Europa Kolleg Hamburg
Institute for European Integration

Study Paper

No 05/16

Drifting Away from the Safe Harbor: Re-Thinking Legal Privacy Protection within EU-US Data Flows

Victoria C. Granda

December 2016

Europa-Kolleg Hamburg
Institute for European Integration

The *Europa-Kolleg Hamburg* is a private law foundation. The foundation has the objective of furthering research and academic teachings in the area of European integration and inter-national cooperation.

The *Institute for European Integration*, an academic institution at the University of Hamburg, constitutes the organizational framework for the academic activities of the *Europa-Kolleg*.

The series Study Papers presents selected master theses of the Master Programme "Master of European and European Legal Studies" at the Europa-Kolleg Hamburg in cooperation with the University Hamburg. The views expressed in these papers are those of the authors only and do not necessarily reflect positions shared by the Institute for European Integration. Please address any comments that you may want to make directly to the author.

Editor:

Europa-Kolleg Hamburg
Institute for European Integration
Prof. Dr. Markus Kotzur, LL.M. (Duke) (managing director),
Dr. Konrad Lammers (research director)
Windmühlenweg 27
22607 Hamburg, Germany
http://www.europa-kolleg-hamburg.de

Please quote as follows:
Europa-Kolleg Hamburg, Institute for European Integration, Study Paper No 05/16,
http://www.europa-kolleg-hamburg.de

Drifting Away from the Safe Harbor:
Re-Thinking Legal Privacy Protection within EU-US Data Flows

Victoria C. Granda*

Abstract

The rise of data is forcing a fundamental reevaluation of legal human rights and freedoms protection. European and American information easily crosses the Atlantic and interconnects, freeing itself of the confines of physical territory. This brings unique challenges to the protection of the right to privacy, as the EU and US conceive this right differently. As the EU has strengthened its protection of personal data, it has sought to ensure its laws are not circumvented when data leaves its territorial jurisdiction. Underneath the 1995 Data Protection Directive, the EU forbid transfers of personal data to third countries unless they provided adequate protection. The 2000 Safe Harbor arrangement enabled data flows to the "inadequate" US until the ECJ struck it down in 2015.

The fall of Safe Harbor and recent enactment of the General Data Protection Regulation create an opportunity to re-think legal protection of privacy within EU-US data flows. With attention to past shortcomings, problematic legal thought, and a dynamic digital future, this thesis proposes a new approach grounded in the reality of data and its traffic, protects the European interest in dignified privacy as it respects the American priority in freedom of expression, and thus allows an open and free Internet to thrive.

Key Words: privacy law, data protection, EU-US data flows, data transfers, Safe Harbor, Schrems decision, Data Protection Directive, General Data Protection Regulation

*This paper was originally submitted in June 2016 as a thesis for the degree "Master of Arts (M.A.)" at the Europa-Kolleg Hamburg (supervisor: Prof. Dr. Armin Hatje). Victoria Granda is currently a Candidate for the degree Juris Doctor at the University of Virginia School of Law, Charlottesville, Virginia, United States.

Contact Information:
Victoria C. Granda
victoria.granda@gmail.com

Acknowledgments

I would like to thank many for their support in writing this thesis. First of all, thank you to Professor Dr. Armin Hatje, who asked critical questions and guided me through my recent arrival in the field of law. Thank you also to the faculty and staff at both the Europa-Kolleg Hamburg and University of Hamburg who prepared me for this thesis, assisted in my research, and helped with even the most trivial requests. This would not have been possible without my alma mater, Case Western Reserve University (Cleveland, Ohio, USA), that financed my graduate studies in Hamburg through the Wright-Plaisance Fellowship for Study Abroad. Thank you to family, friends, and colleagues who answered questions, provided feedback, and as always, gave me the emotional support needed to complete challenging tasks. I would not be here today without you.

I would like to dedicate this thesis to my six beautiful nieces and nephews: Cecilia, Nicolás, Marcelo, Sofía, Paola, and Gabriel Ignacio. May you always value and fight for fundamental human rights and freedoms.

TABLE OF CONTENTS

List of Abbreviations

AEPD – Agencia Española de Protección de Datos

ADR – Alternative Dispute Resolution

CFR – Charter of Fundamental Rights of the European Union

EC – European Community

ECJ – Court of Justice of the European Union

ECHR – European Convention on Human Rights

EB – Exabyte

EU – European Union

GB – Gigabyte

IP – Internet Protocol

FAQs – Frequently Asked Questions

MB – Megabyte

MEP – Member of European Parliament

NIST – National Institute of Standards and Technology

NSA – National Security Agency

OECD – Organization for Economic Cooperation and Development

US – United States of America

ZB – Zettabyte

A. Introduction

On 6 October 2015, the Court of Justice of the European Union (ECJ) declared Commission Decision 2000/520 invalid.[1] Fifteen years prior, this Decision enabled the transfer of European citizens' data to the United States (US), limited to those companies and firms that had subscribed to the Safe Harbor Principles. This arrangement[2] prevented a blockade of European data to the US, which would have halted much trade and information between the two legal jurisdictions. The European Union (EU)[3] had insisted on a high level of data protection of its citizens following Directive 95/46/EC (herein the Directive) requiring that the transfer of data to third countries only be permitted to those countries deemed ensuring an "adequate level of protection."[4] Lacking comprehensive data protection legislation, the US did not qualify as an adequate data recipient in the eyes of the EU. While the Directive severely threatened relations between the EU Member States and the US in an increasingly data-driven and digital world, the Safe Harbor arrangement feebly stopped such a threat, and for several years, allowed each jurisdiction to maintain its own standards while continuing to transfer data and enable cross-border trade.

Since the enactment of the Directive the EU has further solidified its emphasis on protecting the privacy, and thus data, of its citizens, even above other fundamental rights and freedoms. At the same time,

[1] Case C-362/14 *Maximillian Schrems v. Data Protection Commissioner* [2015] EU:C:2015:650. Any references using the term "Case" without further designation indicate cases of the ECJ.

[2] This arrangement is often also referred to the "Safe Harbor Agreement," however, because it was not a formal agreement but rather an arrangement in which the Commission Decision permitted transfers for US companies subscribing to the Safe Harbor Principles, I will use the term "arrangement." In German, the term "Safe Harbor Lösung" or "Safe Harbor solution" is used.

[3] Prior to the Lisbon Treaty entering into force in 2009, the EU was known as the European Community (EC). For the sake of clarity, I will substitute EU for EC in all instances. Unless otherwise noted, the term European is confined to the territory of the EU.

[4] 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 of the free movement of such data, OJ L281.

following the terrorist attacks of 11 September 2001, protection of privacy rights, especially against state intrusion, eroded in the US, concerning both its citizens and allies in Europe. Following the 2013 revelations by *Edward Snowden* on the mass data collection by the US government and its National Security Agency (NSA), European citizens no longer trusted their data held in the US. The European Court of Justice (ECJ) concurred, and in the landmark *Schrems* ruling, deemed the Safe Harbor arrangement no longer sufficient to pass the necessary adequacy test.[5]

Less than seven months after the groundbreaking *Schrems* decision, the EU published its long-awaited replacement of the Directive, in the form of the General Data Protection Regulation (herein the Regulation).[6] The Regulation alters and updates the rules surrounding the transfer of data to third countries, although still requires high protection standards for EU citizens' data outside its territory. The changes are long awaited responses to the problematic rules, yet fall short of providing a long-term solution to the growing issue of transborder data flows, particularly those to the US. Undoubtedly, policymakers in the EU and US will reach another compromise to replace Safe Harbor, as of now expected in the form of the EU-US Privacy Shield, whose details are currently being debated.[7] Regardless of what occurs in the short-term in regards to policy compromise and agreements, at this juncture it is enlightening to observe the problems associated with legally protecting data and privacy in a world increasingly erasing its borders. Ultimately, because the new policy still relies on the arbitrary adequacy criteria,

[5] Case C-362/14.

[6] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L119.

[7] European Commission, "EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield," Press Release Database, 2 February 2016, http://europa.eu/rapid/press-release_IP-16-216_en.htm (accessed 31 May 2016).

the arrangement risks once again collapsing and endangering the flow of data between the EU and US.

Western legal concepts surrounding data need to adapt to the ephemeral nature of the Internet in order to remain effective and maintain freedom, particularly freedom of expression and information and freedom to trade. Neither the EU nor US can force each other to accept different concepts of human rights and freedoms. Yet it is precisely their different strengths of their understandings that can enable new legal protections that make better sense for the future. While their views diverge, the EU and US can reinvigorate their relations and protect privacy through cooperation and a contemporary understanding of data, and meaningful, modern legal principles: principles that allow for flexibility and still maintain steadfast rule of law. The conflict between the EU and US reflects the need for balance between privacy and other freedoms and exposes the problems, along with the strengths, of both legal systems.

This thesis explores the legal issues surrounding data flows between the EU and US, with attention to the recent *Schrems* decision and the new Regulation. It aims to dissect the European evolution on data privacy, particularly on data transfers to third countries, and more specifically, to the US. Rather than divulge into a full comparison of EU and US legal thought on privacy, this study analyzes the EU's relative differences with the US as well as the potential resolutions brought about by recent legislation, contributing to an improved legal framework for transborder data flows. As arrangements and decisions are currently changing and unpredictable, it stays away from offering any short-term policy-related solutions and instead centers on legal concepts emerging from recent problems. The clash between continents provides an opportunity to update priorities in law going forward into the digital age.

B. The Right to Privacy and Data Protection

The right to privacy has a long tradition in the legal systems of Western nations, harkening back to Roman legal codes. As old as the concept of privacy is, however, the understanding of its nature remains elusive and which legal protections it requires remain debatable. The different opinions are starker between national traditions, with a particular divide between continental Europe and the United States.[8] Tracing back its roots to beliefs in honor and the right to develop one's personality, the foundation of privacy protection in Europe rests on the right to human dignity.[9] The consequences of this origin are significant when compared to the results of the American beliefs surrounding privacy, which arise from sacrosanct respect for liberty, especially freedom from state intrusion.[10] The existing differences between the legal jurisdictions are rooted in historical, political, legal, and economic reasons.[11]

Diverging views on privacy, which are even more notable when compared to non-Western thought, could cause one to dismiss privacy's attributes as valuable, useful, or even its status as a fundamental human right. Especially within the context of today's digital world, many no longer believe privacy exists or is possible to protect it, especially legally, if it ever was. These reductionists argue that there is no independent right to privacy; therefore, it does not help to clarify or develop legal protection.[12] Many legal scholars, both American and European, disagree, as would laymen in both continents.

---

[8] For a thorough examination of these differences, see James Q. Whitman, "The Two Western Cultures of Privacy: Dignity versus Liberty" (2004), Faculty Scholarship Series, Paper 649, http://digitalcommons.law.yale.edu/fss_papers/649 (accessed 15 May 2016).

[9] Whitman 1161.

[10] *Ibid.*

[11] Bastian Baumann, *Datenschutzkonflikte zwischen der EU und den USA* (Berlin: Dunker & Humblot, 2016), 234; Francesca Bignami, "European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining," *Boston College Law Review* 48, no. 3 (2007), 681. Unless otherwise noted, all translations are my own.

[12] See footnote 9 in Ruth Gavison, "Privacy and the Limits of Law," *The Yale Law Journal* 89, no.3 (January 1980), 422.

In order to properly articulate what legal protections are appropriate, it is necessary to formulate a general and broad understanding of privacy.

Because of its elusive nature, even legal scholars have difficulty defining privacy. Several scholars use terms of control, such as *Hyman Gross* who defines it as "control over acquaintance with one's personal affairs" or *T. Gerety* who uses the definition "autonomy or control over the intimacies of personal identity."[13] However, as *Ruth Gavison* explains, defining privacy in terms of control is problematic because it depends on choice, thus privacy must be seen as having inherent value, and not whether or not an individual has chosen to exercise control over it.[14] *Gavison* explains that "privacy is a limitation of others' access to an individual," yet because perfect privacy, i.e. complete inaccessibility, is not possible, and privacy is not an "all or nothing concept," what is useful is not focusing on such pure privacy but rather the loss of privacy.[15] In this sense, the complexity of privacy can be understood as containing the interrelated elements of "secrecy, anonymity, and solitude." While *Gavison's* point is notable, it is even more difficult to transfer to concrete legal statutes. Most definitions and understandings of privacy remain centered around the concrete concepts of choice and control.

Within American constitutional law, the right to privacy is said to have three components: 1) the right to be left alone; 2) the right to autonomous choice regarding intimate matters; and 3) the right to autonomous choice regarding other personal matters.[16] The contemporary American understanding of the right to privacy originates in 1890 *Harvard Law Review* article by *Samuel D. Warren* and *Louis D. Brandeis*.[17] In this seminal article, Warren and Brandeis lay down the argument for a new, explicit right to privacy, separate

[13] As quoted in Gavison, 426.
[14] Gavison, 427-428.
[15] Gavison, 428.
[16] See footnote 4 in A. Michael Froomkin, "The Death of Privacy?," *Stanford Law Review* 52, no. 5 "Symposium: Cyberspace and Privacy: A New Legal Paradigm?" (May 2000), 1463.
[17] Baumann, 206.

from the right to property. They define this right as the "right to be left alone" and describe it as a principle which protects products of the intellect or emotions, such as personal writings.[18] In this sense, the American understanding is not too different from the continental European view of privacy as control of one's image, name, and reputation, and as well as of what information is disclosed to the public.[19] Indeed, while there are certain overarching differences in the views on privacy, meaningful similarities should not be dismissed. Americans and Europeans both see the dangers apparent in the loss of human dignity, as well as government intrusion into the private sphere.[20] Some scholars, such as *Francesca Bignami*, even argue against the prevailing view that Americans are more concerned with liberty while Europeans with dignity, and that in fact, Europe protects privacy against state intrusion more so than American law.[21] In both Europe and the US, privacy law has traditionally been directed against the state.[22]

Globally, the first data protection law was adopted in Germany with the Hessian *Datenschutzgesetz* on 30 September 1970. Almost a month later, on 27 October 1970, the US adopted its first data protection law, characteristically limited to one sector, with the Fair Credit Reporting Act.[23] These trends continue to today. While both Europe and the US are certainly concerned with protecting privacy and have been leaders in creating related laws, European regulation tends to be broad and overarching while the US has taken a sectoral approach, regulating in limited private sector areas but mainly relying on litigation and industry self-regulation.[24] These differences will be further discussed subsequently; however, a full examination of

[18] Louis D. Brandeis and Samuel D. Warren, "The Right to Privacy," *Harvard Law Review* 4, no. 5 (December 1890).
[19] Whitman, 1167.
[20] Baumann, 236.
[21] Bignami, 612.
[22] Birte Siemen, *Datenschutz als europäisches Grundrecht* (Berlin, Germany: Dunker & Humblot GmbH, 2006), 51.
[23] Baumann, 237.
[24] US Department of Commerce, "Safe Harbor Privacy Principles" (2000).

contrasting concepts of privacy between Europe and the US is beyond the scope of this thesis. It is more pertinent to begin by examining EU law and the subsection of the right to privacy as it relates to data protection.

