems even to clearly elevate one fundamental right over the other; article 7 and 8 of the Charter over article 11. Article 11 concerns the freedom of expression and information – not an unimportant freedom – and the ECJ did not even mention this article in its verdict. While this could be considered an example of the ECJ not being sufficiently informed or being improperly minimalistic and simplistic in its reasoning, which would make Búrca's (2013) fear at least partially justified; it does indicate a presence of normative intent in the area of privacy and data protection underlining the ECJ's judicial power. And normative intent underlined by power makes normative impact much more likely.

The ECJ's interpretation of article 4(1)a of Directive 95/46 also effectively widened the Directive´s scope of application. The ECJ decision ensured that enterprises operating in the single market are bound to EU law even when their servers are not located in Europe. It thus increased the potential for normative impact because data processors that are established in a third

[75] 'To be forgotten' is an action performed on the subject by someone else; therefore a 'right' to be forgotten implies an obligation for another to forget you.
[76] Google Transparency Report. European privacy requests for search removals (data last updated: July 16 2015): <http://www.google.com/transparencyreport/removals/europeprivacy/?hl=en>

country, yet conduct commercial activities in the single market, like Google, are now bound by EU privacy standards for processing personal data.[77] The ECJ has thus used its judicial power largely in support of privacy and data protection. Whether or not this is proof of normative intent on the part of the ECJ, its power certainly raises the potential for normative impact and contributes to making the EU more of normative power in the area of privacy and data protection.

[77] This decision stands in remarkable contrast with the events surrounding the total relocation of SWIFT's servers to the EU. By moving all of its servers to the EU, SWIFT positioned itself beyond the reach of US jurisdiction (at least in theory). The ECJ has now ruled that server location is no barrier for EU law to apply.

7 Normative Impact

Increased cross-border activity spawns jurisdictional overlaps. (Shaffer, 2000: 3)

Before Directive 95/46 took effect, data transfer bans from one EU Member State to another were a regular occurrence. Transfers from states with higher relative protection, such as Germany and France, to states with lower relative protection, such as Italy, would on occasion be blocked because data protection laws in the latter states were deemed to provide inadequate protection of PII (Shaffer, 2000). Because data transfers are an increasingly important condition of efficient cross-border trade, data transfer bans constitute a barrier to such trade. The Directive was aimed at harmonization of data protection laws; and this harmonization, aside from guaranteeing a high level of protection, was aimed at lowering barriers to trade within the EU caused by the divergence in data protection laws.

While contributing to the liberalization of EU internal trade on the one hand, Directive 95/46 also created barriers to trade with third countries. Adequacy requirements entail data transfer bans to third countries with lower relative protection. A comparison with the pre-Directive situation in the EU is then easily made. Its solution would then supposedly be to also harmonize data protection laws on a global scale. However, this is easier said than done. The EU has no jurisdiction over third countries. As such, it requires other means to induce change and de facto harmonization. It requires other means to achieve normative impact.

7.1 Impact on individual enterprises

"There is only one program of privacy protection at Microsoft," and it's Europe's, says Richard Purcell, Microsoft's director of corporate privacy.[78]

Third countries are not bound by EU law. Therefore, they need other incentives to change. While the EU may actively promote the adoption of data protection standards of a higher level, EU external actors are often more persuaded by economic incentives than they are by moralistic pandering. This is confirmed by the so-called 'Brussels Effect'. The Brussels Effect describes the phenomenon of EU regulations affecting citizens around the world, and not merely those residing within the EU itself (Bradford, 2011; 2012; 2014). It constitutes an extension of the 'California Effect', which describes the phenomenon of larger jurisdictions setting regulatory standards for smaller ones due to the importance of their markets (Vogel, 1995; Bradford, 2012; 2014). California, the largest market in the US, also happens to apply relatively strict regulations, especially in the environmental sector (Vogel, 1995). Large markets are an attractive target for exporters, but to export to California, businesses have to meet the relatively high applicable standards. In this way, California is able to export its own standards to individual enterprises, but also to other US states.

