# EU PRIVACY PROTECTION: A STEP TOWARDS GLOBAL PRIVACY

*Edward R. Alo*[1]



---

1. The author at the time of writing was a second-year law student at Michigan State University College of Law. The author has a B.S. in Education and a B.A. in History with concentrations on United States history and Western European History. The author is also a certified Social Studies teacher in the Commonwealth of Pennsylvania and can teach among others history and economics.

## I. INTRODUCTION

The Internet has provided the world with wondrous benefits, allowing the free flow of information to anywhere in the world that has access to it, while contributing to the growth of the global economy by allowing the consumer to purchase items from all over the world. However, with these great benefits, the Internet does have a serious drawback, online privacy problems. Limiting the privacy issues solely to the Internet is an incredibly narrow definition because the problem generally occurs with the uncontrolled proliferation of information,[2] but for the purpose of this note, privacy issues are strictly limited to online. Uncontrolled proliferation has occurred numerous times in Western history with the invention of the printing press, radio, and television just to name a few. With these proliferation issues, government typically steps in to protect its citizens/subjects and itself. This is true of the European Union and its privacy policy.

In 1995, the European Union instituted the EU Data Protection Directive (Privacy Directive), requiring complete member compliance by 1998.[3] Generally, the Privacy Directive prevents the transmission of personal data to non-EU member countries without adequate protection levels of personal information.[4] The standard imposed by, and noncompliance with, the Privacy Directive threatened to disrupt and possibly prevent United States businesses from operating in the European Member countries, potentially igniting a trade war between two

---

2. *See* David Banisar & Simon Davies, *Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Law and Developments,* 18 J. MARSHALL J. COMPUTER & INFO. L. 1, 4 (1999-2000).

3. *Id.* at 12; Robert M. Gellman, *Can Privacy be Regulation Effectively on a National Level - Thoughts on the Possible Need for International Privacy Rules,* 41 VILL. L. REV. 129, 156 (1996). Integration and adoption was substantially slow. By October 1999, "only six of the fifteen Member States had fully implemented [the Privacy Directive]." Andrew Charlesworth, *Clash of the Data Titans? US and EU Data Privacy Regulation,* 6 EUR. PUB. L. 253, 258 (2000).

4. Gellman, *supra* note 3, at 157.

global powers.[5] However, this threat was alleviated with the negotiation of the Safe Harbor Agreement between the United States Department of Commerce and the European Commission.[6] While the Safe Harbor Agreement continued the trade between EU member countries and U.S. businesses, the Safe Harbor Agreement is just a bandage, and the Privacy Directive will spark change in the United States and other countries' privacy protection to provide protections similar to the conditions in the Privacy Directive.

Americans do not give a second thought when they purchase something from eBay, Amazon, bestbuy.com (the list goes on). Americans pay and receive the product, but what happens to the information they give the companies, such as their name, shipping address, billing address, etc? When people make online purchases or increase their digital presence through social networks, like Facebook, Twitter, or creating a Google account, they voluntarily give the companies personal information, and companies use this information for the companies' benefit. Europeans, on the other hand, will question the necessity of obtaining the same information because privacy protection has developed as a part of the European culture.[7]

However, the businesses are not limited to acquiring information from people voluntarily through purchases and services. The advancements in technology have made collecting,

---

5. *See id*. at 158; Barbara Crutchfield George et al., *U.S. Multinational Employers: Navigating Through the "Safe Harbor" Principles to Comply with the EU Data Privacy Directive*, 7 AM. BUS. L.J. 735, 738-39 (2001).

6. Lauren B. Movius & Nathalie Krup, *U.S. and EU Privacy Policy: Comparison of Regulatory Approaches*, 3 INT'L J. COMM. 167, 173 (2009).

7. *See* George et al., *supra* note 5, at 744-45; Eric Dash, *Europe Zips Lips; U.S. Sells ZIPs*, N.Y. TIMES, (August 7, 2005), http://www.nytimes.com/2005/08/07/weekinreview/07dash.html?pagewanted =print&_r=0; Fred Norman, *Example: US versus EU Internet Privacy Policy*, UNIV. OF TEX., http://www.laits.utexas.edu/~anorman/61N/Text /Information%20Policy/US-Eu.html (last visited Jan. 1, 2013).

storing, and processing information easier and cheaper.[8] To utilize customers' tendencies on the Internet, businesses also use cookies.[9] These cookies can be placed in the computer by just visiting a website.[10] Once programmed in the computer, the cookies allow businesses to track the user's web surfing and collect personal information from the user.[11] Cookies are very different from voluntary information because the cookies only track users' online behavior and do not collect information such as names, addresses, etc.[12] The companies retain and process the information to a usable format and sometimes sell the information to other businesses or collection companies that amass a large database to sell to interested companies; transactions that total in the billions, potentially trillions annually.[13] Typically, businesses will use this collected information to target customers to purchase specific products,[14] which might go through the SPAM filter. The information can be used to give a recommendation of similar products on the home page.[15] For example, the Google method uses targeted

---

8. Testimony on Online Privacy Concerns of 2001: Before the Subcomm. on Commc'n, Trade and Consumer Prot., 107th Cong. (2001) (statement of Paul H. Rubin, Professor of Law and Economics, Emory University) [hereinafter Privacy Concerns].

9. Rebecca Lynch, *What's All the Fuss About?*, CIO MAGAZINE (Nov. 17, 2000), http://www.cio.com.au/article/75438/what_all_fuss_about/.

10. *Id*.

11. *Id*.

12. *Id*.

13. Gregory Shaffer, *Globalization and Social Protections: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1, 18 (2000).

14. *See* Angela Vitale, *The EU Privacy Directive and the Resulting Safe Harbor: The Negative Effects on U.S. Legislation Concerning Privacy on the Internet*, 35 VAND. J. TRANSNAT'L L. 321, 325 (2000); Privacy Concerns, *supra* note 8.

15. Amanda C. Border, *Untangling the Web: An Argument for Comprehensive Data Privacy Legislation in the United States*, 35 SUFFOLK TRANSNAT'L L. REV. 363 (2012); *U.S. Firms Get Privacy Lessons from Europe*, BLOOMBERG BUSINESSWEEK, (July 1, 2010) [hereinafter *Privacy Lessons from Europe*], *available at* http://www.businessweek.com/globalbiz/content/jul2010/gb2010071_033299.htm.

advertisements based on the content of your emails and content from other Google services.[16] Regardless, how the businesses use the personal information, it is typically for the company's economic benefit.

Although Americans may find the SPAM annoying, many Americans likely do not care and ignore the emails, but the information sharing that makes SPAM possible also provides benefits to the consumer, such as lower prices for products because the companies do not spend as much money for advertising by targeting the customers.[17] However, the same cannot be said about the citizens of the European Union Member States. The Privacy Directive established that EU citizens have more control over their individual information processed by businesses. Under the Privacy Directive, businesses can operate similar to how they do in the United States, but the businesses have to "jump through some hoops," which I will discuss later.[18] This does not mean that the United States is completely deficient in privacy protection. In fact, the Supreme Court has interpreted privacy protection in the Bill of Rights, notably the Fourth Amendment, and supplemented by acts of Congress and state legislation.[19]

---

16. Chris Crum, *Europe Isn't Satisfied with Google's Privacy Policy. Are You?*, WEBPRONEWS, (Oct. 16, 2012), http://www.webpronews.com/europe-isnt-satisfied-with-googles-privacy-policy-are-you-2012-10; *Privacy Lessons from Europe*, *supra* note 15; Sunni Yuen, *Exporting Truth With Data: Audited Self-Regulation as a Solution to Cross-Border Data Transfer Protection Concerns in the Offshore Outsourcing Industry*, 9 COLUM. SCI. & TECH. L. REV. 41, 44 (2008).