Furthermore, as a result of the Directive, the Member State laws have been relatively harmonized, albeit imperfectly, since its entry into force in 1995. Member State data protection law will soon be almost completely harmonized, as the Directive will be replaced by the Regulation when it enters into force on 25 May 2018.

I. International principles

Although the first data protection laws were established in Europe and the United States, the belief in the sanctity of privacy as well as the importance of personal data protection is not isolated to these two Western powers. The Universal Declaration of Human Rights, created by the General Assembly of the United Nations in 1948, enshrined in the right to freedom from arbitrary interference in one's privacy, family, home, and correspondence, as well as from attacks on honor and reputation, in its Article 12.[25] This Declaration is not legally binding but rather takes the form of a resolution.[26] The International Covenant on Civil and Political Rights of 1966 used similar language in its protection of the right to privacy in Article 17.[27] Specific recognition of data protection, however, reached the global level when the Organization for Economic Cooperation and Development (OECD) published the "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" (herein the Guidelines) in

[25] United Nations, "The Universal Declaration of Human Rights" (1948).

[26] B. Simma and A. Verdross, *Universelles Völkerrecht 3*, Berlin (1984), § 1234 as cited in: Rudolf Gridl, *Datenschutz in globalen Telekommunikationssystemen*, (Baden-Baden: Nomos Verlagsgesellschaft, 1999), 168.

[27] United Nations, "International Covenant on Civil and Political Rights" (1966).

1980.[28] The Guidelines were updated on 9 September 2013, although they remain the same in essence.[29]

The OECD, which included the major industrialized nations at the time, created the Guidelines with the intention of establishing voluntary general rules and international principles for the fair treatment of personal data.[30] The Preface to the Guidelines explains that the OECD Member countries wished to both prevent violations of human rights as well as prevent the hampering of the free flow of data across borders, as they recognized that the flow of data was only going to continue increasing with new technology.[31] The Guidelines were not intended to prevent national protective measures but rather meant as minimum standards.[32]

Of importance for the discussion on transborder data flows is Part Three of the Guidelines: "Basic Principles of International Application: Free Flow and Legitimate Restrictions."[33] This part, one of five, begins by emphasizing that Member countries should consider the other countries when it comes to both domestic processing and re-export of personal data.[34] This sets the tone of the liberal politics and intentions of the OECD and the spirit of the Guidelines, as they seek to allow freedom of information and encourage data flows between Member countries.[35] Paragraph 16 recommends that all Member countries take steps to ensure that the flow of data across borders is "uninterrupted and secure."[36] Paragraph 17 continues this point by

[28] OECD, "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" (1980).
[29] "OECD Issues Updated Privacy Guidelines," *Privacy & Information Security Law Blog*, 16 September 2013, https://www.huntonprivacyblog.com/2013/09/16/oecd-issues-updated-privacy-guidelines (accessed 9 May 2016).
[30] Joel R. Reidenberg, "Resolving Conflicting International Data Privacy Rules in Cyberspace," *Stanford Law Review* 52, no.5 "Symposium: Cyberspace and Privacy: A New Legal Paradigm?" (May 2000), 1328.
[31] "OECD Guidelines," Preface.
[32] *Ibid.*, Part 1 (6).
[33] *Ibid.*, Part 3.
[34] *Ibid.*, Part 3 (15).
[35] Michael Bergmann, *Grenzüberschreitender Datenschutz* (Baden-Baden, Germany: Nomos Verlagsgesellschaft, 1985), 148.
[36] *Ibid.*, Part 3 (16).

recommending that Member countries refrain from restricting data flows, except from nations that do not "substantially observe these Guidelines," or in specific categories for which another Member country does not provide "equivalent protection." [37] Part Three concludes by again recommending countries to avoid creating "obstacles to transborder flows of personal data" where such obstacles exceed the requirements of privacy protection.[38] The final section, Part Five, of the Guidelines encourages cooperation amongst its Member countries and encourages them to work toward the development of both domestic and international principles.[39]

If these Guidelines had truly been followed, there would, of course, be no need for this thesis as data would flow between Member countries freely. Despite the best intentions of the voluntary guidelines, data neither move freely between Member countries nor have the said nations developed international standards regarding data protection. Regardless, the international consensus on broad views of data protection demonstrated through the Guidelines is noteworthy. *Joel Reidenberg* explains that not only in these Guidelines but also through various the national legislations, scholars have identified a core group of First Principles regarding data privacy and protection. [40] The Principles are related to four sets of standards which he identifies as

1) data quality
2) transparency or openness of processing
3) treatment of particularly sensitive data
4) enforcement mechanisms

These standards then can be divided into ten elements, as laid out by *Colin Bennett*, showing the convergence of data protection policy amongst national legislation. [41] Although today there are still no binding international agreements, and the chances of any in the near

[37] *Ibid.*, Part 3 (17).
[38] *Ibid.*, Part 3 (18).
[39] *Ibid.*, Part 5.
[40] Reidenberg, 1326.
[41] *Ibid.*

future remain slight, when regional or global data protection are discussed, these convergences must be kept in mind. These international principles can also be observed in the Madrid Resolution of 2009, a non-binding agreement on data protection.[42] While the Resolution gave hope that an international consensus could lead to a binding agreement, no progress has yet been made.

II. Statutory development within the EU pre-Regulation

Although not currently binding within the EU legal order, the European Convention on Human Rights (ECHR) is important because of its influence on EU law and it is binding on all 28 EU Member States. The ECHR, created by the then-newly formed Council of Europe, entered into force in 1953 and. Article 8 of the Convention protects "respect for private and family life" as a fundamental human right. As of the completion of this thesis, the ECHR is not binding within the EU legal order, although it is required for interpretation of the binding Charter of Fundamental Rights of the European Union (CFR).[43]

At the wider European level, of particular significance is the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (herein Convention 108) of the Council of Europe due to its impact on EU transborder data flows legislation.[44] The Convention entered into force in 1985 to be acceded to by all the current members of the EU, in addition to other non-EU members of the Council of Europe.[45] Like the Guidelines, the Article 12 of the Convention seeks to prevent unnecessary blocks of transborder data flows. However, Article 12 provides for specific derogations: first, for specific categories of data, unless the Party to which the data is

[42] International Conference of Data Protection and Privacy Commissioners, "The Madrid Resolution" (2009).
[43] Baumann, 252.
[44] Council of Europe, "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data" No. 108 (1981).
[45] Kuner *OECD Papers* No. 187, 15.

transferred provides "equivalent protection," and second, in the case of non-Party States, in order to avoid circumvention of legislation.[46]

In the 1990s, differences in data protection law were significant between the United Kingdom and Ireland and continental Europe, but also between nations within continental Europe, notably France and Italy, as France already had a high level of data protection while Italy had no such legislation.[47] Harmonization was necessary at the time as many Member States had contrasting laws which would have hampered the cross-border data flows necessary for the Internal Market, and thus the European Community (now EU) created the Directive to enshrine protection of personal data.[48]

Article 8 ECHR is explicitly referred to in recital 10 of the Directive, which clarifies that national data protection laws must protect the recognized right to privacy as laid out in the ECHR as well as the general principles of Community law. At the time of the adoption of the Directive in 1995, the CFR was not yet in existence. The ECHR, therefore, had the importance of being the foundation for this understanding of privacy as a fundamental right, worthy of a high level of protection, along with Convention 108. The Directive established data protection as a specific category of protection within the right to privacy in the EU legal order. The objective of the Directive was twofold: two protect the right to privacy regarding personal data processing, and to ensure the free flow of data within and between the Member States.[49]

The EU further raised the importance of data protection when it created an explicit right to it in the CFR. In 2009 the CFR became binding primary EU law when the Lisbon Treaty entered into force,

[46] Convention No. 108, Article 12.

[47] Baumann, 240; Francesca Bignami, "Cooperative Legalism and the Non-Americanization of European Regulatory Styles: The Case of Data Privacy," *The American Journal of Comparative Law* 59, no.1 (Spring 2011), 422.

[48] Recital 7, Directive 95/46/EC.

[49] See Article 1, Directive 95/46/EC of the European Parliament and 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 [1995] OJ L 281/31.

and thus became the main source of rights interpretation of the EU.[50] The CFR contains its own counterpart to Article 8 ECHR in Article 7 which also protects the right to private life. It is Article 8 CFR that is significant, as it establishes the right to data protection as a fundamental right, independent of the right to privacy.[51] Article 8 reads as follows:

1. "Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority."[52]

The CFR "emancipated" data protection from the general right of personality and privacy.[53] Prior to the Lisbon Treaty, no binding statute in any such conventions, bills, or declarations had explicitly protected data separately from the right to privacy.[54] Its strong language, specifically in the second paragraph, brings significant legal ramifications and obligations, previously not explicitly laid out in primary law. This trend within the EU to increase its protection of privacy, and specifically personal data, is a focal point of this thesis. The trend is reflected not only in statutory law, but the case law of the ECJ as well.

III. Transfer of data to third countries under the Directive

The Directive had many important implications and certainly placed the EU as the world leader in broad coverage of data protection

[50] Charlotte Bagger Tranberg, "Proportionality and data protection in the case law of the European Court of Justice," *International Data Privacy Law* 1, no. 4 (2011), 240.
[51] *Ibid.*
[52] Charter of Fundamental Rights of the European Union, Article 8.
[53] Baumann, 252.
[54] Siemen, 51.

regulation.[55] For this discussion, the relevant material is mostly found in Chapter IV "Transfer of Persona Data to Third Countries." Article 25 prohibits the transfer of processed data to a third country unless that country "ensures an adequate level of protection."[56] Thus, unlike nations which as a rule allow transborder data flows unless there is reason to block them, the position of the EU is to block data flows and to require a legal basis in order to allow the transfer to occur at all.[57] Such a rule was enacted in order to prevent circumvention of the data protection laws within the EU following the Directive.[58] Both Member States and the Commission inform each other when a third country does not ensure an adequate level of protection; if the Commission confirms this assessment, the Member States are to prevent any data transfer to the country in question.[59]

At issue remains that the Directive fails to define exactly what is meant by "adequacy." Article 25 (2) clarifies that the assessment shall take place,

> "in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral… and the professional rules and security measures which are complied with in that country."[60]

Whether Article 25 requires a comparatively equivalent or lower level of adequate protection is unclear, although scholars have generally interpreted it as meaning that less protection than that afforded in the EU is suitable.[61] This understanding, however, has changed with time, particularly in ECJ case law, as discussed later.

[55] Kuner, *OECD Papers*, 16.
[56] Directive 95/46/EC, Article 25.
[57] Kuner *OECD Papers*, 27.
[58] *Ibid.*, 28.
[59] Directive 95/46/EC, Article 25 (3) (4).
[60] *Ibid.*, Article 25 (2).
[61] Siemen, 298-299; Eugen Ehmann and Marcus Helfrich, *EG Datenschutzrichtlinie: Kurzkommentar* (Cologne, Germany: Verlag Dr. Otto Schmidt KG, 1999), 290.

Inferred from Article 25 (2) is that the Commission is to analyze the functionality and effectiveness of data protection in a third country's legal system in practice, that European citizens' data, and thus fundamental rights and freedoms, are in reality secured with an effective carry through, not just that laws are in the books.[62] Therefore, the legal position of those affected citizens must be guaranteed.[63] While there are no specific measures, which qualify a country's level of data protection as "adequate," the core of the fundamental right of data protection must be essentially protected.[64] The core of the right to privacy is interpreted as essentially understood by the Member States, thus the Directive gives interpreters an abstract rather than concrete concept of privacy.[65]

Article 25 must not be viewed in isolation to understand the adequacy test, but rather read in context with the subsequent Article 26.[66] The latter presents the derogations when data transfer may take place despite a third country's failure to ensure an adequate level of protection.[67] These derogations include when the data subject has given unambiguous consent, the transfer is contractually necessary, public interest grounds, and the transfer is necessary for the data subject's vital interest protection.[68]

As of June 2016, only seven countries and four territories have been deemed by the Commission as adequately protecting data under Article 25, presenting serious problems for European data and growth of European markets.[69] Here lies the key point: the adequacy test is

[62] Siemen, 299.
[63] Ulrich Dammann and Spiros Simitis, *EG-Datenschutzrichtlinie: Kommentar* (Baden-Baden, Germany: Nomos Verlagsgesellschaft, 1997), 280.
[64] Dammann/Simitis, 272-273.
[65] Ehmann/Helfrich, 290.
[66] Ehmann/Helfrich, 289.
[67] Directive 95/46/EC, Article 26.
[68] *Ibid.*, Article 26 (1).
[69] The countries are Andorra, Argentina, Canada (commercial organizations), Israel, New Zealand, Switzerland, and Uruguay; the territories are the Faeroe Islands, Guernsey, Isle of Man, Jersey. See European Commission, "Commission decisions on the adequacy of the protection of personal data in third countries," last updated

unclear and arbitrary. It is determined by the executive Commission and brings with it politics rather than clear legal standards. Compliance is questionable, as the Commission itself has acknowledged. For example, the Commission has not yet decided on the adequacy level of major economic players, such as China and Japan, yet undoubtedly data transfers are occurring between the EU and these nations.[70] That politics was behind the original Safe Harbor arrangement, as well as its demise, is not difficult to see. The questionable adequacy test is therefore potentially hampering transborder data flows and at the same time not acting as a proper mechanism to protect personal data.

Under the Directive, data flows to countries without adequacy decisions have legally been permitted primarily through two conditions: standard contracting clauses and binding corporate rules.[71] Article 26 (2) allows for transfers to third countries under "appropriate contractual clauses." The Commission created two sets of standard contracts so that each company would not have to write a contract from scratch.[72] The contracts are meant to compensate for the lack of adequate standards in a third country. In addition, binding corporate rules can also function as substitutes, although they only are permitted for a single or group of affiliated companies. [73] These two forms, permitted through the derogations, have been increasingly playing a larger role in transborder data flows.

IV. Relevant ECJ case law under the Directive

The development of the right to privacy and, specifically, to data protection within the EU legal order is not confined to statutory codes

23 March 2016, http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm (accessed 30 May 2016).

[70] Kuner *OECD Papers*, 21.

[71] Paul M. Schwartz, "The EU-US Privacy Collision: A Turn to Institutions and Procedures," *Harvard Law Review* 126, no. 7 (2013), 1980.

[72] *Ibid.*, 1982.