The same could be observed in Europe. Germany and France, due to the importance and relative size of their markets compared to other EU Member States, had the economic 'leverage' to raise collective EU data protection standards to their own higher level. A smaller Member State would not have had the same bargaining power. *It was the convergence of interests of*

[78] Mitchener, Brandon (2002, April 23). Rules, Regulations of Global Economy Are Increasingly Being Set in Brussels. *The Wall Street Journal*: <http://www.wsj.com/articles/SB1019521240262845360> see also Bowcott, Owen (2015, March 24). Facebook data privacy case to be heard before European Union Court. *The Guardian:* <http://www.theguardian.com/technology/2015/mar/24/facebook-data-privacy-european-union-court-maximillian-schrems> and Schechner, Sam (2014, September 25). EU Privacy Watchdogs Warn Google About Its Policy. *The Wall Street Journal:* <http://www.wsj.com/articles/eu-privacy-watchdogs-warn-google-about-its-policy-1411666047>

powerful states, backed by large markets, to both facilitate free information flows and retain stringent data privacy controls which permitted the Directive to go forward. It was France and Germany's political exploitation of market power than enabled protection to be traded up throughout the EU. (Shaffer, 2010: 13)

In line with these observations, the EU, as the largest market in the world, should have this same potential. And this is where the Brussels Effect comes in. The EU has been able to export its standards globally through 'unilateral regulatory globalization' (Bradford, 2011; 2012; 2014). *Unilateral regulatory globalization is a development where a law of one jurisdiction migrates into another in the absence of the former actively imposing it or the latter willingly adopting it.* (Bradford, 2014: 2) Bradford explains how the opportunity costs of resisting adaptation to the EU's high standards are too high. The EU's market power creates 'involuntary incentives' for adaptation. As such, the influence of EU regulation is not the intended result of active persuasion or promotion of EU norms, but rather the unintended consequence of EU acts and aspirations, underlined by its substantial market power (idem).

The EU's market power combined with its relatively strict market regulations sheds an alternative light on globalization. For many, globalization connotes downward pressures on domestic regulatory standards and social protections. Commercial enterprises would target markets with low relative standards, incentivizing states to lower their standards in order to attract such enterprises. This expectation, however, is at least partially negated by the California Effect in that enterprises operating on a global scale have found the benefit of adopting one uniform global high standard to weigh up significantly to adopting multiple lower standards (Bradford, 2011; 2012; 2014; Shaffer, 2000). *Internet companies find it difficult to create different*

programs for different markets and therefore tend to apply the strictest international standards across the board. (Bradford, 2012: 25)

The EU's market is too important for most globally operating enterprises to risk forfeiting access by not adapting to EU standards. Such enterprises will therefore recognize the necessity of adaptation. Because uniform global standardization is economically preferable to applying different standards in different markets, the only prudent option is for enterprises to adopt the highest standard among the most important targeted markets. The EU's tendency to maintain high relative standards in addition to it being the largest market in the world, should thus effectively imply that enterprises are most likely to adopt EU standards rather than those of other jurisdictions. After all, high commercial standards are acceptable in low standard markets, but not vice versa. Adopting the high relative standards of the EU should thus grant access to all targeted markets.

The Brussels Effect entails a major potential for the externalization of EU norms, including privacy and data protection norms. The importance of the single market gives the EU leverage for triggering desired change in external entities. The external entities affected by the Brussels Effect are individual enterprises first and foremost. Independent of third country governments, foreign enterprises are incentivized to change policy for economic reasons. Initial single market access being one of them, the motivations for complying with privacy and data protection regulations extend also to deterrents to noncompliance.[79] That is why the EU in its proposed GDPR intends to include significant fines for enterprises failing to comply with data protection rules.[80]

[79] The Ponemon Institute (2011) conducted a study which showed that while the cost of compliance is great, the cost of noncompliance is far greater. Of course, for any regulation to make any sense at all, the cost of noncompliance should be higher than that of compliance.
[80] European Commission Press Release. Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses. *25-01-2012:*

The EU has the power to anticipate on the economic incentives of commercial enterprises. Foreign enterprises, who are not bound by EU law yet are unwilling to forfeit single market access or risk fines, are likely to adapt to the EU's high relative regulatory standards. This gives the EU additional and, more importantly, effective means to create de facto jurisdictional overlaps. It gives the EU the power to shape global regulatory standards, including those of privacy and data protection, thus enabling the EU to achieve substantial normative impact abroad. Such impact is illustrated by the fact that numerous US enterprises have adapted policy, though perhaps reluctantly, to meet Safe Harbor requirements.[81] Big US corporations are by necessity adopting EU privacy standards. Even where US enterprises have tried to circumvent EU data protection standards by maintaining its data processing activities elsewhere, such as Google in the Right to be Forgotten case, the ECJ has ruled EU law still applicable. The ECJ has thereby increased the strength and scope of the Brussels Effect.