17. *See generally* Vitale, *supra* note 14, at 325-26; Marc Brailor, *AeA Unveils Federal Privacy Principles; Says Balanced Approach, Uniform Standards, Can Build Consumer Confidence, Boost Internet Growth*, AEANET.ORG, (Jan. 18, 2001), http:www.aeanet.org/pressroom/prêt-privacyprinciples011801.asp; Matthew S. Kirsch, *Do-Not-Track: Revising the EU's Data Protection Framework to Require Meaningful Content for Behavioral Adverting*, 18 RICH. J. L. TECH. 1, 1-3 (2011-2012).

18. *See* discussion *infra* sec. II pts (B)-(C).

19. *See* Banisar & Davies, *supra* note 2, at 18; Charlesworth, *supra* note 3, at 259.

This note will consider numerous issues involving the Privacy Directive. Part II will examine the details and impact of compliance with the Privacy Directive as well as how the United States has complied and conflicted with the Directive, including compliance through the Safe Harbor Agreement. Part II will also consider the different approach to privacy protection between the U.S. and EU and how the different cultures developed the different approaches. Part III will explain the changes in privacy protection in the proposed EU Data Regulation, including the potential costs and benefits from proposed changes, while analyzing the potential effects of the EU Data Regulation on the Safe Harbor Agreement. Part III will conclude the Data Regulation will have relatively little effect on the Safe Harbor Agreement. Part IV will weigh the market effect of the European Union and the conflict of laws between the U.S. and EU. Finally, this note will consider and conclude the Privacy Directive, Data Regulation, and U.S. compliance are steps towards creating an international privacy regulation.

## II. UNITED STATES VERSUS THE EUROPEAN UNION

Privacy means different things to people in different contexts and situations and to pinpoint one definition is difficult, if not impossible.[20] For the purpose of this note, privacy is the ability to control one's personal information. In addition, for the purpose of this note privacy protection does not mean prevention of hacking and identity theft, but rather the methods used to give people dominion over their personal information. Privacy protection does, however, have positive correlations to limit hacking and identity theft because the businesses provide more advanced data security.[21] To provide the necessary privacy

20. Lawrence Jenab, *Will the Cookie Crumble?: An Analysis of Internet Privacy Regulatory Schemes Proposed in the 106th Congress*, 49 U. KAN. L. REV. 641, 647 (2001).

21. *See generally* Person Data Privacy and Security Act of 2005, S. 1789, 109th Cong. (2005) (concerning increased privacy protection to assist victims and potential victims of identity theft).

protections in the Age of Information, governments have taken different approaches, but the most notable are the ones taken by the US and the EU.

### A. The United States Approach to Privacy Protection

While some countries and states consider privacy explicitly in their constitutions, the United States Supreme Court has only found privacy implicitly in the Bill of Rights.[22] However, the protection implied by the Court has only been held against the government and only when a citizen had a "reasonable expectation of privacy."[23] This limitation against the government stemmed from a historic fear of government collection and use of information against the people.[24] Similar to the European Union's progressive privacy protection with the advances in technology, the Court has also advanced protections with new technology. Most notably in *Katz v. United States*, the Court held the use of an electronic listening device within a phone booth was a violation of the Fourth Amendment because there was a "reasonable expectation of privacy."[25] Over 30 years later, the Court, in *Kyllo v. United States*, held that using a thermal imager was a search and violated the Fourth Amendment.[26] Even if these privacy protections did not only apply to the federal and state governments, once the person voluntarily discloses information to any company, there is no "expectation of

22. Banisar & Davies, *supra* note 2, at 108.
23. *Id.*
24. *See* Dash, *supra* note 7.
25. Katz v. United States, 389 U.S. 347, 360 (1967) (J. Harlan, concurring). The Court incorporated and continues to incorporate the language in Justice Harlan's concurrence in cases involving Fourth Amendment searches. *See generally* United States v. Karo, 468 U.S. 705 (1984); *see also* Florida v. Jardines, 133 S.Ct. 1409 (2013).
26. Kyllo v. United States, 533 U.S. 27, 40 (2001) (The Court focused on the theory that the thermal imager gave the user "intimate details" of the home. Id. The home has typically received higher protection in privacy jurisprudence. *Id.* at 37).

privacy[,]"unless the privacy policy explicitly provides protection to the data subject.[27]

There are civil protections for privacy, but the protections are generally limited to the "right to be let alone"[28] established through common law privacy torts.[29] Sometimes, a website has privacy policies and a potential breach of contract claim if the business transfers the personal information to a third party.[30] There is also a potential intellectual property claim. Scholars also argue that personal information should be treated as an intellectual property right[31] because the right creates private control over public commercial information.[32] However, this view creates a First Amendment issue. Courts have generally held the information as protected commercial free speech allowing the businesses to transfer the information.[33] Under the United States' approach, the courts attempt to balance the individual's desire to maintain his personal information and society's use of the information.[34]

---

27. Marie Clear, *Falling Into the Gap: The European Union's Data Protection Act and Its Impact on U.S Law and Commerce*, 18 J. MARSHALL J. COMPUTER & INFO. L. 981, 995 (2000).

28. Charlesworth, *supra* note 3, at 259.

29. RESTATEMENT (SECOND) OF TORTS § 652A(2) (1977). The common law privacy torts includes (1) unreasonable intrusion on the privacy of another; (2) use of another's name or likeness; and (3) unreasonable publicizing another's private life. *Id*.

30. *See* Lauren B. Cardonsky, *Towards a Meaningful Right to Privacy in the United Kingdom*, 20 B.U. INT'L L.J. 393, 396 (2002); George et al., *supra* note 5, at 780.

31. Steven Hetcher, *The FTC as Internet Privacy Norm Entrepreneur*, 53 VAND. L. REV. 2041, 2042 (2000).

32. Rochell Cooper Dreyfuss, *Warren and Brandeis Redux: Finding (More) Privacy Protection in Intellectual Property Lore*, 1999 STAN. TECH. L. REV. 8, ¶ 4 (1999).

33. *See id*. ¶ 25. (citing Bonito Boats, Inc. v. Thunder Craft Boats, Inc., 489 U.S. 141 (1989); Compco Corp. v. Day Bright Lighting, Inc., 376 U.S. 234 (1964); Sears, Roebuck & Co. v. Stiffel Co., 376 U.S. 225 (1964)).

34. David A. Castor, *Treading Water in the Data Privacy Age: An Analysis of Safe Harbor's First Year*, 12 IND. INT'L & COMP. L. REV. 265, 271 (2001-2002); *see also* Jonathan P. Cody, *Protecting Privacy Over the*

In addition to constitutional and common law applications, Congress has provided a patchwork of statutes to give privacy protection, but the statutes are limited to specific industries and sectors listed by statute. The examples of Congressional statutory protections include the Fair Credit Reporting Act,[35] Gramm-Leach-Bliley Act,[36] Health Insurance Portability and Accountability Act,[37] and the Privacy Act of 1974,[38] to name a few. The industries and sectors that are not regulated by statute are encouraged by the government to self-regulate the private data they receive.[39] The self-regulation method allows the industries to develop standards without government intervention. This laissez-faire, "hands off" approach by the government is a historical approach traditionally taken by the federal government.[40] There is still government oversight of the self-regulatory approach through the Federal Trade Commission (FTC), but the FTC only has limited power to enforce what the companies have adopted, instead of requiring the companies to adopt policies.[41] The self-regulatory approach still continues even under the Privacy Directive.[42]

---

*Internet: Has the Time Come to Abandon Self-Regulation?*, 48 CATH. U. L. REV. 1183, 1197 (1999).