[73] *Ibid.*, 1983.

but also includes the case law of the ECJ. Since the EU established its high standard of data protection through the Directive, the ECJ has upheld such a standard, and even further raised the status of this right. The Court has prioritized privacy over other rights and freedoms to the point that critics claim it has created a type of "super-human right."[74]

In cases relating to the Directive, the Court has used the principle of proportionality and established a strict necessity test in order to justify violations of privacy.[75] The principle of proportionality was established in 2003 with the *Österreichischer Rundfunk* case in which the Court found that Austrian measures to disclose information regarding public funds–a legitimate state interest–did not pass the proportionality test set down in the Directive, as they infringed on the privacy of the persons in question by potentially causing them harm arising from such publicity.[76] Important cases raising the standard of privacy protection include the 2008 *Huber* case,[77] 2008 *Satamedia* case,[78] and 2010 *Schecke* case.[79] In the *Satamedia* case, the ECJ clarifies that when balancing two fundamental rights, such as privacy and freedom of expression, the right to privacy requires that any derogations and exceptions be applied only as strictly necessary.[80] The "strictly necessary" test was reiterated by the Court more recently in the 2013 *IPI* case[81] and 2014 *Digital Rights Ireland* case.[82]

---

[74] Hans Peter Lehofer, "EuGH: Google muss doch vergessen – das Supergrundrecht auf Datenschutz und die Bowdlerisierung des Internets," E-Comm, entry posted 13 May 2014, http://blog.lehofer.at/2014/05/eugh-google-muss-doch-vergessen-das.html (accessed 18 May 2016).

[75] Tranberg, 239.

[76] Joined Cases C-465/00, C-138/01, and C-139/01 *Österreichischer Rundfunk* [2003] ECR I-6041, EU:C:2003:294.

[77] Case C-524/06 *Huber* [2008] ECR I-9705, EU:C:2008:724.

[78] Case C-73/07 *Satakunnan Markkinapörssi and Satamedia* [2008] ECR I-9831, EU:C:2008:727.

[79] Joined Cases C-92 and C-93/09 *Volker and Marcus Scheke Eifert* [2010], ECR, EU:C:2010:662.

[80] C-73/07; for further explanation see Tranberg, p. 245.

[81] Case C-473/12 *IPI* [2013], ECR, EU:C:2013:715.

[82] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Kärntner Landesregierung* [2014], ECR, EU:C:2014:238.

Two additional cases are of particular relevance for transborder data flows. The question of transfer of data to third countries was first brought to the ECJ in the 2003 *Lindqvist* case.[83] In this case, *Mrs. Lindqvist*, a Swedish woman, uploaded the names, telephone numbers, and other personal data of fellow parishioners on a self-made Internet page without informing the concerned persons. The Swedish public prosecutor brought a suit against *Mrs. Lindqvist* on various counts, including the transfer of personal data to third countries without authorization. While *Mrs. Lindqvist* had not intentionally transferred the data outside of Sweden, for example by using a foreign server, the Swedish government claimed that because this information was made accessible to persons in third countries, this constituted a transfer and thus a breach of the Directive.[84] The ECJ disagreed. The data was not a direct transfer of information between two people but rather through the infrastructure of the Internet and of the hosting provider.[85] Article 25 of the Directive does not concern the activities carried out by hosting providers but rather by users, such as the activities performed by *Mrs. Lindqvist.*[86] The Directive does not concern the use of the Internet, issues concerning the hosting providers, or whether the operations are considered to have occurred in their place of establishment or business address, or the actual location of the computers.[87] Finally, the ECJ recognized that, at the time of the Directive's creation, the Internet's development was still in early stages. Thus, it cannot be presumed that the legislators intended to include any loading of data on an Internet page under the meaning of "transfer."[88] Were this the case, anything posted on an Internet page, and thus made accessible throughout the world, could be deemed a transfer. Article 25 would not then constitute a special regime but

[83] Case C-101/01 *Bodil Lindqvist* [2003] ECR I-12971, EU:C:2003:596.
[84] *Ibid.*, para. 15 (5).
[85] *Ibid.*, para. 61
[86] *Ibid.*, para. 62.
[87] *Ibid.*, para. 67.
[88] *Ibid.*, para. 68.

rather a general regime.[89] If any country with Internet access did not ensure adequate protection, then the Member States would be obliged to prevent any personal data loaded onto the Internet, *reductio ab absurdum*. Through the *Lindqvist* case, the ECJ prevented a potentially serious blockade of European data from the Internet in its entirety.

Not addressing Article 25 of the Directive specifically, the 2014 *Google Spain* case is nonetheless very relevant for transborder data flows.[90] The case involved *Mario Costeja González*, a Spanish national, who wished to remove or alter data relating to him published by the Spanish newspaper *La Vanguardia* concerning events that occurred several years prior; he also wished to remove or conceal this information within Google's search engine so that his information would no longer appear in the links identified through search results.[91] While the Agencia Española de Protección de Datos (AEPD), the Spanish data protection agency, rejected the complaint concerning *La Vanguardia*, it upheld the request concerning Google Spain or Google Inc., taking the view that it had such powers when it considers access to data liable to affect the fundamental right of data protection and dignity, including when this concerned a person's mere wish for this data to not be accessible to the public.[92]

Two points are significant for this discussion, the first being the territorial scope decided by the ECJ. Google Search is operated by Google Inc, located in the US, and is the parent company of Google Spain, which has its own legal personality. The subsidiary acts as a commercial agent for Google Inc to promote sale of advertising space on google.es, a version of Google Search offered in Spanish. While Google Inc is not established in the EU, through the promotion and sale of advertising, Google Spain is regarded as closely linked to the

[89] *Ibid.*, para. 69.
[90] Case C-131/12 *Google Spain SL v. Agencia Española de Protección de Datos* [2014], ECR, EU:C:2014:317.
[91] *Ibid.*, para. 14-15.
[92] *Ibid.*, para. 17.

search engine.[93] Thus, although an undertaking outside the EU operates Google Search, it is carried out "in the context of activities," as defined by the Directive, and it has an establishment– Google Spain–in a Member State.[94] The activities of Google Spain are "inextricably linked" to enabling Google Search to function, as it makes the enterprise economically profitable.[95] Thus the commercial activity of the data controller's establishment is within Member State territory and cannot escape the obligations of the Directive to protect the fundamental right to privacy.[96] With this case, then, the ECJ established that the Directive and the EU understanding of the right to privacy is to apply to data held in the non-EU countries.[97] Search engine operators are therefore subject to the Directive and responsible for deleting personal data upon request.[98]

The *Google Spain* case is significant, not just for such a territorial scope extension, but also for its enshrining of "the right to be forgotten." According to the Court, operators of search engines, which it considers data processors under the Directive's definition[99], are able to significantly affect the right to privacy and data protection.[100] A search engine greatly facilitates access to various aspects of a person's private life by bringing together personal data all through a simple search of the person's individual name. This potential interference of the fundamental right to privacy cannot be justified by the search

[93] *Ibid.*, para. 46.
[94] *Ibid.*, para. 55.
[95] *Ibid.*, para. 56.
[96] *Ibid.*, para. 57-59.
[97] "Recent Cases: Internet Law – Protection of Personal Data – Court of Justice of the European Union Creates Presumption that Google Must Remove Links to Personal Data upon Request – Case C-131/12, *Google Spain SL v. Agencia Española de Protección de Datos* (May 13, 2014)," *Harvard Law Review* 128, no. 2, 737.
[98] For more detailed analysis of the implications of the *Google Spain* case, see Johannes Masing, "Vorläufige Einschätzung der „Google-Entscheidung" des EuGH," Verfassungsblog, entry posted 14 August 2014, http://verfassungsblog.de/ribverfg-masing-vorlaeufige-einschaetzung-der-google-entscheidung-des-eugh (accessed 16 May 2016).
[99] Case C-131/12, para. 73.
[100] *Ibid.*, para 80.

engine's economic interest, although it must be balanced against the legitimate interest of the public to access information.[101] The Court decided that the rights to privacy and data protection, as enumerated under the CFR, as a rule override this general public interest in freedom of information, with exceptions such as the potential role of the data subject in public life.[102] Thus the values of the Directive, through which the EU sought to create an extremely high level of privacy and data protection, were reaffirmed by the Court and given a great amount of weight, even against rights such as freedom of information.[103] The remaining landmark case is *Schrems*, discussed next chapter.

The trend in EU substantive and case law is clear: government forces and legal institutions must protect the privacy, and thus personal data, of its citizens. This is not merely a protection against state intrusion but also against private actors. Even when data leaves the European continent, it is to be highly protected. A violation of this right requires a strict necessity test; as such, Europe promotes a high standard of data protection.

C. The Safe Harbor Arrangement

As established in the preceding chapter, the EU has solidified its commitment to the protection of right to privacy. Interference with this right is prevented, and when violated, the EU requires strict necessity for justification. Under the Directive, the EU created a regime protecting personal data at an unsurpassed level. Because of the EU's strict standards regarding data protection and especially the transfer of data to third countries, EU-US data flows have been threatened since the passing of the Directive. The process leading to the Safe Harbor arrangement, along with its ultimate failure, will now be analyzed.

---

[101] *Ibid.*, para. 81.
[102] *Ibid.*, para. 97.
[103] "Recent Cases," 740.

I. Data Protection in the US

As has been stated, the EU's major trading partner and ally, the US, has a significantly different approach to the right to privacy.[104] Unlike the EU, which views data protection as a fundamental right which trumps most other rights, the US balances privacy rights against others, and it is often seen by courts as secondary to freedom of speech. While the EU stands on the position that data processing and transfers are not permitted unless there are legal basis and sufficient protection, the US as a rule allows data processing unless harm is caused.[105] The American conception of privacy rights lies mainly with protection against government intrusion. The Fourth Amendment of the Bill of Rights of the US Constitution, through which unwarranted searches and seizures are unlawful, is the constitutional basis for such protection. The Privacy Act of 1974 is exemplary in this realm, as it protects personal data as collected, maintained, used, and disseminated by federal agencies.[106] Despite this initial concept, the US legal framework is not as strict over government actors processing personal data as the EU's.[107] There is no such protection against private actors, save for specific categories of personal data, such as that in health and finance.[108] An example of the latter is the aforementioned Fair Credit Reporting Act of 1970, the first legislation protecting privacy against private actors.[109]

The US, unlike most other nations, has resisted imitating the EU's "omnibus" privacy laws, i.e. privacy protection with a broad scope.[110] Instead, it legislates as a response to specific problems on a sector-by-

[104] Whitman, 1163.
[105] Paul M. Schwartz and Daniel J. Solove, "Reconciling Personal Information in the United States and European Union," *California Law Review* 102, no. 4 (April 2014), 880.
[106] 5. U.S.C. §552a (2000 & Supp. IV 2004).
[107] Bignami, 620.
[108] *Ibid.*
[109] Kobrin, 117.
[110] Schwartz, "EU-US Collision,"1974.

sector basis.[111] Examples include the Health Information Portability and Accountability Act of 1996 (HIPAA) [112] and the Family Educational Rights and Privacy Act of 1974 (FERPA). [113] This reactive, rather than proactive, process has led to an incoherent patchwork of privacy legislation that is often not up-to-date and filled with gaps.[114]

The US also has no data protection agency similar to those in each of the EU Member States. The US Federal Trade Commission (FTC) does have powers of oversight outside certain regulated industries, powers which have increased in recent decades, but does not have jurisdiction over companies like the European agencies; the FTC also lacks broad enforcement powers.[115] While the FTC is able to use its powers under the FTC Act Section 5 to protect consumers against unfair practices, this does not grant the FTC fining authority, but rather limited enforcement actions, usually consent decrees prohibiting a company from further misconduct.[116] Notably for the discussion on transborder data flows, it also has no laws restricting the outflow of data to other countries.[117] While the EU remains suspicious of automated data processing, the US has not stopped companies from experimenting with new forms of processing and technology. [118] Because of the sector-by-sector approach, therefore, generally more restrictions are placed on established industries while free reign is given to new enterprises, allowing for more innovation, but also more

[111] *Ibid.*

[112] Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in 26, 29, and 42 U.S.C.)

[113] 20 U.S.C. § 1232g (2006 & Supp. V 2011).

[114] Stephen J. Kobrin and Steve Kobrin, "Safe Harbors are Hard to Find: The Transatlantic Data Privacy Dispute, Territorial Jurisdiction and Global Governance," *Review of International Studies* 30, no.1 (January 2004), 117; Susan Ariel Aaronson and Rob Maxim, "Data Protection and Digital Trade in the Wake of the NSA Revelations," in "Forum: EU Data Protection Reform: Opportunities and Concerns," *Intereconomics* 48, no. 5 (2013), 284.

[115] Schwartz, "EU-US Collision,"1977.

[116] Aaron P. Simpson and Lisa J. Sotto, "United States" in *Data Protection & Privacy 2014* (London: Law Business Research Ltd, 2013), 191.

[117] *Ibid.*

[118] *Ibid.*, 1978.

privacy violations.[119] Beyond the limited sectoral approach, the US also emphasizes industry self-regulation. [120] Because of this decentralized, self-regulated, dynamic approach, US data protection corresponds more closely to the character of the Internet.[121]

The state of American data protection is inadequate for the transfer of data according to the EU. This was the case at the time of the Directive's enactment, remains so today and does not appear likely to change soon. Interestingly, the EU has never officially assessed the US, nor has it requested such a process, yet there is a consensus in the EU that the US's privacy protection approach is not sufficient by European standards. [122] While the harmonization of privacy laws would allow the transfer of data to flow easier and better, as would privacy potentially be better protected, with different goals and approaches such an attempt remains fruitless both now and in the foreseeable future. [123] When the Commission approved the Safe Harbor Principles for the transfer of EU data, they were seen as a promising although still problematic approaches to bridging this divide. Standard contracting clauses and binding corporate rules have also been used to solve the US's inadequacy problem.[124] The new Regulation has given new prominence to the latter of these solutions.

II. Circumstances and Content

Initially after the adoption of the Directive, the US strongly distrusted the legislation and adequacy test, considering such

[119] *Ibid.*

[120] "U.S.-EU 'Safe Harbor' Data Privacy Arrangement," *The American Journal of International Law* 95, no. 1 (January 2001), 157.

[121] Jasmin Merati-Kashani, *Der Datenschutz in E-Commerce: die rechtliche Bewertung der Erstellung von Nutzerprofilen durch Cookies,* (Munich, Germany: Verlag C.H. Beck oHG, 2005), 56.

[122] *Ibid.*, 1980.

[123] Schwartz and Solove, 881.