The single market therefore is and remains the EU's seemingly most effective source of power (Damro, 2012). It gives the EU options and opportunities that it would otherwise not have. However, this market power is no sufficient condition for regulatory externalization. It also requires political means such as 'regulatory capacity and propensity' (Bradford, 2014). The EU's regulatory capacity and propensity in the area of privacy and data protection is confirmed by the upcoming GDPR. As a regulation rather than a directive, the regulatory capacity of the EU should increase; and because the regulation is meant to enhance protection in this digital era, the EU's regulatory propensity is ensured as well. With an ECJ's ruling having even enhanced the EU's regulatory scope, this observation gives

<http://europa.eu/rapid/press-release_IP-12-46_en.htm> *Independent national data protection authorities will be strengthened so they can better enforce the EU rules at home. They will be empowered to fine companier that violate EU data protection rules. This can lead to penalties of up to €1 million or up to 2% of global annual turnover of a company*.

[81] US-EU Safe Harbor List: <https://safeharbor.export.gov/list.aspx>

credence to the notion that a normative power requires other 'forms' of power to be effective. Economic and political means are much more likely to achieve normative ends than any supposed 'normative means' would.

7.2 Impact on third country legislation

Although the US has waged a vocal campaign against Europe's approach, it has failed to contain the spread of European rules. Seven countries – including leading economies such as Japan, Canada, and Australia – that previously shared the US approach have switched to Europe's comprehensive system. (Bach and Newman, 2007: 833)

Third country governments are constrained in their ability to retaliate against the EU and its strict data protection regulations, because WTO rules do not allow it. WTO rules thus constitute a 'shield' against foreign governments who disapprove (Shaffer, 2000). But this is consequential only if those foreign governments are actually desiring retaliation. The evidence, rather, shows that they are not. More and more other countries are willingly adopting their own data privacy laws, and are measurably influenced by EU regulatory standards (Greenleaf, 2012; 2015). In the area of data protection, European regulations have become the aspired international standard (Shaffer, 2000).

The particular influence of EU regulations is measured by those provisions and requirements that are found in Directive 95/46 but not in for example the OECD Guidelines or the APEC framework (Greenleaf, 2012). There are, of course, elements common to all data protection laws, and those could therefore be seen as most influential. However, there are also those elements which were initially unique to the EU approach, which are not present in other transnational frameworks, and are not always present in

national data protection laws outside the EU. Such elements being adopted by third country legislatures may be considered evidence of EU standards influencing decision-making abroad.[82]

Graham Greenleaf (2012) identified 10 elements which are supposedly 'European' in that none of those elements are recommended or mandated by the OECD or APEC, such as the presence of an independent Data Protection Authority, judicial protection against violations of data privacy rights, obligations for data processors to use data only to the extent necessary for some declared purpose, etc. Greenleaf's findings confirm the influence of EU data privacy laws in the 33 countries that were included in the study. Nineteen had seven or more European elements, while thirteen had at least nine. His latest research confirmed that 109 countries have so far already enacted data privacy laws (Greenleaf, 2015).