35. Fair Credit Reporting Act, 15 U.S.C. § 1681 (1994 & Supp. 1998) (regulating crediting reporting agencies and employment related data).

36. Gramm-Leach-Bliley Financial Modernization Act, Pub. L. No. 106-012, 113 Stat. 1338 (1999) (regulating data processing practices of financial institutions).

37. Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 100 Stat. 1936 (1996) (regulating data collected by health care institutions).

38. Privacy Act of 1974, 5 U.S.C. § 552(a). While the government is limited in how information is collected, the Privacy Act of 1974 governs the government's use and dissemination of personal information. Border, *supra* note 15, at 366.

39. Cody, *supra* note 34, at 1203.

40. *Id.*

41. Laura Ybarra, *The E.U. Model as an Adoptable Approach for U.S. Privacy Laws: A Comparative Analysis of Data Collection Laws in the United Kingdom, Germany, and the United States*, 34 LOY. L.A. INT'L & COMP. L. REV. 267, 272 (2011). Michael D. Scott, *The FTC, The Unfairness Doctrine,*

One piece of legislation passed in 2001 still has a considerable impact on privacy in the United States and privacy interests abroad: the USA PATRIOT Act (Patriot Act).[43] Under the Patriot Act, the federal government has more power to obtain information.[44] The act does not prevent businesses from obtaining information from consumers like the Privacy Directive. However, the Patriot Act allows the federal government to obtain access to businesses' data records to track potential terrorists.[45] The Patriot Act has caused concern under the Privacy Directive and is an issue that the note will address later.[46]

B. The European Union's approach

In Europe, privacy is a fundamental human right.[47] In 1995, the European Council of Ministers enacted the EU Data Protection Directive.[48] To understand how the Privacy Directive applies, it is fundamental to understand the composition and function of the European Union. First, there are three major branches: the European Commission, which recommends policy; the European Council of Ministers, which passes the policies; and the European Court of Justice, which hears violations of, interprets, and applies the European Union's law.[49] Think of the European Union government as similar to the United States

---

*and Data Security Breach Litigation: Has the Commission Gone Too Far?*, 60 ADMIN. L. REV. 127, 128-29 (2008).

42. *See* discussion *infra* Sec. II.C.

43. *See generally* USA PATRIOT ACT of 2001, Pub. L. No. 107–56, 115 Stat. 272 (codified in scattered sections of 5, 8, 10, 12, 15, 18, 20, 21, 22, 28, 31, 42, 47, 49, 50 U.S.C.).

44. *See generally id*.

45. *See generally id*.

46. *See* discussion, *infra* Sec IV.B.

47. Fred H. Crate, *The EU Data Protection Directive, Information Privacy, and the Public Interest*, 80 IOWA L. REV. 431, 432-33 (1994-95), *available at* http://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1647&context=facpub.

48. *Id.* at 432-33.

49. Clear, *supra* note 27, at 982.

government; there are three branches and they all pass preempting laws affecting its members, who also have sovereign authority.[50] However, the European Union also contains numerous associations, commissions, committees, and councils in addition to the three bodies named above.[51]

When the European Union adopted the Privacy Directive, it intended the directive to create uniform rules and privacy standards among the member countries.[52] Before the Privacy Directive, the member countries' privacy standards were scattered. The European Union used the Privacy Directive to further the European Union's purpose, which was to create and maintain a unified market and free flow of information among the member states, which is self-evident from the language of the Privacy Directive.[53]

The Privacy Directive begins by acknowledging that privacy protection is a fundamental human right with the purpose of allowing the free flow of information between Member States.[54] Under Article 3, the Privacy Directive identifies the scope as "the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system."[55] However, the Privacy Directive excludes from the scope any "processing operations concerning public security, defen[s]e, [national] security. . . and

50. Currently, the European Union has 27 countries, including Austria, Belgium, Bulgaria, Cyprus, Czech Republic, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherland, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and the United Kingdom. However, only 15 of the 27 were member states at the time of adopting the Privacy Directive. *See Countries*, EUROPEAN UNION, http://europa.eu/about-eu/countries/index_en.htm (last visited Feb. 16, 2013).

51. Clear, *supra* note 27, at 982.

52. *See id*.

53. Dash, *supra* note 7; Shaffer, *supra* note 13, at 10-11.

54. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, art. 1(1), 1990 O.J. (L 281) 31, 38 [hereinafter Privacy Directive].

55. *Id*. art. 3(1).

the activities of the State in areas of criminal law" and "by a natural person in the course of a purely personal or household activity."[56] Article 2 defines personal data as "any information relating to an identified or identifiable natural person ('data subject');[57] . . . by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."[58] Also, Article 2 defines processing as "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction."[59] When the Article 2 definitions are combined with the scope from Article 3, the Privacy Directive creates a broad scope for enforcement for an inclusive range of interpretation and for the Privacy Directive to have a continued effect with advances in technology beyond the European Union's initial vision.[60]

Furthermore, Article 4 addresses the structure and process to obtain information from the "data subject." Article 4 places minimum requirements on businesses. First, the businesses will

---

56. Id. art. 3(2).

57. A data subject is an identified or identifiable natural person. *Id*. art. 2(a). "Natural person in the course of a purely personal or household activity" is a narrow exception to the scope of the Privacy Directive. *Id*. art. 3(2). This exception likely exists because 1) it is difficult to enforce against an individual person, 2) there is no threat of mass proliferation for profit from individuals using the information for personal reasons, 3) it provides a balance between compelling individual interests and the free flow of information.

58. A data subject is an identified or identifiable natural person. *Id*. art. 2(a). "Natural person in the course of a purely personal or household activity" is a narrow exception to the scope of the Privacy Directive. *Id*. art. 3(2). This exception likely exists because 1) it is difficult to enforce against an individual person, 2) there is no threat of mass proliferation for profit from individuals using the information for personal reasons, 3) it provides a balance between compelling individual interests and the free flow of information.