[124] *Ibid.*, 1979.

requirements as a protectionist scheme by the EU.[125] Eventually, however, EU officials were able to convince US officials and companies that the Directive was indeed targeting data protection and not at attempt to create an obstacle to trade.[126] It became clear that an arrangement would have to be reached to prevent a disruption of data flows between the EU and US, and so in 1998 the US Department of Commerce initiated negotiations.[127] The US refused to increase government oversight of the private sector, while the EU saw self-regulation as an inadequate type of "fox guarding the hen-house."[128] Instead of forcing their ideas on each other, the EU and US agreed to the Safe Harbor program, a way of respecting their "deeply rooted differences."[129]

During negotiations, officials had difficulty reconciling each other's views but were eager to continue data flows. The idea that Article 25 of the Directive's adequacy test did not have to be applied to the entire territory of the US but could be confined to specific firms was brought about by US Ambassador *David Aaron* in his informal discussions with *John Mogg*, the EU Commission Internal Market Director-General.[130] Because both sides still believed they were defending fundamental rights and sincere values, the negotiators ultimately did not try to force different normative views into the agreement.[131] In 2000, the negotiations finally came to a point of mutual satisfaction, in which the US was able to put forward substantial industry self-regulation but with enforcement mechanisms that satisfied the EU's concerns.[132] The arrangement known as Safe

[125] Sebastiaan Princen, "Trading up in the Transatlantic Relationship," *Journal of Public Policy* 24, no.1 (2004), 133.
[126] *Ibid.*
[127] "'Safe Harbor' Data Privacy Arrangement," 157.
[128] *Ibid.*
[129] Kobrin, 116
[130] Henry Farrell, "Constructing the International Foundations of E-Commerce: The EU-U.S. Safe Harbor Arrangement," *International Organization* 57, no. 2 (2003), 292.
[131] *Ibid.*, 293.
[132] *Ibid.*, 294.

Harbor was thus seen as a model for dispute resolution between contrasting regulatory systems in the new world of e-commerce and digital data.[133] This arrangement was not a formal international agreement but rather consisted of unilateral actions by the EU and US.[134] *Henry Farrell* has argued it is best described as an "interface," which mediates two incompatible systems of regulation.[135]

On 21 July 2000, the US Department of Commerce issued the "Safe Harbor Privacy Principles" in order to create a framework that enabled certainty for companies wishing to engage in trade between the EU and US.[136] Five days later, on 26 July 2000, the Commission issued Decision 2000/520/EC stating that the required adequate level of protection for the transfer of data from the EU to the US would be attained through organizations complying with said Principles.[137] The Principles were designed only for use by US organizations importing data from the EU that wished to qualify for the "safe harbor," i.e. those organizations considered adequate for the transfer of data. Organizations could agree to adhere to the Principles and Frequently Asked Questions (FAQs), as well as agree that failure to comply would be actionable under Section 5 of the FTC Act. Notably, however, adherence to the Principles could be limited by necessary national security, public interest, or law enforcement requirements, or by statutes, regulations, or case law creating conflicting obligations or explicit authorizations.

The Safe Harbor arrangement included seven enumerated Principles: notice, choice, onward transfer, security, data integrity, access, and enforcement. Each of these Principles was briefly defined, and then further clarification and guidance were found in the fifteen

[133] *Ibid.*, 297.
[134] Kobrin, 121.
[135] Farrell, 299.
[136] No longer publicly available, text can be found in 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce.
[137] Decision 2000/520/EC.

FAQs. An enforcement overview, explaining the authority of the FTC, as well as clarification over damages were annexed to the Principles. The US Department of Commerce created that same year a website listing companies participating in the Safe Harbor arrangement to facilitate EU verification before sending data to a company.[138] Organizations would self-certify by agreeing to the Principles and were issued an annual certification mark by the Department of Commerce and visually placed on their website.[139] The arrangement involved a mixed form of enforcement through both state and private actors.[140] Organizations could agree to the jurisdiction of an Alternative Dispute Resolution (ADR) mechanism or a European data protection authority.[141] For those using ADR, however, the EU insisted on back-up mechanisms, and thus the FTC could take action against those violating the principles.[142] A third layer of enforcement was included, as EU authorities retained power to stop data flows if they were informed of a violation.[143] The Safe Harbor arrangement provided a means for the EU to strengthen regulatory standards of data protection in the US because, in many ways, these enforcement mechanisms increased the power of the FTC.[144]

III. Criticisms

Despite the merits of the Safe Harbor arrangement, it encountered much criticism throughout its fifteen-year period of validity. Europeans remained skeptical of its efficiency and control mechanisms, especially because of the lack of guaranteed external

[138] "'Safe Harbor' Data Privacy Arrangement," 159; this list is also no longer available.
[139] "Instructions for Self-Certified Organizations on the Use of the U.S.-EU Safe Harbor Framework Certification Mark," Export.gov, http://www.export.gov/safeharbor/eu/eg_main_018362.asp (accessed 9 May 2016).
[140] Farrell, 287.
[141] *Ibid.*
[142] *Ibid.*
[143] *Ibid.*
[144] Princen, 135.

control over the self-regulation.[145] That the EU in a way imposed its standards on the US also raised questions of territorial jurisdiction and democratic governance.[146] Indeed, neither Europeans nor Americans were fully satisfied with Safe Harbor as both were subject to a hybrid arrangement that was not in line with either of their values.[147] American businesses were hesitant to join the scheme, which they saw it as going too far and potentially bringing liabilities in Europe, while both American and European privacy proponents saw Safe Harbor as a weak arrangement.[148] Much criticism was directed at enforcement of the arrangement, which was seen as legally "dubious."[149] German *Alexander Genz* put forward harsh legal criticisms in 2004, yet any motion for change remained confined to academic writing.[150] *Genz* saw the arrangement as weakening and even damaging the meaning of European data protection principles, and a missed opportunity to pressure the US to raise its standards.[151]

In 2002, in the European Commission Staff Working Paper studying the implementation of the program, the Commission acknowledged that enrollment in the program was low. Moreover, many of the few companies enrolled did not actually satisfy the Principles.[152] For example, many self-certified companies were not publicly listing their privacy policies on their website as required. By 2004, while enrollment had grown to around 400, the Commission

[145] Alexandra Engel, "Reichweite und Umsetzung des Datenschutzes gemäß der Richtlinie 95/46/EC für aus der Europäisches Union in Drittländer exportierte Daten am Beispiel der USA" (PhD diss., Freie Universität Berlin, 2003), 163-175; Clemens David Cowans, *Ein „modernes" europäisches Datenschutzrecht* (Frankfurt, Germany: Peter Lang GmbH, 2012), 94.

[146] Cowans, 112.

[147] *Ibid*., 113.

[148] Kobrin, 121-122.

[149] Joel R. Reidenberg, "E-Commerce and Trans-Atlantic Privacy," *Houston Law Review* 38, no. 3 (2001), 740.

[150] Alexander Genz, *Datenschutz in Europa und den USA: Eine rechtsvergleichende Untersuchung unter besonderer Berücksichtigung der Safe-Harbor-Lösung* (Wiesbaden, Germany: Deutscher Universitätsverlag, 2004), 176-184.

[151] *Ibid.*, 174-177, 184.

[152] European Commission, "The Application of Commission Decision 520/2000/EC of 26 July 2000 Pursuant to Directive 95/46 of the European Parliament and the Council," Brussels: European Commission (2002).

remained concerned about compliance with the Principles both on the part of the self-certifying organizations as well as the ADR mechanisms.[153] Other criticisms arose with the growth of new technology, such as cloud computing. The nature of cloud computing made data protection difficult: under the Safe Harbor arrangement data protection in cloud computing was seen as neither possible nor practical.[154] Doubts and criticism kept piling during Safe Harbor's period of validity, but lacked an impetus for change.

IV. The *Schrems* decision

Despite all the apparent problems with the Safe Harbor arrangement, it did not appear that any substantial changes would occur because of economic and political interests on the part of both the EU and US.[155] This was the situation until June 2013, when former US National Security Agency (NSA) contractor *Edward Snowden* upended the debate on data protection and privacy by leaking a series of documents on the mass surveillance activities of the NSA.[156] In addition to learning of the NSA's mass data collection on both Americans and foreigners, the public soon knew that the NSA was spying on the governments and leaders of its allies, including those in

[153] European Commission, "The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce," Brussels: European Commission (2004); based on Jan Dhont, María Verónica Pérez Asinari, and Yves Poullet, "Safe Harbour Decision Implementation Study" (19 April 2004), http://ec.europa.eu/justice/data-protection/document/studies/files/safe-harbour-2004_en.pdf (accessed 22 May 2016).

[154] Kirstin Brennscheidt, *Cloud Computing und Datenschutz* (Baden-Baden, Germany: Nomos Verlagsgesellschaft, 2013), 211.

[155] Petri, 802.

[156] *Ibid.* For more on *Snowden* see: Glenn Greenwald, Ewen MacAskill, and Laura Poitras, "Edward Snowden: the whistleblower behind the NSA surveillance revelations," *The Guardian,* 11 June 2013, http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance (accessed 22 May 2016); for timeline of events and links to important documents up to May 2014 see Matthew Cole and Mike Brunker, "Edward Snowden: A Timeline," *NBC News,* 24 May 2014, http://www.nbcnews.com/feature/edward-snowden-interview/edward-snowden-timeline-n114871 (accessed 22 May 2016).

Europe.[157] The revelations sparked outrage among Europeans, who no longer trusted data in the hands of their trading partner across the Atlantic.[158] The leaks caused a "political earthquake" that put pressure on the governments both in the EU and US and raised calls to universally recognize data protection as a human right.[159]

Following the revelations, the Commission issued a Communication on "Rebuilding Trust in EU-US Data Flows."[160] While the Communication showed that the number of enrolled companies in the Safe Harbor scheme had risen to 3246, the problems identified a decade prior continued and were now backed with years of evidence. In this Communication, the Commission included 13 Recommendations addressing transparency, redress, enforcement, and access by US authorities. It was issued alongside another Communication on the "Functioning of the Safe Harbor from the Perspective of EU Citizens and Companies Established in the EU," in which the Commission acknowledged a "growing concern" amongst Europeans with the scheme.[161] Most of the problems already identified in 2004 were still unresolved: companies were often not following the Principles in practice, there was a serious lack of transparency regarding privacy policies, and the US authorities were not issuing sanctions. Under the scheme, the FTC only issued actions against six corporations for falsely self-certifying.[162] The following year, German *Professor Dr. Franziska Böhm* dissected several problematic aspects of Safe Harbor, noting, amongst other issues, a serious lack of

[157] James Ball, "NSA monitored calls of 35 world leaders after US official handed over contacts," *The Guardian,* 25 October 2013), http://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls (accessed 22 May 2016).

[158] Aaronson and Maxim, 281.

[159] Markus Kotzur, "Datenschutz als Menschenrecht?" *Zeitschift für Rechtspolitik* 46, no. 7 (2013), 216.

[160] European Commission, Communication from 27.11.2013, "Rebuilding trust in EU-US Data Flows," COM(2013) 846 final.

[161] European Commission, Communication from 27.11.2013, "Functioning of the Safe Harbor from the Perspective of EU Citizens and Companies Established in the EU," COM(2013) 847 final.

[162] Thomas Petri, "Die Safe-Harbor-Entscheidung: Erste Anmerkungen," *Datenschutz und Datensicherheit* 39, no.12 (November 2015), 802.

enforcement on both the part of the FTC and ARD mechanisms.[163] This legal opinion cast doubts over whether the Safe Harbor was indeed adequate according to European standards. It was requested by *Maximilian Schrems* and used as evidence for the final blow dealt to Safe Harbor, Case 362/14.

1. Facts of the case

In 2013, *Maximilian Schrems,* an Austrian national, requested that the Irish Data Protection Commissioner investigate the situation regarding the transfer of personal data from Facebook Ireland to its parent company, Facebook, Inc, in the US.[164] Any resident of the EU who wishes to be a member of Facebook must make a contract with Facebook Ireland, and either some or all of the member's data is transferred to Facebook Inc's servers in the US.[165] *Schrems* held that in light of *Snowden's* revelations, European personal data held by Facebook, Inc, which was self-certified under the Safe Harbor regime, was not meaningfully protected by US law or in practice.[166] The PRISM program, through which the NSA could collect personal data on a mass scale from Internet providers such as Facebook,[167] demonstrated this, as did the revelations that US officials and law enforcement agencies could access PRISM data without the need for a court order or court order showing probable cause.[168] The Commissioner argued that because Facebook was self-certified through the Safe Harbor framework, the complaint merited no further investigation.[169] *Mr. Schrems* appealed to the Irish High Court, which requested a preliminary ruling from the ECJ on the interpretation of

[163] Franziska Böhm, "Legal opinion on the adequacy of the safe harbor decision, Case 362/14 Maximillian Schrems v. Data Protection Commissioner," in Case 362/14, Annex A.1.
[164] *Schrems v. Data Protection Commissioner* [2014] IEHC 310, para. 2, 18.
[165] Case 362/14, para. 27.
[166] IEHC 310, para. 29.
[167] *Ibid.*, para. 11.
[168] *Ibid.*, para. 29.
[169] *Ibid*., para. 32.

Articles 25(6) and 28 of the Directive and to the validity of Decision 2000/520/EC.[170]

2. Judgment of the Court

According to the Court, read together, the questions referred in essence asked:

> "whether and to what extent Article 25(6) of Directive 95/46, read in the light of Articles 7, 8 and 47 of the Charter, must be interpreted as meaning that a decision…such as Decision 2000/520… prevents a supervisory authority of a Member State…from being able to examine the claim of a person concerning the protection of his rights and freedoms in regard to the processing of [his/her] personal data… which has been transferred from a Member State to [a] third country when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection."[171]

The Court then divided its response into two parts: first, it addressed the powers of the national supervisory authorities, and second, it went beyond the referred question and addressed the validity of Decision 2000/520.

When evaluating the powers of the national supervisory authorities, the Court first reaffirmed that that Directive sought to ensure a high level of protection of the fundamental rights to respect for private life and personal data, and must be interpreted in light of these rights guaranteed by the Charter.[172] It considered the establishment of independent supervisory authorities as essential to the protection of personal data.[173] These authorities must balance the right to privacy against the interest in the free movement of data, and have a wide range of powers for this reason.[174] While the Court acknowledged, as laid out in recital 56 of the Directive, that transfers of data to third

[170] Case 362/14, para. 1.
[171] *Ibid.*, para. 37.
[172] *Ibid.*, para. 38-39.
[173] *Ibid.*, para. 41.
[174] *Ibid.*, para. 42-43.

countries are necessary for international trade, such transfers may only occur if an adequate level of protection is guaranteed in said country, and the supervisory authorities are vested to check for compliance of these requirements.[175] While there is in principle a presumption of legality regarding measures of EU institutions,[176] this cannot prevent a supervisory authority from examining a claim concerning the right to data protection,[177] and in fact, must do so with all due diligence.[178] If such a claim is indeed well-founded, then the authority must bring legal action, provided by national legal remedies. If a national court then shares doubts regarding the validity of a Commission decision, it is to request a preliminary ruling,[179] as only the ECJ may invalidate an EU act.[180]

The crux of the judgment is the second section, in which the court reviews the validity of Decision 2000/520. The Court first acknowledged the Directive contained no definition of "adequate level of protection," as required for the transfer of data to a third country.[181] While in this regard "adequate" does not mean "identical," the Court argued it *must be understood as "essentially equivalent"* in protecting the fundamental rights and freedoms guaranteed in the EU by the Charter, or else such a high level of protection could be circumvented by transferring data to third countries.[182] The Court explained that after the Commission has assessed a third country and adopted a decision, it must regularly check whether such a finding is still factually and legally justified, and take into account circumstances after the decision.[183]

[175] *Ibid.*, para. 47-48.
[176] *Ibid.*, para. 52.
[177] *Ibid.*, para. 56.
[178] *Ibid.*, para. 57, 63.
[179] *Ibid.*, para. 65.
[180] *Ibid.*, para. 61.
[181] *Ibid.*, para. 70.
[182] *Ibid.*, para. 73, emphasis my own.
[183] *Ibid.*, para. 75-77.