The influence of EU data protection regulations on legislation abroad takes differing trajectories, and are often determined by linguistic factors.[83] South- and Middle-American countries, such as Argentina, Uruguay, and Mexico are influenced by Spain's data protection law (Eustace and Bohn, 2013), while Macau's Personal Data Protection Act[84] is known to be based on Portuguese law (Greenleaf, 2008; 2012). On the other hand, a country like South-Korea, whose amended data protection law became effective on November 29 2014[85], has no apparent links with European states or languages yet has been seemingly influenced by as much as nine of the European elements

[82] Greenleaf (2012) recognizes that it is difficult to know for certain whether laws adopted by third country governments are actually influenced by EU regulation. It is challenging to prove direct causation. However, reasonable inferences can be made.
[83] See for example <http://www.redipd.org/> ; and Eustace and Bohn (2013) for the influence of Spanish data protection laws on adopted legislation in third countries, primarily in South-America, through the Spanish language; and <http://www.afapdp.org/> for a data protection association using the French language as means for spreading privacy ideas and influencing relevant law.
[84] Macao Act 8/2005. Personal Data Protection Act <http://www.gpdp.gov.mo/uploadfile/2013/1217/20131217120421182.pdf>
[85] The Act on Promotion of Information and Communications Network Utilization and Data Protection, Etc. <http://koreanlii.or.kr/w/images/d/df/DPAct2014_ext.pdf>

(Greenleaf, 2012). Therefore, though linguistic factors are influential, they are no prerequisite.

There are various explanations imaginable for the far-reaching influence of EU data protection rules. The first is that third country governments simply recognize the inherent value in having stricter rules for protecting their citizens' privacy and PII, and consider that copying EU rules would have such effect. Another plausible reason is that they have considered the economic benefit of adopting EU rules rather than rules applying in jurisdictions with lower relative protection. Although tougher regulations often entail a higher administrative burden for enterprises as well as government; adoption of EU standards would increase the likelihood of them meeting the EU's adequacy requirements, thus effectively enabling additional trade to take place between the EU market and theirs. Yet another explanation is that third country governments consider the merit of commercial enterprises or other governments recognizing the ability to ensure adequate protection and means to process trans-border data flows, thus making them a more attractive target for trade.[86]

There is no definitive answer to the question of '*why?*' It is difficult to tell what the actual incentives are for third country governments to change their data protection laws. It could have multiple reasons for that matter. Providing clear-cut evidence for the incentives of foreign governments to change is beyond the scope of this paper. It is apparent, however, that EU regulations in the area of privacy and data protection are having significant impact beyond EU borders. The Brussels Effect explains how economic considerations incentivize individual foreign enterprises to adapt to EU

[86] Commission (2012c: 39)

standards, while the governments who should supposedly exercise jurisdiction over these enterprises are visibly following suit.[87]

[87] While it is less clear what drives legislative changes abroad, Bradford (2014) considered the possibility of enterprises lobbying their respective governments to change policy in order to level the playing field domestically, because domestic enterprises who are less export-oriented and thus less dependent on and influenced by foreign jurisdictions, would supposedly have a local competitive advantage otherwise.

8 Conclusions

In conclusion of this paper, the PPE ideal type features are revisited in light of the findings in previous chapters.

PPE should have the intent to defend, promote and spread the privacy norm.

While EU legislation covering data protection and the implicit right to privacy are in its application limited by its territorial scope, the texts do hint at an underlying 'higher goal'. Provision 2 of the DPD as well as the inclusion in the Charter of the right to private life and data protection under articles 7 and 8 respectively, indicate an acknowledgment of these rights being applicable to 'individuals', and not merely those residing in the EU. One may conclude on that basis that although EU action is oftentimes limited by practicalities and bounded jurisdiction, its relevant policies are intended to affect, in the best scenario, individuals outside the EU as well. Article 21 of the TEU codifies this intention. EU action in line with this intent is therefore consonant with a cosmopolitan mindset.

That is, if and only if one presumes or accepts the universal validity of the privacy norm, of course. This universal validity is partly assumed but to a large extent also confirmed by the evidence. NGO's consisting of thinkers of all kinds of different backgrounds are more than ever acting, writing and speaking in defense of the assumed fundamental right to privacy. The revelations of Edward Snowden about the NSA's indiscriminate and intrusive surveillance activities caused a monumental backlash against governments violating individual privacy, while at the same time lending substantial momentum to the ideational spread of the privacy norm. Nations around the world are or have been enacting data privacy laws. The EU does not stand alone in its normative intentions, and should not refrain from taking the lead on this issue, and to be more effective than others ever could.

PPE should act in accordance with the privacy norm and should show internal consistency in doing so.