59. Privacy Directive, *supra* note 54, art. 2(b).

60. *See* George et al., *supra* note 5, at 753.

have a *data controller*, the person who is personally responsible for how the personal data will be processed within the specific business.[61] The controller also has the responsibility to contact a "supervisory authority" in the Member State before processing.[62] The supervisory authority is an independent authority established by the Member State to monitor that the Privacy Directive is "implemented into national law."[63] However, the supervisory authority has significant powers; it can "block the transmittal of data, ban the processing of data, or destroy data processed in violation of the law."[64] This authority is also responsible to ensure that the data quality principles, listed in Article 6, are met.[65]

Article 6 provides that the Member State, through the controller, must ensure personal data is:

> (a) processed fairly and lawfully;
>
> (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;
>
> (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
>
> (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are

---

61. Privacy Directive, *supra* note 54, art. 6(2) (emphasis added); George et al., *supra* note 5, at 753.

62. Privacy Directive, *supra* note 54, art. 18(1); George et al., *supra* note 5, at 753-54.

63. Privacy Directive, *supra* note 54, art. 18; George et al., *supra* note 5, at 754.

64. Privacy Directive, *supra* note 54, art. 28(3); George et al., *supra* note 5, at 754.

65. Privacy Directive, *supra* note 54, art. 28(2); George et al., *supra* note 5, at 754.

> inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
>
> (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.[66]

Generally, the requirements given to the controllers reflect four general obligations: data quality, security, notification, and how to complete processing.[67]

Article 7 provides a complete bar toward processing personal information.[68] However, Article 7 explains that personal data may only be processed if the business meets one of the Privacy Directive exceptions.[69] Article 7 exceptions state:

> (a) the data subject has unambiguously given his consent; or
>
> (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
>
> (c) processing is necessary for compliance with a legal obligation to which the controller is subject; or
>
> (d) processing is necessary in order to protect the vital interests of the data subject; or
>
> (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official

66. Privacy Directive, *supra* note 54, art. 6.
67. *Id*. pmbl. para. 25.
68. *Id.* art. 7.
69. *Id.*

> authority vested in the controller or in a third party to whom the data are disclosed; or
>
> (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).[70]

In addition to the prohibition in Article 7, Article 8 also provides for a complete prohibition to "processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life,"[71] also known as "sensitive information." Similar to Article 7, Article 8 also allows processing if "the data subject has given his explicit consent," but a Member State is allowed to provide a complete ban without exception.[72]

Articles 10, 11, and 12 refer to the data subject's right to certain information. These articles include the information that must be given to the data subject before processing - such as the identity of the controller, the purpose for the processing, and the identity of the third party transfers.[73] Most importantly, the articles provide the data subject with the right to access his or her information, as the data subject must be given the ability to edit and modify the information and keep the information correct.[74]

Finally, Article 25 and 26 are the most important articles when determining the effect of the Privacy Directive and the Safe Harbor Agreement. Article 25 is a complete prohibition against transfers of personal data to "third countries" (any country that is not a member of the European Union). However, Article 25 does permit transfers of personal data to third

70. *Id.*
71. *Id*. art. 8.
72. *Id.*
73. *See id*. art. 10-12.
74. *Id*.

countries if "the third country in question ensures an *adequate level of protection*."[75] Article 26 provides other exceptions than an "adequate level of protection," such as unambiguous consent from the data subject or the transfer is necessary to complete a contract with the data subject.[76] However, the European Union Commission added to the Article 26 exception by providing Standard Contractual Clauses.[77] The standard form contract clauses provide the protection standard required by the Privacy Directive that can be negotiated into individual contracts and relied upon for supervisory authority approval in all member countries.[78] The European Union Commission did not limit itself to the standard contract clauses or the exceptions provided in the Privacy Directive, the Commission negotiated and approved the Safe Harbor Agreement to provide a guaranty of "adequate protection" to companies in the United States.[79]

### C. European Union-United States Safe Harbor Agreement

When the European Union adopted the Privacy Directive, the United States could not meet the "adequate protection" standards. As a result of the Privacy Directive, United States businesses were faced with the potential loss of billions of dollars in annual transactions[80] and a potential trade war between the two economic powers.[81] Therefore, the United States Department of Commerce and the European Commission began an agreement to continue business between the countries. After

---

75. *Id*. art. 25 (emphasis added). The European Commission determines if the third country meets the adequate protection requirement. *Id*.

76. *Id*. art. 26.

77. *Id*.; *see generally* Commission Decision 2002/16/EC of 27 December 2001 on Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries, Under Directive 95/46/EC, 2002 O.J. (L 6) 52 [hereinafter Model Contracts].

78. Model Contracts, *supra* note 77, at 53; Privacy Directive, *supra* note 54, art. 26(4).

79. Charlesworth, *supra* note 3, at 265.

80. Shaffer, *supra* note 13, at 18.

81. George et al., *supra* note 5, at 738-39.

two years of negotiations, the European Union and the Department of Commerce settled for an agreement that enacted the European Union's interest in the Privacy Directive protection requirement without requiring a wholesale change in the United States' self- regulation approach.[82] In July 2000, the European Union announced the acceptance of the Safe Harbor Agreement.[83] Two very important elements of the Safe Harbor Agreement are 1) the Safe Harbor Agreement establishes the presumption of "adequate level of protection"[84] and 2) the Safe Harbor Agreement is voluntary.[85] If a business decided to enroll in the Safe Harbor Agreement, the business must comply with the principles and procedure set forth in the Safe Harbor Agreement.[86] First, to enroll in the Safe Harbor Agreement, the business must self- certify annually to the Department of Commerce that they will follow the principles in the Agreement and declare its adherence to the Agreement publicly.[87] By joining TRUSTe and/or BBBOnline, independent consumer watch/rating organizations specifically for online businesses, United States companies can fulfill the self-certifying requirement.[88] Under the compliance requirements, the

82. *See Safe Harbor Privacy Principles*, EXPORT.GOV, http://export.gov/safeharbor/eu/eg_main_018475.asp (last visited Mar. 20, 2013).

83. *U.S.-EU Safe Harbor Overview*, EXPORT.GOV, http://export.gov/safeharbor/eu/eg_main_018475.asp (last visited Mar. 20, 2013). *Id.* The Safe Harbor Agreement began November 1, 2000 and has been in place since. *Id.* In addition, the Safe Harbor Agreement is unique because other countries such as Canada must still adopt "adequate privacy protection" and cannot take the benefits of the Safe Harbor Agreement. *See* DOROTHEE HEISENBERG, NEGOTIATING PRIVACY—THE EUROPEAN UNION, THE UNITED STATES, AND PERSONAL DATA PROTECTION 103 (2005).

84. George et al., *supra* note 5, at 764-65; *U.S.-EU Safe Harbor Overview*, *supra* note 83.

85. *U.S.-EU Safe Harbor Overview*, *supra* note 83.

86. *See* George et al., *supra* note 5, at 765; *U.S.-EU Safe Harbor Overview*, *supra* note 83.

87. *U.S.-EU Safe Harbor Overview, supra* note 83*;* George et al., *supra* note 5, at 765.

88. *BBB EU Safe Harbor Program*, BBB, http://www.bbb.org/council/eusafeharbor/bbb-eu-safe-harbor-dispute-resolution-program/ (last visited Mar. 30, 2013); EU Safe Harbor, TRUSTE, http://www.truste.com/

businesses create a privacy policy[89] that abides by the seven principles: notice, which acknowledges the purpose of processing;[90] choice, which allows the data subject to "opt out" or "opt in;"[91] onward transfer, which provides the data subject with the same protection if a third party misuses the information;[92] technical security, which protects the information from "loss, misuse and unauthorized access, disclosure, alteration and destruction;"[93] data integrity, which limits the use of the information relevant to its purpose;[94] access, which provides the data subject the ability to access and amend their personal information;[95] and enforcement, which provides a means of recourse to investigate and resolve with respect to the principles.[96]

However, enforcement is not limited to the dispute resolution procedures provided in the business's privacy policy. The data subject could report the business to the Federal Trade Commission[97] or the European citizen can bring an action in the Member State.[98] The FTC's power is limited as it only has the power to enforce the privacy policies already adopted by the

---

products-and-services/enterprise-privacy/eu-safe-harbor-sea (last visited Mar. 30, 2013). Generally, you can find the TRUSTe and/or BBBonline symbols on the company's website.

89. The policy will also include the contact information for complaints. George et al., *supra* note 5, at 766.

90. *U.S.-EU Safe Harbor Overview*, *supra* note 83.