The Court then specifically assessed the situation regarding Safe Harbor. It noted that the Principles were "intended for use solely by US organizations" and thus compliance by US public authorities was not required.[184] The agreement allowed for non-compliance with the Principles "to the extent necessary to meet [overriding legitimate interests regarding] national security, public interest, or law enforcement requirements" which would "create conflicting obligations" and thus an organization would have to comply both with the Principles and US law.[185] Decision 2000/520 therefore allowed for interference with fundamental rights of data protection, for which case law does not distinguish whether the personal data was sensitive or the interference caused adverse consequences.[186] The Decision contained no finding of US laws or rules intending to limit such an interference with the data of EU citizens, for which the State would be authorized in the pursuit of national security interests, or of any "effective legal protection against interference of that kind."[187] The Commission's own analysis in the two Communications[188] showed that US state authorities were able to access and process EU citizens' transferred data "beyond what was strictly necessary and proportionate to the protection of national security" and such "data subjects had no administrative or judicial means of redress."[189]

The Court reiterated the need for minimum safeguards protecting the fundamental rights and freedoms, which are even more necessary when data is automatically processed and there is a "significant risk of unlawful access to that data."[190] It also again affirmed its "strictly necessary" test regarding derogations and limitations to the rights to privacy and data protection.[191] It emphasized the major violation to

[184] *Ibid.*, para. 82.
[185] *Ibid.*, para. 84-85.
[186] *Ibid.*, para. 87.
[187] *Ibid.*, para 88-89.
[188] COM(2013) 846; COM(2013) 847.
[189] *Ibid.*, para. 90.
[190] *Ibid.*, para. 91.
[191] *Ibid.*, para. 92-93.

such rights committed by the US: legislation permitted authorities to access data content on a *generalized* basis and without possibilities of pursuing legal remedies.[192] Here the Court cited the fundamental right to an effective remedy guaranteed by Article 47 of the CFR, seen as "inherent in the existence of the rule of law."[193] As such, Article 1 of the Decision was declared invalid.[194] As Article 3 then denied the national supervisory authorities of the possibility of taking action to ensure compliance with the Directive, Article 3 was also declared invalid.[195] Because these two articles were inseparable from Articles 2 and 4 and the Annexes, the entirety of Decision 2000/520 was declared invalid.[196]

3. Implications

Following the *Snowden* revelations and Commission Communication in 2013, the Commission began discussions with US officials to renegotiate and strengthen Safe Harbor in January 2014, following the aforementioned 13 recommendations.[197] The *Schrems* ruling gave these negotiations urgency and also gave the EU an upper hand on insisting on a much higher level of protection, transparency, enforcement, and judicial redress. The decision threw data transfers to the US into legal uncertainty, as companies were not sure if flows would be blocked. However, the alternate means of standard contracts and binding corporate rules, although painstaking and tedious, have allowed for transfers to continue. US companies can also move data storage directly within the EU territory, and indeed, to avoid future problems, some have already begun this process.[198] Critics have

[192] *Ibid.*, para. 94-95; emphasis my own.
[193] *Ibid.*, para. 95.
[194] *Ibid.*, para. 98.
[195] *Ibid.*, para. 99-104.
[196] *Ibid.*, para. 105-106.
[197] European Commission, Communication from 29.2.2016 "Transatlantic Data Flows: Restoring Trust through Strong Safeguards," COM(2016) 117 final.
[198] Camino Mortera-Martinez and Rem Korteweg, "Adrift: The impact of the ECJ's Safe Harbour ruling," *Centre for European Reform Bulletin* (November 2015),

accused the ECJ of political motives by ruling on the Safe Harbor arrangement itself when it was not asked that question by the Irish Court.[199] Neither Facebook, Inc nor US officials were part of the hearings, potentially contributing to bias on the part of the Court. It also did not take into consideration 2014 surveillance reforms in the US because it relied on the 2013 Communication.[200] As the EU and US are bringing their ties closer together, particularly in trade through the current TTIP negotiations, many see this decision as disruptive and potentially a barrier to trade.[201] Others welcome the decision, particularly those in the European digital economy who must follow the high standards in EU and want the same rules for competitors.[202]

On 2 February 2016 a political agreement to replace Safe Harbor was released in the form of the EU-US Privacy Shield Framework, although it had still not been confirmed in a decision as of the completion of this thesis.[203] Some of the European Parliament have been critical of this sort of Safe Harbor 2.0, unsatisfied with the US promises and potential loopholes in the arrangement.[204] Because of this uncertainty, instead of discussing this replacement, it is more important to recognize what the *Schrems* ruling means for the future: that the EU is not willing to compromise or sacrifice the protection of fundamental rights.[205]

---

https://www.cer.org.uk/sites/default/files/bulletin_105_cmm_rk_article2.pdf (accessed 23 May 2016).

[199] Mortera-Martinez/Korteweg.

[200] Karin Kornbluh, "The Implications of the Safe Harbor Decision," Net Politics Blog, Council of Foreign Relations, entry posted 7 October 2015, http://blogs.cfr.org/cyber/2015/10/07/the-implications-of-the-european-safe-harbor-decision (accessed 23 May 2016).

[201] Petri, 805; Mortera-Martinez/Korteweg.

[202] Petri, 804.

[203] COM(2016) 117 final; see "Fact Sheet: Overview of the EU-U.S. Privacy Shield Framework," US Department of Commerce, entry posted 29 February 2016, http://www.commerce.gov/print/1834 (accessed 9 May 2016).

[204] "Safe-Harbor-Ersatz: EU und USA einig über neue Regeln für Datenaustausch," *Der Spiegel Online*, 2 February 2016, http://www.spiegel.de/netzwelt/netzpolitik/safe-harbor-ersatz-eu-und-usa-beschliessen-neue-regeln-a-1075304.html (accessed 23 May 2016).

[205] Petri, 805.

D. A New Era of Data Protection

Data flows between the EU and US will not only be affected by the striking down of Safe Harbor. After publication of a Proposal in January 2012 and much debate within the EU institutions, the new Regulation replacing the Directive was adopted on 27 April 2016. It is one part of the Commission's Data Reform Package, the other component being a directive in the area of police and judicial cooperation.[206] Cross-border data flows were one of the most debated topics in the Parliament, especially following the *Snowden* revelations, as Members of the European Parliament (MEPs) wanted to ensure European data was safe in the US.[207] The Regulation seeks to modernize the rules of the Directive, harmonize Member State data protection laws, simply procedures for companies and thus promote innovation in the European digital market, as well as raise the level of personal data protection.[208] While in some ways the Regulation opens the transfer of data to third countries to more possibilities and facilitates such processes, it also makes certain rules and conditions for such transfers more stringent and creates problems with its approach.

As has been established in the previous two chapters, the Directive and its approach to the transfer of data to third countries were problematic. It led to the creation of a political solution with the US, Safe Harbor, which from its inception had major weaknesses and ultimately fell apart. The problems of the Directive's adequacy test and its view of data protection in the international sphere have been transferred to the Regulation. Data protection needs to adapt to a world where data is no longer stored in physical books on shelves or within the handwritten letters of Warren and Brandeis. A "right to be left alone" takes on another meaning when major portions of citizens'

[206] COM(2016) 117 final.
[207] Christopher Kuner, Cédric Burton, and Anna Pateraki, "The Proposed EU Data Protection Regulation Two Years Later" *BNA Bloomberg, Privacy & Security Law Report, PVLR* 13, no. 8 (6 January 2014), 6.
[208] COM(2016) 117 final.

lives are publicly available and voluntarily uploaded onto various digital platforms. Such a change in understanding is necessary to consider for legislation if data is to flow efficiently across borders and legal protection is to remain effective.

This chapter analyzes issues regarding EU-US data flows moving forward into the 21st century. Data and privacy have changed, especially in the context of the Internet and technology. The Regulation is the EU's response to these circumstances, yet falls short in many regards, and even brings more questions than the Directive with it. Finally, the chapter presents suggestions for a new approach, one with more flexibility, balanced with respect for other interests such as free expression and information, and grounded in the reality of contemporary and future technology.

Many, if not most, discussions on modern privacy involve balancing this right with national security. While this is an extremely important argument, as governments increasingly use security interests to violate privacy, this thesis focuses on balancing privacy with freedom of expression and information, and freedom to trade. These freedoms are vital for data flows to flourish, and are also a natural part of the structure of the Internet.

I. Changing reality

For law to be effective, it must reflect the realities of the world and humanity. This section considers factors that have arisen in recent years regarding data on the Internet, along with the changing values that have come along with them. Certain legal privacy protections will have no meaning if they are not actually possible in the context of the Internet age. At the same time, such protections could also be used to severely hinder the incredible potential of the Internet for freedom of expression and information, as well as trade and economic development. Of course, law will always be "behind" technological development, even very far behind because of the pace of the

legislative process, particularly in the EU.[209] It is exactly because of this that more fundamental understanding of the Internet and today's technology is required, so that law, like the digital world, can be to a certain extent flexible and dynamic.

As has been acknowledged, the sheer amount of data available, collected, and processed has vastly grown in recent years, and is continuing to increase exponentially every year. With such dynamic numbers, law should not reflect specific studies, but it is still useful to note concrete numbers to understand the digital data world going forward. Because data flows are the concern here, it is most important to examine Internet traffic. As the Internet is not a centralized platform but rather has a distributed nature, it is difficult to accurately measure traffic. Internet traffic numbers do not measure data stored in a single server, but rather as data crosses from one point to another across the Internet. Useful figures are those in Internet Protocol (IP) traffic, as IP essentially enables the Internet. Simply defined, IP is the code or protocol used to deliver data packets from a server to a specified IP address. Cisco Systems, a major networking company, has published several studies estimating the growth of Internet traffic in the next few years.

According to Cisco, annual global data center IP traffic will grow "3-fold over the next 5 years," reaching "10.4 zettabytes (863 exabytes [EB] per month) by the end of 2019, up from 3.4 zettabytes (ZB) per year (287 EB per month) in 2014."[210] During the same time period, global cloud IP traffic will more than quadruple, reaching "8.6 ZB (719 EB per month) by the end of 2019, up from 2.1 ZB per year (176 EB per month) in 2014." For this reason, Cisco has labeled

[209] Christopher Kuner, et al., "The (data privacy) law hasn't even checked in when technology takes off," *International Data Privacy Law* 4, no. 3 (2014).

[210] "Cisco Global Cloud Index: Forecast and Methodology, 2014-2019 White Paper," Cisco, entry posted 21 April 2016, http://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/Cloud_Index_White_Paper.html?referring_site=RE&pos=3&page=http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/VNI_Hyperconnectivity_WP.html (accessed 29 May 2016).

contemporary times "The Zettabyte Era."[211] In case these numbers are not clear, the reader should consider the size of a kilobyte (kB) that is 1000 bytes, a megabyte (MB), 1000^2 bytes, and gigabyte (GB), 1000^3 bytes. Most active Internet and computer users today should comprehend such figures. Then, consider that an EB is 1000^6 bytes and a ZB is 1000^7 bytes. To put it another way, just 1 ZB is the equivalent to 1 trillion GB.

The use of cloud storage by consumers is rapidly growing. Cisco estimates that "by 2019, 55 percent (2 billion) of the consumer Internet population will use personal cloud storage, up from 42 percent (1.1 billion users) in 2014." There is a trend toward using online, remote storage and computing models, known as cloud computing. Cloud computing uses various pooled resources, including networks, servers, and storage, so that public and private sector users can conveniently work without requiring their own physical data base. The National Institute of Standards and Technology (NIST) of the US Department of Commerce defines cloud computing as containing five essential characteristics: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service.[212] Users are increasingly interconnected and networked, rather than working through a single data server.

Consumers, particularly in North America and Europe, are using multiple devices to connect to the Internet. By 2019, Cisco estimates that the average user in North America will own 13.6 devices or connections, in Western Europe 9.9, and in Central and Eastern Europe 6.2. It is notable, of course, that users are no longer limited to one home computer as in the days when the Directive was enacted. A huge increase has occurred in global mobile data traffic, which grew

[211] "The Zettabyte Era – Trends and Analysis," Cisco, entry posted 23 June 2015, http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/VNI_Hyperconnectivity_WP.html (accessed 29 May 2016).

[212] Timothy Grance and Peter Mell, "The NIST Definition of Cloud Computing," *National Institute of Standards and Technology* Special publication 800-145 (September 2011), 2.

74 percent in 2015 alone.[213] By 2020, these numbers are expected to grow eightfold, meaning "30.6 EB per month." Indeed, these figures are so large, they are difficult for the layman to comprehend. While more statistics could be enumerated, it should by now be clear: global data flows, and particularly those between major world players, such as the EU and US, will be increasing at rapid rates in upcoming years. Data is transferred, stored in various locations, copied, collected, processed, and shared at unprecedented levels.

It is not just the sheer amount of data and Internet traffic, and increasing use of networked structures, such as cloud computing, that needs to be taken into account. The Internet, and especially social media, has changed humanity's mentality surrounding every day privacy and markets. Business models are now social media driven: companies mine for data on customer preferences, including through their demonstrated interests on social media, to market their products. While traditional ideas about privacy would find such data mining intrusive, new approaches see the market now as an interconnected "ecosystem," through which consumers connect and interact with producers at a much higher degree than in the past.[214] Internet and social media users willingly and freely post pictures, videos, thoughts, political views, and more every day on various platforms such as Facebook, Twitter, and personal blogs and websites. Increased knowledge and interactivity in such a social media driven environment is leading to better products, consumer satisfaction, entrepreneurial opportunity, and innovation in the private sector, as well as more knowledge and information for citizens about their governments, politicians, rights, and liberties in the public sector. Yet

[213] "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2015-2020 White Paper," Cisco, entry posted 1 February 2016, http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html?referring_site=RE&pos=2&page=http://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/Cloud_Index_White_Paper.html (accessed 29 May 2016).