The EU does not consist of a single entity and is not uniform in its positions and approaches. The EU consists of various institutions, which in turn consist of even more individuals, all having their own views and opinions. General observations can, however, be made. The EP has been most vocal and most adamant about defending and promoting privacy and effective data protection. In comparison, the Commission and the Council have clearly taken more moderate views, and have, much more often than the EP, taken a less normative position in the negotiations with the US. The Commission and Council were more willing to compromise, and this tendency to compromise may be related to the underlying power of the entities taking part in the negotiations. The EP as well apparently moderated its position when its power was enhanced.

The EU can thus not be said to show internal consistency in its positions and actions when it comes to privacy and data protection. Even though it is difficult for anyone to deny the importance of privacy, the EU seems very much divided on its comparative value, and does not always prioritize defending its privacy standards to strategic considerations. The NSA revelations, however, have seemingly brought back the fervor in the EU's defense of the privacy norm. The far-reaching violations of our privacy have confirmed the desirability of protecting it. The recognition of the importance of privacy has taken back its place in the minds of our representatives.

PPE should elevate concerns about privacy and data protection over strategic concerns.

More often than not, different institutions within the EU have elevated concerns about privacy and data protection over particular other concerns. The Commission's adequacy decisions are meant to lift barriers to trade with

third countries. However, these barriers were raised by the EU's DPD in the first place. This entailed a forgoing of potential trade with the aim of ensuring adequate protection, and thus an elevation of the EU's data protection standards over the economic benefits of trading with particular third countries.

The Safe Harbor agreement, on the other hand, can be interpreted in different ways. It inhibits trade by raising requirements for enterprises being granted market access, while enhancing the adequacy of the privacy policies of those enterprises, but it also entails a compromise with the US government on existing EU standards, while being unable to ensure protection of the PII of EU citizens because the US has jurisdiction over these enterprises. The NSA revelations have made it patently obvious that the law did not really matter at all. The NSA had access to our data anyway. As such, Safe Harbor is currently being renegotiated, and the EU is now less willing to compromise. While this situation has seemingly resulted in an impasse in the negotiations, this uncompromising stance re-illustrates the normative intent of the EU.

The ECJ, too, has on at least two occasions elevated concerns about privacy and data protection over other concerns. The DRD was found to infringe on our right to private life and data protection, despite functioning as a supposed means to effectively fight and solve transnational crimes. Its objective was judged legitimate, but was considered not an appropriate means to achieve this objective. The law was not proportionate. In the right to be forgotten case, the ECJ has elevated articles 7 and 8 of the Charter over article 11. Although article 11 cannot be considered a strategic interest, the ECJ's ruling did enhance the scope of application of EU privacy standards and confirms the ECJ's contribution to the EU being a normative power in the area of privacy and data protection.

PPE should be effective in achieving the spread of privacy and data protection norms.

It is absolutely essential for a privacy power to be effective in achieving its relevant aims. Being ineffectual, after all, implies a lack of power. Perhaps this is stating the obvious; but one cannot be a Privacy Power without power. If power is understood as an ability to make others do what one wants, and thus to induce change in particular chosen areas, then it is uncertain whether normative forms of power are truly relevant forms of power. If military power, for example, entails the ability to use military means to cause effects, then normative power should entail the ability to use normative means to cause effects. What those 'means' are is quite important.

It is unclear what 'normative means' really are. If they merely include the power of persuasion on the basis of valid argumentation or behaving in an ethical way, then the EU would be no different from an NGO. NGO's have these same means at their disposal. As a concept, therefore, a normative power should have a defining differential element to it. For the EU, its market is what sets it apart from other international actors. The single market is and remains the EU's most effective source of power. Foreign entities may be dependent on being granted market access to some extent, and this can be used as a means; as leverage (a form of power). This economic power enables the EU to translate its normative intent into actual normative impact.

In the area of privacy and data protection, the impact is strong. governments around the world are influenced by EU standards when adopting their own data privacy laws. 109 nations have already enacted such laws. Furthermore, the Brussels Effect allows the EU to externalize its standards to foreign enterprises and third country governments. The

importance of the single market in combination with the EU having relatively high regulatory data protection standards, creates 'involuntary incentives' for commercial enterprises to adopt EU standards across the board rather than adhering to various lower standards elsewhere. Adopting the highest uniform standard across the board is the only prudent option.