91. George et al., *supra* note 5, at 767; *U.S.-EU Safe Harbor Overview*, *supra* note 83. The company must provide the data subject with the necessary information. However, the data subject can decide to process the information and the data subject must decide that he or she does not want the personal information processed by opting-out. *Id.* Or, the company could provide that the data subject must go out of his or her way to have the information processed by opting-in. *Id.*

92. *U.S.-EU Safe Harbor Overview*, *supra* note 83.

93. *Id.*

94. *Id.*

95. *Id.*

96. *Id.*

97. *Id.;* George et al., *supra* note 5, at 780.

98. George et. al., *supra* note 5, at 779.

businesses.[99] In addition, the data subjects rarely learn of the violation with his or her personal information, so the data subjects rarely take action on the violation.[100]

This problem is likely further escalated by the different legislation and additional restrictions of the Member States.[101] The Privacy Directive sets a minimum standard and allows for the member countries to apply higher standards as long as the member countries' standards do not restrict the flow of information between the member countries.[102] By complying with the different standards in the different member countries, the businesses may have different standards for the different countries,[103] and a layperson may find it difficult to determine which privacy policy applies to them. Since the Privacy Directive began in 1995, and the Safe Harbor Agreement in 2000, some United States businesses were likely reluctant to join the Safe Harbor Agreement and conduct business in the European Union during the first two years[104] because of the significant commitment of resources.[105] Since 2002, big

---

99. *Id.* at 779-80; Scott, *supra* note 41, at 129.

100. *See* Francoise Gilbert, *European Data Protection 2.0: New Compliance Requirements in Sight – What the Proposed EU Data Protection Regulation Means for U.S. Companies*, 28 SANTA CLARA COMPUTER & HIGH TECH. L.J. 815, 848-49 (2012).

101. *See* Shaffer, *supra* note 13, at 11-12; *Commission Staff Working Paper: Impact Assessment* (Eur. Comm'n, Working Paper No. 25.1.2012 SEC (2012) 72 final 2012), *available at* http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf.

102. Privacy Directive, *supra* note 54, art. 1(2).

103. *See* FRED H. CATE, PRIVACY IN THE INFORMATION AGE 1-4 (1997); LRDP KANTOR LIMITED & CENTRE FOR PUBLIC REFORM, COMPARATIVE STUDY ON DIFFERENT APPROACHES TO NEW PROPERTY CHALLENGES, IN PARTICULAR IN THE LIGHT OF TECHNOLOGICAL DEVELOPMENT 31 (2010).

104. *See* David A. Tallman, *Financial Institutions and the Safe Harbor Agreement: Securing Cross-Border Financial Data Flows*, 34 LAW & POL'Y INT'L BUS. 747, 773 (2003).

105. *See* James M. Assey, Jr. & Demetrios A. Eleftheriou, *The EU-U.S. Privacy Safe Harbor: Smooth Sailing or Troubled Waters?*, 9 COMMLAW CONSPECTUS 145, 156-58 (2001); James A. Harvey & Kimberly A. Verska, *What the European Data Privacy Obligations Mean for U.S. Businesses*, GIGALAW, http://www.gigalaw.com/articles/2001/harvey-

businesses like Microsoft, Apple, and Google[106] have adapted and remained self-certified, sparking a strong interest in the Safe Harbor Agreement with hundreds of companies on the list.[107] The Safe Harbor Agreement, however, has its critics. The critics argue the Safe Harbor Agreement does not follow the purpose of the Privacy Directive because of its difficulty in enforcing the privacy protections intended by the Privacy Directive.[108]

### D. The Privacy Directive Legislation's Compliance by Multinational Corporations

When the European Union passed the Privacy Directive in 1995 and Member States subsequent legislation in 1998, the Privacy Directive forced restrictions and requirements on the companies located within the European Union. However, in the current global economy, companies are not singular entities with one location. Companies develop corporate structures that include subsidiary companies to operate, either independently or dependently, in different countries or regions all over the world. These companies are known as multinational corporations. In the global economy, multinational corporations have data storage all over the world that can be accessed by the controlling company/location or the subsidiaries for efficiency. The transfer of information within the corporate structure shows that the Privacy Directive not only affects the companies that operate within Europe but also the locations and subsidiaries outside of the jurisdiction.

One may think that because one of the locations or subsidiaries in the European Union provides privacy protection under the Privacy Directive that the data may still be accessed by

---

2001-02-pl.html (last visited Mar. 30, 2013); Joseph J. Laferrera, *Implications of the European Union Directive on Data Protection for US Companies*, GESMER UPDEGROVE LLP (Mar. 17, 2005), http://www.gesmer.com/insights.php?NewsID=795.

106. *U.S.-EU Safe Harbor List*, EXPORT.GOV, http://safeharbor.export.gov/list.aspx (last visited Feb. 17, 2013).

107. *See id.*

108. Tallman, *supra* note 104.

other locations of the corporation, permitting the company to run around Article 25 and/or the Safe Harbor Agreement. That is not the case, as each part of the multinational corporation that wants to access the information under the jurisdiction of the European Union must adhere to the Article 25 adequate protection requirement.[109] In addition, the EU location of the multinational corporation must obtain the consent from the data subject under the Privacy Directive and Member State's legislation, unless it is required to perform a contract.[110] The adequate protection standard has frustrated multinational corporations because they cannot access employment records, for example, without consent and adequate protection.[111] However, a multinational corporation is not completely prohibited from access. They could acquire consent through the employment contract or enter the Safe Harbor Program.

### E. Differences between the United States and the European Union approaches

Americans may wonder why the European Union considered the Privacy Directive necessary. The quick answer is that the United States and the EU have different beliefs and approaches to privacy. For example, Europeans believe that privacy is a fundamental right and it is the responsibility of the government to protect privacy, whereas Americans believe that privacy is a commodity that can be traded away for economic benefits.

Americans generally have a "healthy" distrust of the government and a traditional hands-off approach to regulation. The federal government has usually only regulated when there

---

109. Zack Whittaker, *Safe Harbor: Why EU Data Needs 'Protecting' from US Law*, ZDNET (Apr. 25, 2011), http://www.zdnet.com/blog/igeneration/safe-harbor-why-eu-data-needs-protecting-from-us-law/8801; *see also European Data Privacy: Beware of the Pitfalls*, SMITH, GAMBRELL & RUSSELL, LLP, http://www.sgrlaw.com/print/?id=2047 (last visited Jan. 22, 2013).

110. Privacy Directive, *supra* note 54, art. 7(b); Model Contracts, *supra* note 77.

111. George et al., *supra* note 5, at 768-78.

was a need created by the market, and, without a need, trusted the market would regulate itself.[112] Since the Revolutionary era, Americans have feared the government collecting and controlling information about the citizens, considering the British government obtained private information and misused it for public perception and criminal acts.[113] In fact, the Bill of Rights is evidence that Americans feared the collection of information through the British's methods. While some industries over-extend themselves and the government has stepped in and placed restrictions on the industries, the hands-off approach and the reactionary regulation is predominately true for privacy in the United States.