[214] Victoria L. Crittenden, Richard Hanna, and Andrew Rohm, "We're all connected: The power of the social media ecosystem," *Business Horizons* 54, no.3 (2011), 266.

of course, this means that the concept of privacy as was envisioned in Western culture may belong to the past, for better or for worse.[215] Perhaps privacy is not fully dead, but it needs to be reformulated in today's information age.[216] Privacy is a trade-off with many interests: security, free speech, technology, better business, and more.[217] Where exactly Internet users draw the line to protect their personal information is dependent on many factors such as age and culture. There is no one-size-fits-all answer.

Data flows are also affected by an increasingly globalized market and political sphere. Communication and media, business and trade, education, transportation, and more are all eliminating traditional ideas about borders. The concept of physical territory is losing meaning as society is tied to borderless networks. While acknowledging that such a philosophical idea is much beyond the scope of this thesis, the general thought needs to be kept in mind when discussing data flows.

II. The Regulation: Effects on EU-US data flows

The current environment of the digital world has brought about calls for legislative change in data protection. In the EU, this ushered in the replacement of the Directive. The decision to change legislative tools from a directive to a regulation is part of accomplishing the goal of harmonizing Member State data protection law. While the objectives and principles remain the same, the Regulation intends to correct the legal uncertainty and distortion of the Internal Market that arose from fragmentation in the Directive implementation process

[215] For more on social media and its effects, see Erik Qualman, *Socialnomics: How Social Media Transforms the Way We Live and Do Business* (Hoboken, New Jersey: John Wiley & Sons, 2011).

[216] See Katherine Sarah Raynes-Goldie, "Rethinking Privacy in the Age of Facebook," in Privacy in the Age of Facebook: Discourse, Architecture, Consequences" (PhD diss., Curtin University, 2012), 208-225.

[217] David E. Pozen, "Privacy-Privacy Tradeoffs," *The University of Chicago Law Review* 83, no.1 (2016), 221-222.

amongst Member States.[218] Member States had interpreted the Directive, especially in regards to the meaning of consent, in different ways and the Commission sought to rectify this. Such a change in legal tools also sends a political message from the EU institutions, as it fully Europeanizes data protection law and empowers the EU to continue its role promoting a high level of protection in the world.[219]

The Regulation acknowledges rapidly changing technology, globalization, a massive increase in data collection and sharing, as well the tendency of natural persons to publicize their personal information globally.[220] It seeks to respond to such trends while ensuring a high level of data protection. The change from a Directive to a Regulation is one of these responses. It intends to strengthen and make data protection more coherent and better enforced.[221] As a regulation, it has direct effect on the Member States. However, Member States are still permitted to specify the applications of its rules by maintaining or introducing provisions in its national legislation, for which the Regulation provides a "margin of manouevre," especially in sector-specific laws and special categories of data ("sensitive data").[222] Member States can also maintain or introduce legislation regarding data processing for legal obligation compliance, public interest tasks, or exercise of official authority vested in a controller. As with the Directive, the Regulation does not apply to activities outside the scope of EU law, such as activities concerning national security, as well as processing by Member States when carrying out activities related to the EU common foreign and security policy.[223]

Three areas of the Regulation will have a profound effect on data flows. First, the Regulation codifies new concepts surrounding privacy rights, which are absent in the US. Next, it expands the territorial

[218] Regulation 2016/679, Recital 9.
[219] Schwartz, "EU-US Collision," 1993.
[220] Regulation 2016/679, Recital 6.
[221] *Ibid.*, Recital 7.
[222] *Ibid.*, Recital 10.
[223] *Ibid.*, Recital 16.

scope of application to have extra-territorial effects. Lastly, it updates and alters its requirements for the transfer of data to third countries.

1. Concepts of privacy rights

The Regulation intends to strengthen and specify the rights of data subjects.[224] In this regard it introduces new rights and protections. Of particular prominence is the extension of the right to erasure to also entail a codified right to be forgotten in Article 17. This goes far beyond the right to rectification in Article 16, through which data collectors must correct inaccurate personal data upon the request of the data subject. According to Article 17, data controllers will be obliged to erase personal data of a data subject upon request on the following grounds:

a) the data is no longer necessary for the purposes it was collected or processed

b) the data subject withdraws consent on which the processing is based and where there is no other legal ground for the processing

c) the data subject objects to the processing and there are no overriding legitimate grounds to justify the processing

d) the data was unlawfully processed

e) for the data subject's compliance with a Union or national legal obligation

f) the data was collected for the offer of information society services.

Such grounds do not apply when the processing is necessary for the following reasons:

a) the exercise of freedom of expression and information

b) the data controller's compliance with a Union or national legal obligation

c) public interest in the area of public health

d) public interest archiving, scientific research, historical research, or statistical purposes if it would render such purposes impossible or seriously impair their objectives achievement

e) establishment, exercise, or defense of legal claims.

[224] *Ibid.*, Recital 11.

Further strengthening the individual data subjects' rights over their personal data is the creation of the right to data portability in Article 20. Data subjects have the right to request and receive their personal data from a controller in a "structured, commonly used and machine-readable format" and "the right to transmit the data to another controller without hindrance" from the original controller, on the conditions that the processing:

> a) was based on consent or on a contract, and
>
> b) is carried out by automated means.

Such a right applies neither to processing necessary for public interest tasks or exercised through official authority, and it "shall not adversely affect the rights and freedoms of others."

These rights demonstrate a new understanding of privacy rights and data. At the time of its draft stage, *Jacob Victor* argued that despite articulating a fundamental-rights-based approach to privacy rights, the Regulation actually uses a property-rights-based approach as conceived by *Paul Schwartz*.[225] His claim was based on three elements he identified in the Regulation Proposal:

> "consumers are granted clear entitlements to their own data; the data, even after it is transferred, carries a burden that 'runs with' it and binds third parties; and consumers are protected through remedies grounded in 'property rules.'"[226]

Such a concept will undoubtedly affect data flows: with the Regulation, the EU is viewing electronic personal data almost as physical files that would be placed on a plane and flown over to the US, and thus could be fully controlled, transferred easily, and even deleted.

Inclusion of these rights is controversial, as previously discussed when the ECJ created the right to be forgotten in the *Google Spain*

[225] Jacob M. Victor, "The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy," *Yale Law Journal* 123, no. 2 (November 2013), 515. For more on this distinction and approach, see Paul M. Schwartz, "Property, Privacy, and Personal Data," *Harvard Law Review* 117, no. 7 (May 2004), 2056-2128.
[226] Victor, 515.

case. First and foremost, it brings with it a serious threat to freedom of expression and information. When the Regulation was first proposed in its draft form in 2012, American scholar *Jeffrey Rosen* had strong words for the new right, stating that it had the potential to "transform Google, for example, into a censor-in-chief for the European Union, rather than a neutral platform."[227] The right is written very broadly to include any data concerning the data subject and includes obligations from controllers and processors, thus the potential effects would be far-reaching and could compromise the freedom and openness of the Internet. It is understandable that European regulators are concerned that in today's Internet, users cannot escape information posted about them (which they may have posted themselves) however regrettable they may consider it years later.

An approach that compromises the fundamental right of freedom of information is no proper answer. The right be forgotten also leads to a potential clash with the US, and could affect data flows. Americans have taken a very different approach to such a problem, and have prioritized First Amendment speech rights. *Rosen* has noted that the US Supreme Court already ruled in 1989 that laws cannot restrict media from revealing truthful information if it was legally obtained, even if it is embarrassing.[228]

Furthermore, whether guaranteeing such a right is feasible is seriously questionable. A purely technical approach is outright impossible, and an attempt to achieve it will require much coordination and control over data on the Internet.[229] With such levels of control will an open and free Internet even remain for Europeans to use? Another issue arising from such a right as written both in the

[227] Jeffrey Rosen, "The Right to Be Forgotten," *Stanford Law Review Online* 64 (2012), 88-92.

[228] Florida Star v. B.J.F., 491 U.S. 524.

[229] Peter Druschel et al., "The Right to Be Forgotten-Between Expectations and Practice," *European Network and Information Security Agency* (20 November 2012), https://cispa.saarland/wp-content/uploads/2016/03/right_to_be_forgotten_112012.pdf (accessed 28 May 2016).

Google Spain ruling and the Regulation is that the process of erasing data is left in the hands of data controllers and processors. Following thousands of requests to delink material after the ECJ ruling, Google began by deciding which requests were valid. Two issues have already surfaced. First, some of the deleted material has reappeared on sites such as "Hidden from Google"[230] which are documenting what they see as censorship.[231] Second, there is a lack of transparency on Google's decision making process. Critics have characterized Google as a sort of judge, jury, and executioner, the result of the legal language, not Google's own making.[232] In 2015, Google's archived Transparency Report was leaked, revealing thousands of the delisting requests.[233] Promisingly, only about 5% of the leaks were under the categories serious crime, public figure, political, or child protection. Most requests were related to the personal information of average citizens, calming some concerns thus far about censorship. Notwithstanding details about Google's decision-making process, and even data categorization, remain to be revealed. The ability to find archived web material, just like was done with the Transparency Report, also puts into question the efficacy of the right to be forgotten, especially if Google's own data regarding the requests are susceptible to leakage. Finally, the judge-jury concern will only be expanded with the right applying to all controllers and processors, not just Google and search engines.

[230] Hidden from Google, http://hiddenfromgoogle.afaqtariq.com/ (accessed 30 May 2016).
[231] Pozen, 222.
[232] Julia Powles, "Google's data leak reveals flaws in making it judge and jury over our rights," *The Guardian* (14 July 2015), https://www.theguardian.com/technology/2015/jul/14/googles-data-leak-right-to-be-forgotten (accessed 29 May 2016).
[233] Julia Powles and Sylvia Tippmann, "Google accidentally reveals data on 'right to be forgotten' requests," *The Guardian* (14 July 2015), https://www.theguardian.com/technology/2015/jul/14/google-accidentally-reveals-right-to-be-forgotten-requests (accessed 29 May 2016).

2. Territorial scope

The territorial scope of the Regulation, laid out in Article 3, marks a clear break from that of the Directive. Article 3(1) establishes that the "Regulation applies to processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not."[234] With this latter clause, EU data protection law now has extraterritorial effect.[235] This codifies the reasoning behind the ECJ's ruling in the *Google Spain* case on the territorial scope of the Directive.[236] As aforementioned, the *Google Spain* case extended the reach of the Directive to the processing of data "in the context of activities" of establishments, including search engines, outside of the EU who had established a branch or subsidiary within the EU that offered advertising space and oriented their activities toward EU inhabitants.[237] The ECJ had argued that if a search engine were able to escape the obligations of the Directive, it would compromise the effectiveness of the Directive and protection of fundamental rights.[238] The Regulation not only makes such extra-territorial effect binding, it goes beyond the requirements of the ECJ. Article 3(2) of the Regulation clarifies that its contents apply to data controllers and processors outside of Union territory when the activities related to

> a) offering goods or services to data subjects in the EU, whether or not payment is required, or
>
> b) monitoring the behavior of said data subjects, as far as such behavior occurs within EU territory.

According to Recital 23, to qualify for the requirement of Article 3(2a), controllers or processors must "envisage" offering goods or

[234] Regulation 2016/679, Art. 3.

[235] Kuner, et al, "Proposed Regulation Two Years Later,"2.

[236] Pietro Franzina, "The EU General Data Protection Regulation: a look at the provisions that deal specifically with cross-border situations," Conflict of Laws .net, entry posted 10 May 2016, http://conflictoflaws.net/2016/the-eu-general-data-protection-regulation-a-look-at-the-provisions-that-deal-specifically-with-cross-border-situations (accessed 24 May 2016).

[237] Case C-131/12, para. 60.

[238] *Ibid.*, para. 58.

services to EU data subjects in one or more Member State. Such a determination should include factors such as EU language or currency use or mentioning EU customers or users. It would be insufficient to make such a determination only because of website accessibility, email or contact details, or use of the language in said controller's country. As for Article 3(2b), Recital 24 clarifies that such monitoring is determined by behavior tracking natural persons on the Internet, and includes subsequent processing techniques such as profiling, particularly when such data is used for analysis or prediction of the data subject's personal preferences, behaviors, and attitudes.

As for the use of the term "inhabitants" of the EU, it is unclear whether protection is limited to those who are explicit residents, whether or not such residence can be temporary or only permanent, and whether those who have resident both in the EU and outside the territory would be afforded the same protection.[239]

Such extraterritorial effect therefore brings the activities of many American data processors and controllers, both private and public, within the jurisdiction of the Regulation. This accomplishes the EU's goal to make the European digital market a more equal playing field for all competitors.[240] Any American company working within the EU, especially the large digital corporations such as Facebook and Google, will have to follow the same data protection rules as European ones. The effect, however, brings with it the question of judicial remedy. It is not clear yet, how judgments against companies and firms in third countries would be enforced.[241] In line with Article 47 CFR, Article 79 of the Regulation guarantees the right to an effective judicial

[239] Christopher Kuner, "The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law," *BNA Bloomberg, Privacy & Security Law Report, PVLR* 11, no. 6 (6 February 2012), 4.

[240] Alexander Roßnagel and Maxi Nebel, "Policy Paper: Die neue Datenschutzgrundverordnung: Ist das Datenschutzrecht nun für heutige Herausforderungen gerüstet?," *Forum Privatheit und Selbstbestimmtes Leben in der digitalen Welt* (Karlsruhe: Frauenhofer Institut für System- und Innovationsforschüng ISI, 2016), 4.

[241] Ulrich Emmert, "Europäische und nationale Regulierungen: Konsequenzen für den Datenschutz nach dem Ende von Safe Harbor," *Datenschutz und Datensicherheit* 40, no.1 (January 2016), 4.

remedy against a controller or processor. Data subjects who consider that their rights have been infringed upon may bring forward proceedings before Member State courts where the controller or processer has an establishment or where the data subjects have habitual residence, unless said controller or processor is a Member State public authority exercising public power. If an American controller or processor has no establishment within the Union, but because of Article 3 its activities are within the scope of the Regulation and thus proceedings can be initiated against it, how can a national court's ruling be enforced against it? Will courts and supervisory authorities easily stop the flow of data to the US?

3. Transfer of data to third countries

As with the Directive, the Regulation it clear in its Recital 101 that the rights and protections it ensures shall not be undermined by the transfer of data to non-EU countries. It adds that the principle of transfers applies as well to international organizations, not just third countries. Chapter V of the Regulation, composed of Articles 44 through 50, is devoted to transfers to third countries or international organizations.[242] The incredibly important shift in the Regulation is that rather than presume transfers will be forbidden unless a third country provides adequate protection as in the Directive, it sets forth criteria for which transfers are permitted.[243] Transfers are permissible under three conditions: an adequacy decision of the third country from the Commission, appropriate safeguards provided by data controllers or processors, or specific situations laid out in the derogations.