Economic incentives of external actors lead to normative opportunities for the EU. To know what others need and how much they need it, is to know what one can ask for in return. The EU is able to use the importance of its market as a means to make others do things that are in line with the EU's normative ends. Other means play their roles and should be factored in, but it is the single market which makes the important difference. It is market access that others want, and it is market access that the EU can either provide or prohibit. In the context of international relations, this is the main power that the EU possesses. Economic rather than normative power, perhaps, but it is clearly possible to use this economic power to achieve significant normative impact. As such, its proven impact abroad significantly contributes to making the EU a Privacy Power.

Final Words

To revisit the NPE hypothesis, I lay claim to a new but concise definition of a normative power: a civilian power with normative intent and the means to achieve significant normative impact, on condition of the norm being universally valid. A privacy power then constitutes a subset of this definition. Because the EU shows a large degree of normative intent, and through its economic power is able to achieve substantial normative impact, the internal inconsistencies and occasional contradictions in the area of privacy and data protection are not sufficient to delegitimize the hypothesized concept of Privacy Power Europe.

9 References

APEC (2005). APEC Privacy Framework. *APEC Secretariat, ISBN: 981-05-4471-5*

Bach, David; Newman, Abraham L. (2007). The European regulatory state and global public policy: micro-institutions, macro influence. *Journal of European Public Policy*

Bloomberg (2013). Privacy and Security Law Report: Privacy in Latin America. *The Bureau of National Affairs, Inc. (800-372-1033)*

Boehm, Franziska (2014). Opinion on the adequacy of the Safe Harbor Decision: Comparison between Safe Harbor and Directive 95/46. *Case C-362/14*

Bradford, Anu (2011). European Regulatory Imperialism.

Bradford, Anu (2012). The Brussels Effect. *Nw. UL Rev, 107*

Bradford, Anu (2014). Exporting Standards: The externalization of the EU's regulatory power via markets. *International Review of Law and Economics*

Burca, Grainne De (2013). After the EU Charter of Fundamental Rights: The Court of Justice as a Human Rights Adjudicator? *Maastricht Journal of European and Comparative Law, 20. 13-51*

COM (1995). Directive 95/46/EC of the European Parliament and of the Council, of 24 October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal of the European Communities. No L. 281/31*

COM (2010). Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council. *C(2010) 593*

COM (2012a). Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and

on the free movement of such data (General Data Protection Regulation). *2012/0011 (COD)*

COM (2012b). EU Factsheet: Why do we need an EU data protection reform?

COM (2012c). Commission Staff Working Paper: Impact Assessment. *SEC (2012) 72 final*

COM (2014). DG Connect Internal Report on the implementation of the Commission Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification.

Cremona, Marise (2011). Justice and Home Affairs in a Global World: Ambitions and Reality in the tale of the EU-US SWIFT Agreement (No. 4). *Institute for European integration research*.

Damro, Chad (2012). Market power Europe. *Journal of European Public Policy, 19(5). 682-699*

De Goede, Marieke (2012). The SWIFT Affair and the Global Politics of European Security. *JCMS: Journal of Common Market Studies, 50(2). 214-230*

Diez, Thomas (2005). Constructing the Self and Changing Others: Reconsidering Normative Power Europe. *Millenium-Journal of International Studies, 33(3). 613-636*

EDPS (2015). Leading by Example

European Council (1981). Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data

Eustace and Bohn (2013). Navigating the Gauntlet: A Survey of Data Protection Privacy Laws in Three Key Latin American Countries. *The Sedona Conference.*

Forsberg, Tuomas (2011). Normative Power Europe, Once Again: A Conceptual Analysis of an Ideal Type. *Journal of Common Market Studies, 49(6). 1183-1204*

Francois, Joseph et al. (2013). Reducing Trans-Atlantic Barriers to Trade and Investment. *Centre for Economic Policy Research*

Greenleaf, Graham (2008). Macao's EU-influences Personal Data Protection Act. *Privacy Laws & Business International Newsletter 96. 21-22*

Greenleaf, Graham (2012). The influence of European data privacy standards outside Europe: Implications for globalization of Convention 108? *Edinburgh School of Law Research Paper Series*