On the other hand in Europe, beginning in the 1970s, Germany passed the first comprehensive privacy protection.[114] When Germany established the privacy protection, the country had in its mind the horrible acts, murders, and torture that resulted from the misuse of information by Hitler's secret police.[115] The government saw privacy as a right, and the right needed to be protected by placing the necessary restrictions on collections resulting from the proliferation of data from the Information Age. The government enforced these restrictions.[116] Once Germany passed a comprehensive privacy protection, other European countries, such as Sweden, passed similar protections.[117] The motivation was possibly due to witnessing the horrible acts resulting from the KGB's collection and misuse of

112. *See generally* Michael Les Benedict, *Laissez-faire and Liberty: A Re-Evaluation of the Meaning and Origins of Laissez-faire Constitutionalism*, 3 LAW & HIST. REV. 293 (1985) (describing the laissez-fair approach, historically taken by the United States).

113. The United States government adopted the Bill of Rights to limit the federal government's power in response British authority before and during the American Revolution. *Alexander Hamilton, Federalist, no. 84, 575--81*, THE FOUNDERS' CONSTITUTION, http://press-pubs.uchicago.edu/founders/documents/bill_of_rightss7.html (last visited Feb. 1, 2014).

114. Dash, *supra* note 7*; see also* Assey & Eleftheriou, *supra* note 105, at 148.

115. *See* George et al., *supra* note 5, at 743; Dash, *supra* note 7.

116. *See* Assey & Eleftheriou, *supra* note 105, at 148.

117. FRED H. CATE, PRIVACY IN THE INFORMATION AGE 32 (1997).

information, due to the economic strength/market power Germany built after World War II, or a combination of both.

## III. EUROPEAN UNION GENERAL DATA REGULATION

On January 25, 2012, the European Commission released its plans to completely reform data protection in the European Union, known as the E.U. General Data Protection Regulation (Data Regulation).[118] It also released the proposed regulation to obtain input for the final regulation that the European Commission plans to adopt by 2015.[119] In many ways the proposed Data Regulation would operate the same way as the Privacy Directive, but the Data Regulation stems from the principle established by the European Union in 2010. In 2010, the European Union clearly specified a desire to "shift to a single law that would be common to all of the Member States."[120] The purpose behind the reform is to place more responsibilities on the companies with the processed data, give more rights to the citizens, and reduce the costs of compliance for the companies.[121]

However, the main purpose is the current fragmentation and incoherence under the Privacy Directive.[122] Currently, when businesses operate in multiple Member States, the businesses must follow each of the Member States' Privacy Directive legislation. Since the Privacy Directive only established a minimum standard for personal data protection and processing, the Member States were able to establish higher standards, which some did. With varying standards, businesses have been forced to comply with the different requirements for each Member State, redundantly performing tasks for each Member State.[123]

---

118. Gilbert, *supra* note 100, at 815.

119. *Id.* at 816.

120. *Id.*

121. *Id.* at 818.

122. *The Proposed General Data Protection Regulation: The Consistency Mechanism Explained*, EUROPEAN COMMISSION (June 2, 2013), http://ec.europa.eu/justice/newsroom/data-protection/news/130206_en.htm [hereinafter Regulation Explained].

123. *See generally id.*

The European Commission sought to remove those barriers by establishing one unified regulation for businesses and one application by the European Data Protection Board, with some discretion remaining for the European Commission.[124]

When the European Commission revealed the Data Regulation, it also revealed the Police and Criminal Justice Data Protection Directive.[125] The Police and Criminal Justice Data Protection Directive would apply like the Privacy Directive and the Member States would follow the guidelines set by the Directive when establishing the Member States' legislation.[126] Under this new E.U. Criminal Data Protection Directive, the Member States would develop legislation that would allow data collection and processing by the authorities for preventing, investigating, detecting, or prosecuting criminal offenses and the free movement of data.[127] The E.U. Criminal Data Protection Directive is also opened for changes to the final version.[128] While the European Commission revealed both documents as a part of a plan, this note will only consider the Data Regulation in detail.

### A. Developing the Data Regulation

Since the European Union approved the Privacy Directive in 1995, the organization has modified its operation, as it previously operated like a confederation, with relatively limited power.[129] However, in December 2009, the Member States ratified the Lisbon Treaty[130] and established a streamlined

---

124. *Id.*
125. Gilbert, *supra* note 100, at 820.
126. *Id* at 816-17.
127. *Id.* at 820.
128. *Id.* at 820-21.
129. *See id.* at 821-22.
130. The European Union, after the Treaty of Lisbon, with its structure and day-to-day function, appears similar to the United States. Like the United States, the European Union has three branches with committees and other subdivision that could be compared to the United States' administrative agencies. The European Union also is the single representative of all of the Member State for the areas that the European

process so the 27 Member States could operate as one unified body under the European Union,[131] similar to the United States' development of a centralized federal government in the 1780s. Under the ratified treaty, the Member States established a bicameral legislature with the Council of Ministers, known as the European Parliament, and established a long term President of the European Council, an executive figure.[132] Almost a year after ratification of the European Union's new power, the European Officials announced their intent to reform the data protection.[133]

Although the European Union revealed a new document, with a different title and different effect on the Member States, the Data Regulation does not substantially differ from policies adopted in the Privacy Directive.[134] In fact, the 119-page Data Regulation possibly provides a more detailed protection of personal data and provides more protection to the data subject among other things.[135] However, due to the substantial similarities between the Privacy Directive and the Data Regulation, this note will focus on the provisions of the Data Regulation that differ, the effect from those differences, and the essential provisions for enforcement.

---

Union has the power to regulate or adopt policy in; essentially like the state governments in the United States, the Member States maintain their own governmental system. However, unlike the states that compose the United States, the Member State are seen as an individual entity in foreign affairs and can adopt foreign policy on their own, except when the European Union is controlling in the specific area. *See* Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, Dec. 13, 2007, 2007 O.J. (C306) 1, *available at* http://eur-lex.europa.eu/JOHtml.do?uri=OJ:C:2007:306:SOM:en:HTML.

131. Gilbert, *supra* note 100, at 822-23; *Q&A: The Lisbon Treaty*, BBC NEWS (Jan. 1, 2011), http://news.bbc.co.uk/2/hi/europe/6901353.stm [hereinafter *Q&A: The Lisbon Treaty*].

132. *Q&A: The Lisbon Treaty*, *supra* note 131.

133. Gilbert, *supra* note 100, at 823.

134. *See generally* Regulation Explained, *supra* note 122.

135. *See generally id.*

### B. The Data Regulation versus the Privacy Directive

When the European Union decided to reform its personal data protection policies, it had to decide between a reformed directive and a new regulation. According to one source, the European Union considered that "EU regulations are the most direct form of EU law. As soon as a regulation is passed, it automatically becomes part of the national legal system of each Member State."[136] On the other hand, the European Union also considered that "EU directives . . . are used to bring different national laws in-line with each other. Once a directive is passed at the European Union level, each Member State must implement or 'transpose' the directive into its legal system. . . . A directive only takes effect through national legislation that implements the measures."[137]

Beginning with Article 1, the Data Regulation, like the Privacy Directive, maintains the European Union's view on privacy protection through defining privacy as a human right and other actions.[138] One of the key differences with the purpose of the Data Regulation from the Privacy Directive is that the Data "Regulation *lays down* rules relating to the protection of individuals."[139] Article 2 of the Data Regulation provides that the regulation applies to *all* processing of personal data *except* for exclusions such as national security and criminal investigation,[140] which is exactly like the Privacy Directive.[141]

Article 3 is the first instance where the Data Regulation significantly differs from the Privacy Directive. Article 3

---

136. Gilbert, *supra* note 100, at 823.

137. *Id*. at 824.