The Regulation is much more precise than the Directive on the meaning of adequacy, which as previously criticized, was a serious problem leading to arbitrariness and politicization of decisions. Using

[242] For the sake of simplicity, I will simply refer to third countries, but keep in mind that this also includes transfers to international organizations.

[243] Rolf H. Weber, "Transborder data transfers: concepts, regulatory approaches and new legislative initiatives," *International Data Privacy Law* 3, no.2 (2013), 127.

the language of the ECJ, the Regulation states that a third country must provide "essentially equivalent" protection to be considered adequate. It goes on to clarify that "the third country should ensure effective independent data protection supervision and should provide for cooperation mechanisms with the Member States' data protection authorities, and the data subjects should be provided with effective and enforceable rights and effective administrative and judicial redress."[244]

Article 45 lays out the criteria for an adequacy decision, requiring the Commission to take several factors into consideration. Unlike the Directive, which vaguely stated that the Commission and Member States are to inform each other when they believe a country's protection is not adequate and does not put forward a procedure, the Regulation makes it clear that the Commission will make decisions regarding adequacy. This centralizes power on data protection within the hands of the Commission. In addition to more general factors such as rule of law and respect for human rights, the Commission must also consider whether the third country provides "effective and enforceable data subject rights" along with administrative and judicial redress possibilities. It explicitly requires Commission to consider whether the third country has an independent supervisory authority, which is to cooperate with the authorities in Member States, and whether the third country has committed to international agreements on data protection. Decisions are to be reviewed at least every four years and the Commission is to monitor developments which may affect the decision, and take action such as repealing, amending, or suspending the decision if the third country no longer provides adequate protection. Undoubtedly, this language and specifications are a noteworthy improvement to the shortcomings of the Directive.

While the Directive only mentioned the possibility of approving transfers under adequate safeguards provided for by controllers as a derogation, the Regulation sees such safeguards as alternatives to

[244] Regulation 2016/679, Recital 104.

adequacy decisions. It provides two articles on such conditions. Article 46 first qualifies the condition for appropriate safeguards: data subject rights and effect legal remedies must be available. Appropriate safeguards may take the following forms without specific authorization from a supervisory authority: a legally binding and enforceable instrument between public authorities or bodies, binding corporate rules (clarified in Article 47), standard data protection clauses approved by the Commission, an approved code of conduct, or an approved certification mechanism. Additionally, contractual clauses between the controller, processors, and/or recipients, as well as provisions inserted into administrative arrangements between public authorities may be approved by the competent supervisory authority. The Regulation devotes Article 47 to binding corporate rules, giving weight to such arrangements. It marks a move away from relying primarily on a geographically-based approach to transborder data flow protection to one that is organizationally-based.[245] Article 47(2) lays out the requirements for binding corporate rules, which apply to a group of undertakings or a group of enterprises engaged in a joint economic activity. Similar requirements for binding corporate rules were already laid out by the Article 29 Working Party, but previously were limited to controllers and not permitted for use by processors.[246] Additionally, such explicit legal recognition eliminates any remaining barriers in Member State law.[247] The Working Party defines binding corporate rules as "internal rules (such as a Code of Conduct) adopted by multinational group of companies which define its global policy with regard to the international transfers of personal data within the same corporate group." They are used by entities located in third countries that the Commission has not approved as providing an adequate level of data protection.

[245] For more on this distinction, see Kuner *OECD Papers No. 187*, 20.

[246] The procedures and requirements were laid out in various documents, see European Commission, "Overview on Binding Corporate rules," http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm (accessed 27 May 2016).

[247] Kuner "Data Protection Regulation," 10.

The Regulation also allows for unauthorized transfers required by a court or tribunal judgment or third country administrative authority only if it is based on an international agreement between the requesting third country and the Union or a Member State.[248] Article 49 specifies the situational derogations permitted, which remain similar to those listed in the Directive.

Lastly, the Directive will still have certain legal effects here in that authorizations by a Member State or supervisory board based as well as Commission Decisions based on Article 26 of the Directive will remain valid until amended, replaced, or repealed.[249] If the Safe Harbor arrangement had not been invalidated by the ECJ, therefore, it would have remained in effect.

Overall, this chapter is a significant improvement over the Directive in that it makes the process of approval for transfers clearer and more precise, which could help avoid the issues the Directive brought with Safe Harbor.

III. Suggestions for sustainable solutions

In a globalized, interconnected world, data flows are only going to increase in importance in individual lives. Adoption of the Regulation recognized this, and in some areas facilitated transborder data flows, but in others, erected potential barriers. It contradicts itself, and as *Paul Schwartz* noted, has potential both to destabilize and forge new paths for EU-US data flows.[250] Ultimately, the Regulation still falls short of a future-minded approach to the problems arising from transborder data flows, especially those with the US. Data flows have less to do with borders as technology changes: information constantly moves through networks and servers in various countries. Societally, Internet users are also progressively more connected, especially through social networks and the sharing of information via platforms

[248] Regulation 2016/679, Article 48.
[249] *Ibid.*, Article 46 (5).
[250] *Schwartz* was referring to the Proposal and goes on to examine the issues addressed here as well as others; Schwartz, "EU-US Collision," 1992-2008.

such as Wikipedia. For this reason, protection of privacy and data must not be seen as a territorial issue but rather a global one. International agreements on data protection are not only difficult, if not impossible, to create. They are also likely to fail and provide worse data protection: with such vast amounts of data flowing through complex networks, international agencies and regulators would be unlikely to be able to provide protection of individuals while maintaining an open and free Internet.

In his 2013 book *Transborder Data Flows and Data Privacy Law*, data protection legal scholar *Christopher Kuner* proposes a global regulatory framework for transborder data flows based on approaching the issue as a case of legal pluralism.[251] A starting point to achieving such a framework could be applying principles based on legal pluralism to the smaller scope of EU-US, rather than global, data flows. Because of their contrasting approaches to data protection and views on privacy, conflict is likely to continue occurring between the two legal jurisdictions. Because of their massive share of global data flows, it is vital to prevent such conflict. An agreement that draws on the strengths of the jurisdictions, respects each other's values, and is based firmly in the reality of Internet traffic could accomplish such a goal. If successfully implemented, such an agreement could then provide a basis for an international arrangement. It should also not merely be an arrangement based on a Commission Decision, like Safe Harbor or the current proposed EU-US Data Privacy Shield, but a formal agreement in order to last. It would also need more democratic legitimacy than an arrangement between the Commission and US Department of Commerce. The following are elements that should be incorporated as well as pre-requisites for its success. They are not meant as a complete list of requirements for a framework, but selected considerations for a functional future agreement.

[251] Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (Oxford, UK: Oxford University Press, 2013), 157-187.

a) Eliminate additional legal basis for transfers of data outside of the EU

Here, the Regulation was a step in the right direction but did not go far enough. Fortunately, the Regulation abandoned the presumption that transfers to a third country are prohibited unless adequate protection is provided. Unfortunately, it still requires additional criteria for data to be transferred out of the EU and still keeps the avenue of territorial adequacy decisions as the primary means of approval for transfers. As *Kuner* argues, because data flows function the same whether they are crossing "borders" or not, and data is so interconnected, making it difficult to distinguish when it is supposedly crossing borders, it does not make sense to require a legal basis *before* transfers occur.[252] Simply put, restrictions on data transfers based on borders do not accommodate the reality of networked computing.[253] The requirements for data protection in the EU could still be enforced, and violations would be solved *after* the fact.

This would eliminate the arbitrary and political nature of adequacy decisions, especially those targeted to other third countries. Even although the Regulation clarified the procedure for decisions, they remain too vague and potentially problematic. It is incredibly difficult to accurately and objectively assess protection in a third country, leading to questionable decisions. The history of Safe Harbor demonstrates this: the deficient arrangement was created and fell apart for political reasons. Organizational arrangements such as binding corporate rules can be used for purposes of

[252] Kuner, *Transborder Data Flows*, 166.
[253] Horacio E. Gutiérrez and Daniel Korn, "Facilitando the Cloud: Data Protection Regulation as a Driver of National Competitiveness in Latin America," *The University of Miami Inter-American Law Review* 45, no. 1 (Fall 2013), 49.

data protection law enforcement, but requirements for data flows should not be based on the crossing of borders.

b) *Enforce extraterritorial effect*

If point a) is achieved, the Regulation would have to apply to activities involving its citizens regardless of where a violation occurred in order to maintain data protection standards. The Regulation does this by creating extraterritorial effect. Following a theory of legal pluralism, the agreement would respect and enforce this. As aforementioned, enforcement of such an effect could be problematic without agreements for cooperation outside EU territory. Therefore, it is necessary that the EU and US cooperate to enforce each other's data protection laws. Rather than base the applicability of laws on physical location of data, it should solely be based on the activities of those it involves.

c) *Ensure protection against State intrusion*

The fall of Safe Harbor was ultimately caused by its inability to prevent the US government, not private actors, from violating the privacy rights of EU citizens. Compliance with data protection on the part of public actors is not essential for effective privacy rights, it is possible to legally achieve: what limited data protection law exists in the US is primarily to protect against state intrusion, and thus the US cannot argue it is against its fundamental rights values. Politically, the US would most likely want broad discretion for its national security interests, but here, perhaps the EU could use political maneuvers. After all, it is not in the US economic and growth interests for another *Schrems*-like ruling to occur. This is not the place for political conjecture, however. If a lasting and meaningful agreement is to be created, it must include such protection. Access to judicial remedy follows from this protection.

d) *Prioritize freedom of expression and information*

Where the EU, both in case law and the Regulation, has truly gone astray is failing to prioritize the rights of freedom of expression and information. The entire conversation on transborder data flows, *Kuner* explains, has not prioritized these rights, so essential to human freedom and democratic values.[254] An open and free Internet is desirable for trade, economic growth, and development, but much more importantly, for the ability of humans throughout the world to have an uncensored voice and access to unfiltered knowledge. Data flows therefore serve freedom of expression, and likewise, freedom of expression and information is an essential component of data flows, and must be part of the conversation. The US strength in protecting free speech can serve as a counterweight to the EU trend.

e) Prioritize transparency

Along the lines of point d), rather than focusing on control of information, protection of privacy and data should spend its efforts on greater transparency. Effective enforcement of data protection law has already been questionable. An attainable objective will be to prioritize transparency on the part of both public and private actors. If citizens are unaware of their rights, the uses of their data by private and public actors, the meanings behind policies, and other issues, then solutions such as guaranteed judicial remedy are pointless. Furthermore, data protection procedures and regulations are often complex and unclear, making compliance less probable as well as endangering data flows.

f) Ensure flexibility of definitions in regulation

Because means of data flows are rapidly changing and growing, any agreement should not be dependent on specific technology. In the EU, for much time there was argument over definitions of controllers, processors, transits, and other terms,

[254] Kuner, *Transborder Data Flows*, 169.

which led to confusion, lack of compliance, and loss of meaning as technology changed.[255] Lack of compliance with the Safe Harbor principles and issues with binding corporate rules were also related to confusion on definitions.[256] Arbitrary decisions based on vague terms are naturally to be avoided, but so are such strict terms that they would no longer make sense five years later.

g) Re-formulate privacy

This is the most difficult and vague suggestion, but one that needs to be said. Whether it is possible in a legal and political context is not certain. The forces of the Internet, and particularly social media, are changing the concept of privacy in the EU and US. Agreement on what constitutes privacy that should be protected will not be easy to reconcile in one jurisdiction, much less both. Here, time and slower societal change may bring about potential answers. However, if the EU is to effectively protect privacy, it cannot hold onto concepts that are not in line with reality. The example of the right to be forgotten is key. As data flows and the size of global data grow, citizens are naturally concerned about the easy availability and accessibility of their personal information. Responses that treat data like a book that can be burned are not proper solutions.

Re-formulating the meaning of privacy as well as the role of privacy law will take time. Possible solutions is turning privacy law more toward the attainable goals of ensuring data is secure and controllers and processors are held accountable for leaks. Meanwhile, preventing personal information that was willingly and freely uploaded to public forums from spreading through the Internet is a fruitless effort with dangerous implications. Already in the early 1990's, Internet pioneer John Gilmore put it best: "The Net interprets

[255] Kuner, "Copernican Revolution," 3-5.
[256] *Ibid.,* 10

censorship as damage and routes around it."[257] Law that ignores this wisdom is bound to fail.

E. Conclusion

This thesis sought to present considerations for a future digital landscape in which law matches reality, ensures effective protection of fundamental rights, and avoids the shortcomings of the past. Data will continue to flow between the EU and US no matter if legislation is in place or not, save for the highly unlikely event of a complete shutdown of the Internet. Despite all its problems and lack of enforcement, data still flowed between the jurisdictions under the previous Safe Harbor arrangement forged under the 1995 Directive. During the Directive years, the EU sharpened its protection of data and understanding of privacy rights. This environment led to higher tensions with the US, which continues to promulgate a contrasting understanding of said privacy rights and the appropriate role of legislation. As always, politics played a role in this conflict, first enabling Safe Harbor and later inducing the *Schrems* decision. Both jurisdictions acknowledge the importance of data flows but have been unable to formulate a proper and lasting framework.

As the EU and US prepare for the entering into force of the General Data Protection Regulation, it is useful to take a step back and understand how the current situation arose. It is a ripe juncture to look beyond political solutions and Safe Harbor replacements and instead envision a better landscape for EU-US data flows. Together with a consideration of the strengths and mistakes of the past, such future-minded proposals enable an informed reading of the newly minted Regulation. There are no simple answers to the complexity of transborder data flow regulation, much less between the EU and US. Yet it is precisely out of such conflict, a manifestation of the difficulty

[257] As quoted in Philip Elmer Dewitt, "First Nation in Cyberspace," *TIME International* 49 (6 December 1993), available at http://www.chemie.fu-berlin.de/outerspace/internet-article.html (accessed 30 May 2016).

of balancing fundamental rights, that a meaningful resolution can be found.

List of Documents

Böhm, Franziska. "Legal opinion on the adequacy of the safe harbor decision, Case 362/14 Maximillian Schrems v. Data Protection Commissioner," in Case 362/14, Annex A.1. [n.d.].

European Commission. "Commission decisions on the adequacy of the protection of personal data in third countries," last updated 23 March 2016. http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm (accessed 30 May 2016).

_____. Communication from 29.2.2016, "Transatlantic Data Flows: Restoring Trust through Strong Safeguards," COM(2016) 117 final, Brussels.

_____. "EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield." Press Release Database, 2 February 2016. http://europa.eu/rapid/press-release_IP-16-216_en.htm (accessed 31 May 2016).

_____. Communication from 27.11.2013, "Functioning of the Safe Harbor from the Perspective of EU Citizens and Companies Established in the EU," COM(2013) 847 final, Brussels.