Greenleaf, Graham (2015). Global data privacy laws 2015: 109 countries, with European laws now a minority. *Privacy Laws & Business International Report*

Greenwald, Glen (2014) No place to hide, *Brilliance Audio.*

Groves, Peter; Kayyali, Basel; Knott, David; Van Kuiken, Steve (2013). The Big Data Revolution in Health Care. *Center for US Health System Reform Business Technology Office. McKinsey&Company*

Harding, Luke (2014) The Snowden Files: The inside story of the world's most wanted man. *Guardian Faber Publishing.*

Hogan Lovells (2014). Data Privacy Regulation Comes of Age in Asia.

Hogan Lovells (2014b). South Africa: data protection legislation. *Hogan Lovells Global Media and Communications Quarterly.*

Human Rights Watch (2014). Why Liberty to Monitor All – How Large-Scale US Surveillance is Harming Journalism, Law, and American Democracy. *ISBN: 978-1-62313-1814*

Manners, Ian (2002). Normative Power Europe: a contradiction in terms? *Journal of Common Market Studies, 40. 235-258*

Manners, Ian (2008). The normative ethics of the European Union. *International Affairs. 45-60*

McAfee, Andrew and Brynjolfsson, Erik (2012). Big data. The management revolution. *Harvard Bus Rev, 90(10). 61-67*

Mayer-Schönberger, Viktor (2009). Delete: the virtue of forgetting in the digital age. *Princeton University Press.*

Mayer-Schönberger, Viktor (2007). Useful Void: the art of forgetting in the age of ubiquitous computing.

Monar, Jörg (2010). The rejection of the EU-US SWIFT interim agreement by the European Parliament: a historic vote and its implications. *European foreign affairs review, 15(2). 143-151*

Negley, Glenn (1966). Philosophical views on the value of privacy. *Law and Contemporary Problems. 319-325*

OECD (1980) Guidelines covering the protection of privacy and transborder flows of personal data.

Pawlak, Patryk (2009). The External Dimension of the Area of Freedom, Security and Justice: Hijacker or Hostage of Cross-pillarization? *European Integration 31(1). 25-44*

Pearce, Graham; Platten, Nicholas (1998). Achieving personal data protection in the European Union. *JCMS: Journal of Common Market Studies 36.4 (1998). 529-547*

Peers, Steve (2005). The European Parliament and data retention: Chronicle of a 'sell-out' foretold? *Statewatch Analysis*

Ponemon Institute (2011). The True Cost of Compliance. *Independently Conducted by Ponemon Institute LLC*

PWC (2013). Capitalizing on the Promise of Big Data

Rachels, James (1975). Why Privacy is Important. *Philosophy & Public Affairs. 323-333*

Ripoll Servent, Ariadna; MacKenzie, Alex (2011). Is the EP still a data protection champion? The case of SWIFT. *Perspectives on European politics and society, 12(4). 390-406*

Romaniello, Maria (2013). The international role of the European Parliament: The SWIFT Affair and the 're-assessed' European institutional balance of power. *Perspectives on Federalism, Vol.5. 97-121*

Shaffer, Gregory (2000). Globalization and Social Protection: The impact of EU and international rules in the ratcheting up of U.S. data privacy standards. *Yale journal of International Law, Vol. 25*

Sjursen, Helene (2006). The EU as a 'normative' power: how can this be? *Journal of European Public Policy, 13(2). 235-251*

Smolan, Rick (2013). The Human Face of Big Data.

Solove, Daniel (2008). Understanding Privacy

Surveille (2014). SURVEILLE Paper Assessing Surveillance in the Context of Preventing a Terrorist Act. *FP7 – SEC – 2011-284725*

United Nations (1948). Universal Declaration of Human Rights

United Nations (1966). The International Covenant on Civil and Political Rights

Vogel, David (1997). Trading up and governing across: transnational governance and environmental protection. *Journal of European public policy, 4(4). 556-571*

Weber, Rolf (2010) Internet of Things–New security and privacy challenges.*Computer Law & Security Review*, *26*(1), 23-30.

Xanthoulis, Napoleon (2013). The Right to Oblivion in the Information Age: A Human-Rights Based Approach. *US-China L. Rev*