138. *Commission Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, art. 1, COM (2012) 11 final (Jan. 1, 2012) [hereinafter Data Regulation], *available at* http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:EN:PDF.

139. *Id*. (emphasis added).

140. *Id.*

141. *See* Privacy Directive, *supra* note 54, art. 2.

provides the regulation applies when the controller is within the European Union, when processing occurs within the European Union, and/or when laws of the Member State would apply under public international law.[142] Article 3 of the Data Regulation is different from the Privacy Directive because, first, the Privacy Directive never identified the jurisdiction and, second, the jurisdiction is too broad to cover the reach of Internet users.[143]

Under Article 4, the Data Regulation established definitions for the Data Regulation that includes similar definitions to the Privacy Directive, especially for the definitions listed above.[144] However, Article 4 is different than the Privacy Directive because the Data Regulation includes more specific terms.[145] Similar to Article 5 of the Privacy Directive, the Data Regulation contains the same principles for personal data processing.[146] Under the principles in Article 5, Personal data must be:

> (a) processed lawfully, fairly and in a transparent manner . . . ;
>
> (b) collected for specified, explicit and legitimate purposes . . . ;
>
> (c) adequate, relevant, and limited to the . . . purposes for which they are processed . . . ;
>
> (d) accurate and kept up to date; every reasonable step . . . to ensure that personal data that are inaccurate . . . are erased or rectified without delay;
>
> (e) kept . . . no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the data will be processed

142. Data Regulation, *supra* note 138, art. 3.
143. *See* Privacy Directive, *supra* note 54.
144. *See* discussion, *infra* Sec.II.C.
145. Data Regulation, *supra* note 138, art. 4.
146. *Id.* art. 5.

> solely for historical, statistical or scientific research purposes . . . ;
>
> (f) processed under the responsibility and liability of the controller, who shall ensure and demonstrate for each processing operation the compliance with the provisions of (E.U. General Data) Regulation.[147]

Article 6 of the Data Regulation elaborated the principles of the regulation by identifying how the personal data may be processed. Processing is only lawful if one of the following applies:

> (a) the data subject has given consent to the processing . . . for one or more specific purposes;
>
> (b) processing is necessary for the performance of a contract to which the data subject is party or . . . at the request of the data subject prior to entering into a contract;
>
> (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
>
> (d) processing is necessary in order to protect the vital interests of the data subject;
>
> (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
>
> (f) processing is necessary for the purposes of the legitimate interests pursued by a controller, except . . . overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This [is] not app[licable] to processing . . . by public authorities.[148]

147. *Id.*
148. *Id.* art. 6.

The principles enumerated in the Data Regulation may not use the exact language as the principles of Article 6 of the Privacy Directive, but the principles are substantively the same.[149] However, Article 6 is not just limited to the lawfulness of the processing listed above. Article 6 considers processing for historical, statistical, or scientific research consistent with the safeguard under Article 83 of the Data Regulation.[150] Finally, Article 6 also requires that paragraphs (c) and (e) from paragraph 1 can only apply when the basis for processing is established under European Union law or the law of the Member State under which the controller is subject.[151]

Article 7 is a unique departure from the Privacy Directive. Article 7 is specifically about how businesses can obtain personal information. Under the Privacy Directive, companies generally had the option to give the data subjects the opportunity to "opt-in" or "opt-out"[152] because the Privacy Directive only required "unambiguous consent." When the Member States attempted to define "unambiguous consent," they defined "unambiguous consent" as the data subject clearly understanding why his or her data will be processed and the identity of the data processor without legalese.[153] However, the Data Regulation requires the data subject consents to processing for specific purposes. The specific purpose requirement limits how much the personal data can be proliferated because the processor must obtain consent for reason the information is processed. The Data Regulation is not limited to consent on specific purposes, but also imposes the following burdens:

---

149. *See id*. The Data Regulation appears to be more lenient and willing to allow processing for more purposes but only under strict exceptions.

150. *Id*.

151. *Id*.

152. *See* Privacy Directive, *supra* note 54, arts. 6-7 (the opt-in/opt-out requirement stems from the Article 7 and Article 8 requirement of the E.U. Privacy Directive).

153. *Id*. art. 7.

> 1. The controller shall bear the burden of proof for the data subject's consent to the processing of their personal data for specified purposes.
>
> 2. If the data subject's consent is to be given in the context of a written declaration which also concerns another matter, the requirement to give consent must be presented distinguishable in its appearance from this other matter.[154]

The burden shift requires the processors to prove that they obtained the consent from the data subject. With the new requirement, the processors are likely to be explicit to obtain consent so there would be little or no question about the data subject's consent to the processing.

In Article 8 of the Data Regulation, the European Union explicitly protects and prohibits the processing of children's[155] personal data.[156] However, children's data can be processed if the child's parent consents to the processing.[157] Article 8 also places requirements on the controller to verify the parent actually gave consent.[158]

Article 9 specifically prohibits processing certain types of personal information, including "revealing race or ethnic origin, political opinions, religion or beliefs, trade- union membership, and the processing of genetic data or data concerning health or sex life or criminal convictions or related security measures."[159] This special data is known as sensitive data under the Privacy Directive and the Data Regulation. However, the Data Regulation does allow this strict prohibition to be waived if the data subject has given consent pursuant to Article 7 and Article 8.[160] While Article 9 provides more requirements than in Article

---

154. Data Regulation, *supra* note 138, art. 7.

155. *Id*. art. 8 (the Regulation defines a child as a data subject who is 13 year old or younger).

156. *Id*.

157. *Id*.

158. *Id*.

159. *Id*. art. 9.

160. *Id*.

7 and Article 8, the exemptions to the strict prohibition in Article 9 of the Data Regulation are the same exemptions to the sensitive data prohibition in the Privacy Directive.

Articles 11, 12, 13, 14, and 15 provide that the data subject must be given certain information. Within these articles, the Data Regulation provides that the controller must provide clear information and communication about the data subject's rights in an "intelligible form."[161] Article 14 specifically provides that the following information at a minimum must be provided to the data subject:

> (a) the identity and the contact details of the controller and, if any, of the controller's representative and of the data protection officer;
>
> (b) the purposes of the processing for which the personal data are intended, including the contract terms and general conditions where the processing is based on point (b) of Article 6(1) and the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);
>
> (c) the period for which the personal data will be stored;
>
> (d) the existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject or to object to the processing of such personal data;
>
> (e) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;
>
> (f) the recipients or categories of recipients of the personal data;

161. *See id*. arts. 11-15. Intelligible form likely means intelligible to the data subject and is not in legalese so the data subject can understand the information.

> (g) where applicable, that the controller intends to transfer to a third country or international organi[z]ation and on the level of protection afforded by that third country or international organi[z]ation by reference to an adequacy decision by the Commission;
>
> (h) any further information necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are collected.[162]

Finally, the articles provide the data subjects with the "Right to Access" their information. Like the Privacy Directive, the Data Regulation provides data subjects with the "Right to Access" the information obtained from them.[163] Accordingly, Article 16 provides the data subject with the ability to modify and correct the data subject's personal and sensitive data.[164]

However, the Data Regulation does not end with the "Right to Access." Article 17 of the Data Regulation provides data subjects with the "Right to Be Forgotten."[165] "The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data."[166] While there appears to be a general right by the data subject to erase his or her information, the Data Regulation requires one of the following to apply:

> (a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

---

162. *Id.* art. 14. Article 14 also provides instances when the information does not need to be provided to the data subject. Id. art. 14. Article 14 gives the European Union Commission the authority to adopt a standard form to disseminate the required information. *Id.* art. 14.