_____. Communication from 27.11.2013, "Rebuilding trust in EU-US Data Flows," COM(2013) 846 final, Brussels.

_____. The implementation of Commission Decision 2000/520/EC on the adequate protection of personal data provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce. 2004, Brussels.

_____. The Application of Commission Decision 2000/520/EC of 26 July 2000 Pursuant to Directive 95/46 of the European Parliament and the Council. 2002, Brussels.

_____. 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce.

_____. "Overview on Binding Corporate rules." [n.d.]. http://ec.europa.eu/justice/data-protection/international-

transfers/binding-corporate-rules/index_en.htm (accessed 27 May 2016).

United States Department of Commerce. Safe Harbor Privacy Principles. 21 July 2000.

Bibliography

Aaronson, Susan Ariel and Rob Maxim. "Data Protection and Digital Trade in the Wake of the NSA Revelations," in "Forum: EU Data Protection Reform: Opportunities and Concerns." *Intereconomics* 48, no. 5 (2013): 281-285.

Ball, James. "NSA monitored calls of 35 world leaders after US official handed over contacts." *The Guardian*, 25 October 2013. http://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls (accessed 22 May 2016).

Baumann, Bastian. *Datenschutzkonflikte zwischen der EU und den USA*. Berlin, Germany: Dunker & Humblot, 2016.

Bergmann, Michael. *Grenzüberschreitender Datenschutz*, Baden-Baden, Germany: Nomos Verlagsgesellschaft, 1985.

Bignami, Francesca. "Cooperative Legalism and the Non-Americanization of European Regulatory Styles: The Case of Data Privacy." *The American Journal of Comparative Law* 59, no. 1 (Spring 2011): 411-461.

_____. "European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining." *Boston College Law Review* 48, issue 3, no. 3 (2007): 609-698.

Brandeis, Louis D. and Samuel D. Warren. "The Right to Privacy." *Harvard Law Review* 4, no. 5 (December 1890).

Brennscheidt, Kirstin. *Cloud Computing und Datenschutz.* Baden-Baden, Germany: Nomos Verlagsgesellschaft, 2013.

Cole, Matthew and Mike Brunker. "Edward Snowden: A Timeline." *NBC News*, 24 May 2014. http://www.nbcnews.com/feature/edward-snowden-interview/edward-snowden-timeline-n114871 (accessed 22 May 2016).

"Cisco Global Cloud Index: Forecast and Methodology, 2014-2019 White Paper." Cisco, entry posted 21 April 2016. http://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/Cloud_Index_White_Paper.html?referring_site=RE&pos=3&page=http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/VNI_Hyperconnectivity_WP.html (accessed 29 May 2016).

"Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2015-2020 White Paper," Cisco, entry posted 1 February 2016. http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html?referring_site=RE&pos=2&page=http://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/Cloud_Index_White_Paper.html (accessed 29 May 2016).

Cowans, Clemens David. *Ein „modernes" europäisches Datenschutzrecht*. Frankfurt, Germany: Peter Lang GmbH, 2012.

Crittenden, Victoria L., Richard Hanna, and Andrew Rohm. "We're all connected: The power of the social media ecosystem." *Business Horizons* 54, no. 3 (2011).

Dammann, Ulrich and Spiros Simitis. *EG-Datenschutzrichtlinie: Kommentar*, Baden-Baden, Germany: Nomos Verlagsgesellschaft, 1997.

Dewitt, Philip Elmer. "First Nation in Cyberspace." *TIME International* 49 (6 December 1993), available at http://www.chemie.fu-berlin.de/outerspace/internet-article.html (accessed 30 May 2016).

Dhont, Jan, María Verónica Pérez Asinari, and Yves Poullet. "Safe Harbour Decision Implementation Study." 19 April 2004. http://ec.europa.eu/justice/data-protection/document/studies/files/safe-harbour-2004_en.pdf (accessed 22 May 2016).

Druschel, Peter, et al. "The Right to Be Forgotten-Between Expectations and Practice." *European Network and Information Security Agency* (20 November 2012). https://cispa.saarland/wp-content/uploads/2016/03/right_to_be_forgotten_112012.pdf (accessed 28 May 2016).

Ehmann, Eugen and Marcus Helfrich. *EG Datenschutzrichtlinie: Kurzkommentar*, Cologne, Germany: Verlag Dr. Otto Schmidt KG, 1999.

Engel, Alexandra. "Reichweite und Umsetzung des Datenschutzes gemäß der Richtlinie 95/46/EC für aus der Europäisches Union

in Drittländer exportierte Daten am Beispiel der USA." PhD diss, Freie Universität Berlin, 2003.

Emmert, Ulrich. "Europäische und nationale Regulierungen: Konsequenzen für den Datenschutz nach dem Ende von Safe Harbor." *Datenschutz und Datensicherheit* 40, no.1 (January 2016): 34-37.

"Fact Sheet: Overview of the EU-U.S. Privacy Shield Framework." US Department of Commerce, entry posted 29 February 2016. http://www.commerce.gov/print/1834 (accessed 9 May 2016).

Farrell, Henry. "Constructing the International Foundations of E-Commerce: The EU-U.S. Safe Harbor Arrangement." *International Organization* 57, no. 2 (2003): 277-306.

Franzina, Pietro. "The EU General Data Protection Regulation: a look at the provisions that deal specifically with cross-border situations." Conflict of Laws .net, entry posted 10 May 2016. http://conflictoflaws.net/2016/the-eu-general-data-protection-regulation-a-look-at-the-provisions-that-deal-specifically-with-cross-border-situations (accessed 24 May 2016).

Froomkin, A. Michael. "The Death of Privacy?" *Stanford Law Review* 52, no. 5 "Symposium: Cyberspace and Privacy: A New Legal Paradigm?" (May 2000): 1461-1543.

Gavison, Ruth. "Privacy and the Limits of Law." *The Yale Law Journal* 89, no. 3 (January 1980): 421-471.

Genz, Alexander. *Datenschutz in Europa und den USA: Eine rechtsvergleichende Untersuchung unter besonderer Berücksichtigung der Safe-Harbor-Lösung*, Wiesbaden, Germany: Deutscher Universitätsverlag, 2004.

Grance, Timothy and Peter Mell. "The NIST Definition of Cloud Computing." *National Institute of Standards and Technology* Special publication 800-145 (September 2011). http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf (accessed 28 May 2016).

Greenwald, Glenn, Ewen MacAskill, and Laura Poitras. "Edward Snowden: the whistleblower behind the NSA surveillance revelations." *The Guardian*, 11 June 2013. http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance (accessed 22 May 2016).

Gridl, Rudolf. *Datenschutz in globalen Telekommunikationssystemen.* Baden-Baden, Germany: Nomos Verlagsgesellschaft, 1999.

Gutiérrez, Horacio E. and Daniel Korn. "Facilitando the Cloud: Data Protection Regulation as a Driver of National Competitiveness in Latin America." *The University of Miami Inter-American Law Review* 45, no. 1 (Fall 2013): 33-61.

"Instructions for Self-Certified Organizations on the Use of the U.S.-EU Safe Harbor Framework Certification Mark." Export.gov. http://www.export.gov/safeharbor/eu/eg_main_018362.asp (accessed 9 May 2016).

Kotzur, Markus. "Datenschutz als Menschenrecht?" *Zeitschift für Rechtspolitik* 46, no. 7 (2013): 216-217.

Kobrin, Stephen J. and Steve Kobrin. "Safe Harbors are Hard to Find: The Transatlantic Data Privacy Dispute, Territorial Jurisdiction and Global Governance." *Review of International Studies* 30, no. 1 (January 2004): 111-131.

Kornbluh, Karin. "The Implications of the Safe Harbor Decision." Net Politics Blog, Council of Foreign Relations, entry posted 7 October 2015. http://blogs.cfr.org/cyber/2015/10/07/the-implications-of-the-european-safe-harbor-decision (accessed 23 May 2016).

Kuner, Christopher. "Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future." *OECD Digital Economy Papers*, No. 187. http://dx.doi.org/10.1787/5kg0s2fk315f-en (accessed 16 May 2016).

_____. *Transborder Data Flows and Data Privacy Law.* Oxford, UK: Oxford University Press, 2013.

_____. "The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law." *BNA Bloomberg, Privacy & Security Law Report, PVLR* 11, no. 6 (6 February 2012).

Kuner, Christopher, Cédric Burton, and Anna Pateraki. "The Proposed EU Data Protection Regulation Two Years Later." *BNA Bloomberg, Privacy & Security Law Report, PVLR* 13, no. 8 (6 January 2014).

Kuner, Christopher, et al. "The (data privacy) law hasn't even checked in when technology takes off." *International Data Privacy Law* 4, no. 3 (2014): 175-176.

Lehofer, Hans Peter. "EuGH: Google muss doch vergessen – das Supergrundrecht auf Datenschutz und die Bowdlerisierung des Internets." E-Comm, entry posted 13 May 2014. http://blog.lehofer.at/2014/05/eugh-google-muss-doch-vergessen-das.html (accessed 18 May 2016).

Masing, Johannes. "Vorläufige Einschätzung der „Google-Entscheidung "des EuGH." Verfassungsblog, entry posted 14 August 2014. http://verfassungsblog.de/ribverfg-masing-vorlaeufige-einschaetzung-der-google-entscheidung-des-eugh (accessed 16 May 2016).

Merati-Kashani, Jasmin. *Der Datenschutz in E-Commerce: die rechtliche Bewertung der Erstellung von Nutzerprofilen durch Cookies,* Munich, Germany: Verlag C.H. Beck oHG, 2005.

Mortera-Martinez, Camino and Rem Korteweg. "Adrift: The impact of the ECJ's Safe Harbour ruling." *Centre for European Reform Bulletin* (November 2015). https://www.cer.org.uk/sites/default/files/bulletin_105_cmm_rk_article2.pdf (accessed 23 May 2016).

Roßnagel, Alexander and Maxi Nebel. "Policy Paper: Die neue Datenschutzgrundverordnung: Ist das Datenschutzrecht nun für heutige Herausforderungen gerüstet?" *Forum Privatheit und Selbstbestimmtes Leben in der digitalen Welt.* Karlsruhe, Germany: Frauenhofer Institut für System- und Innovationsforschüng (ISI), 2016.

"OECD Issues Updated Privacy Guidelines." *Privacy & Information Security Law Blog*, entry posted 16 September 2013. https://www.huntonprivacyblog.com/2013/09/16/oecd-issues-updated-privacy-guidelines (accessed 9 May 2016).

Petri, Thomas. "Die Safe-Harbor-Entscheidung: Erste Anmerkungen." *Datenschutz und Datensicherheit* 39, no. 12 (November 2015): 801-805.

Powles, Julia. "Google's data leak reveals flaws in making it judge and jury over our rights." *The Guardian*, 14 July 2015. https://www.theguardian.com/technology/2015/jul/14/googles-data-leak-right-to-be-forgotten (accessed 29 May 2016).

Powles, Julia and Sylvia Tippmann. "Google accidentally reveals data on 'right to be forgotten' requests." *The Guardian,* 14 July 2015. https://www.theguardian.com/technology/2015/jul/14/google-

accidentally-reveals-right-to-be-forgotten-requests (accessed 29 May 2016).

Pozen, David E. "Privacy-Privacy Tradeoffs." *The University of Chicago Law Review* 83, no.1 (2016): 221-247.

Princen, Sebastiaan. "Trading up in the Transatlantic Relationship." *Journal of Public Policy* 24, no. 1 (2004): 127-144.

Qualman, Erik. *Socialnomics: How Social Media Transforms the Way We Live and Do Business*. Hoboken, New Jersey: John Wiley & Sons, 2011.

Raynes-Goldie, Katherine Sarah. "Privacy in the Age of Facebook: Discourse, Architecture, Consequences." PhD diss., Curtin University, 2012.

"Recent Cases: Internet Law – Protection of Personal Data – Court of Justice of the European Union Creates Presumption that Google Must Remove Links to Personal Data upon Request – Case C-131/12, *Google Spain SL v. Agencia Española de Protección de Datos* (May 13, 2014)." *Harvard Law Review* 128, no. 2 (December 2014): 735-742.

Reidenberg, Joel R. "E-Commerce and Trans-Atlantic Privacy." *Houston Law Review* 38, no. 3 (2001): 717-749.

_____. "Resolving Conflicting International Data Privacy Rules in Cyberspace." *Stanford Law Review* 52, no. 5 "Symposium: Cyberspace and Privacy: A New Legal Paradigm?" (May 2000): 1315-1371.

Rosen, Jeffrey. "The Right to Be Forgotten." *Stanford Law Review Online* 64 (2012): 88-92. http://www.stanfordlawreview.org/sites/default/files/online/topics/64-SLRO-88.pdf (accessed 29 May 2016).

"Safe-Harbor-Ersatz: EU und USA einig über neue Regeln für Datenaustausch," *Der Spiegel Online,* 2 February 2016. http://www.spiegel.de/netzwelt/netzpolitik/safe-harbor-ersatz-eu-und-usa-beschliessen-neue-regeln-a-1075304.html (accessed 23 May 2016).

Simpson, Aaron P. and Lisa J. Sotto. "United States." In *Data Protection & Privacy 2014*. London, UK: Law Business Research Ltd, 2013.

Schwartz, Paul M. “The EU-US Privacy Collision: A Turn to Institutions and Procedures.” *Harvard Law Review* 126, no. 7 (2013): 1966-2009.

_____. “Property, Privacy, and Personal Data.” *Harvard Law Review* 117, no. 7 (May 2004): 2056-2128.

Schwartz, Paul M. and Daniel J. Solove. “Reconciling Personal Information in the United States and European Union.” *California Law Review* 102, no. 4 (April 2014): 877-916.

Siemen, Birte. *Datenschutz als europäisches Grundrecht*. Berlin, Germany: Dunker & Humblot GmbH, 2006.

Victor, Jacob M. “The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy.” *Yale Law Journal* 123, no. 2 (November 2013): 513-529.

“The Zettabyte Era – Trends and Analysis.” Cisco, entry posted 23 June 2015. http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/VNI_Hyperconnectivity_WP.html (accessed 29 May 2016).

Tranberg, Charlotte Bagger. “Proportionality and data protection in the case law of the European Court of Justice.” *International Data Privacy Law* 1, no. 4 (2011): 239-248.

“U.S.-EU ‘Safe Harbor’ Data Privacy Arrangement.” *The American Journal of International Law* 95, no.1 (January 2001): 156-159.

Weber, Rolf H. “Transborder data transfers: concepts, regulatory approaches and new legislative initiatives.” *International Data Privacy Law* 3, no. 2 (2013): 117-130.

Whitman, James Q. “The Two Western Cultures of Privacy: Dignity versus Liberty.” Faculty Scholarship Series, Paper 649 (2009): 1151-1221. http://digitalcommons.law.yale.edu/fss_papers/649 (accessed 15 May 2016).