163. *Id.* art. 15.

164. *Id.* art. 16.

165. *Id.* art. 17.

166. *Id.*

> (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;
>
> (c) the data subject objects to the processing of personal data pursuant to Article 19;
>
> (d) the processing of the data does not comply with this Regulation for other reasons.[167]

Similar to the other articles in the Data Regulation, Article 17, while giving the "Right to be Forgotten" to the data subject, establishes specific instances when the controller does not need to delete the data subject's personal and sensitive data.[168] However, Article 17 also lays out how the controller must handle the data subject's deletion request.[169]

While the European Union adopted the Safe Harbor Agreement with the United States, the Data Regulation maintains the Privacy Directive's prohibition towards transferring information to third countries that do not possess adequate privacy protection.[170] Article 40 contains the general provision that prohibits the transfer, processing, etc. of data of citizens of the European Union by third countries unless third countries have the adequate privacy protection.[171] Similar to the Privacy Directive, the European Commission retains the power to declare a third country protection as adequate. However, Article 41 of the Data Regulation is explicit about its ability to determine adequacy and how the Commission should go about determining adequacy.[172] The Privacy Directive gave the same

---

167. *Id.*
168. *See id.*
169. *See id.*
170. *See id.* art. 40.
171. *Id.* The language for Article 40 of the Data Regulation is about the same language from Article 25 of the Privacy Directive. *See id.*; Privacy Directive, *supra* note 54, art. 25.
172. Data Regulation, *supra* note 138, art. 41. Article 41 states:

power to the Commission, but, under the Privacy Directive, the Member States retained some power to authorize transfers to the third countries, which the Member States do not have under the Data Regulation.[173] If the Commission has not determined the adequacy of a third country, the controller can proceed if one of the safeguards from Article 42 is in place.[174] Article 42 references, and Article 43 elaborates on what are known as binding corporate rules.[175] Binding corporate rules affect and are established by the individual company, which is completely different then the adequate protection requirement because it does bind the entire country. The binding corporate rule provision is similar to the Safe Harbor Agreement because it does not require the entire country to have adequate protection under the Data Regulation and is enforced by the policies established by the individual companies.

The final notable difference between the Data Regulation and the Privacy Directive is the notification of a data breach found in Article 31 and 32. Article 31 requires notification to the

---

When assessing the adequacy of the level of protection, the Commission shall give consideration to the following elements:
(a) the rule of law, relevant legislation in force, both general and sectoral, including concerning public security, defence, national security and criminal law, the professional rules and security measures which are complied with in that country or by that international organisation, as well as effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred;
(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or international organisation in question responsible for ensuring compliance with the data protection rules, for assisting and advising the data subjects in exercising their rights and for co- operation with the supervisory authorities of the Union and of Member States; and
(c) the international commitments the third country or international organisation in question has entered into.
*Id*.

173. *Cf*. Privacy Directive, *supra* note 54, art. 5.

174. Data Regulation, *supra* note 138, art. 42.

175. *See id.* arts. 42-43. The Data Regulation establishes the minimum requirements for the company's binding corporate rules. *See id.* art. 43.

regulatory agency within 24 hours of the breach.[176] Article 32 requires communication of the data breach to the data subject.[177] Articles 31 and 32 are important and consistent with the overall theme of the Data Regulation by giving the data subject more control over his or her personal and/or sensitive information. By communicating the breach to the data subject, the data subject will have sufficient knowledge to determine if he or she would like to either be "forgotten" or continue keeping his or her data with the business. The purpose behind notifying the regulatory agency in the affected Member State(s) would assist in enforcement, making sure the security protection is sufficient and the processor fulfills its obligations under the Data Regulation.

### C. The Data Regulation and the Safe Harbor Agreement

While the Data Regulation mirrors the Privacy Directive in key areas, the Data Regulation still differs in the key areas that may affect how United States companies operate in the E.U. pursuant to the Safe Harbor Agreement. The purpose of this section is to consider if the Safe Harbor Agreement can continue as it is under the principles and policies behind the Data Regulation. While it is impossible for Safe Harbor Agreement to continue the status quo, United States businesses can continue functionally in the same way, fulfilling the principles and policies from the Data Regulation without a wholesale change in privacy protection.

With the additional rights in the Data Regulation from the Privacy Directive, the additional rights must be transposed to the Safe Harbor Agreement. Currently under the Safe Harbor Agreement, United States companies must create a privacy policy incorporating the seven principles discussed above:[178] choice, notice, onward transfer, technical security, data integrity, access, and enforcement. The notice principle under the Privacy

176. Data Regulation, *supra* note 138, art. 31.
177. *Id.* art. 32.
178. *See* discussion, *supra* sec. II.C.

Directive only requires notice about why the data is collected, but notice under the Data Regulation also requires notice about security breaches. To require notice about security breaches could also fall under the technical security principle because the companies will increase their security protection to prevent data breaches. The Data Regulation's notice requirement would allow the data subjects to stay informed about their data, allow the data subject to maintain their consent, and help with enforcing the lawful processing and transferring to third parties.

The Data Regulation also requires United States companies to provide a greater level of access to the data subject. Instead of solely allowing the data subjects to access their data to correct and update the information, the Data Regulation will require the companies to provide the data subjects with the ability to delete their data, modifying the access principle of the Safe Harbor Agreement. This increased access would also require the companies to provide greater technical security. With more access by the data subjects, the companies will need to increase the security to ensure that only the specific data subject will be able to access his or her data.

The Data Regulation's change in the requirements for consent and onward transfer will force a change in the choice and onward transfer principles as well. Instead of the traditional "opt-in" or "opt-out" consent requirement, the Data Regulation requires the data subject's consent for each purpose of processing. This change will likely require companies to contact each data subject to obtain consent about each additional purpose and each onward transfer, with the communication monthly or annually. This modification to consent in the Data Regulation is relatively similar to the data integrity principle, limiting the data to relevant use related to the original purpose. However, the companies must obtain consent for each purpose and explain each purpose to the data subject, as well as identify the controller for the onward transfers. The companies also retain the burden to prove the data subject consented to the processing. The explanations and surely numerous purposes for processing personal and sensitive data will likely result in countless pages of a user agreement for the data subject to read. However, this sort

of reaction by companies will be limited because Article 11 requires the information be provided to the data subject in an "intelligible form."[179]

Finally, the companies will likely continue to operate as a result of the binding corporate rules provision from Article 32 while providing the necessary rights to the data subject. The binding corporate rules exception appears to be the European Union's incorporation of the Safe Harbor Agreement skeleton into its proposed Data Regulation. Like the Safe Harbor Agreement, the binding corporate rule provision focuses on an individual company's privacy protection, not an entire country. Also like the Safe Harbor Agreement, this provision requires individual companies to adopt policies/rules to protect the data that are enforceable against the company. The provision provides for binding corporate rules that are consistent with the other articles of the Data Regulation. Therefore, based on the similarities between the binding corporate rules and the simple changes required by the Data Regulation, United States businesses can continue their business in the European Union under the Safe Harbor Agreement.

## IV. BREAKING GROUND FOR AN INTERNATIONAL PRIVACY STANDARD

This section will consider the effect of the Privacy Directive towards voluntary and involuntary compliance with the European Union's privacy standards by individual companies/industries. This section will also consider the Privacy Directive's political and sovereign effect on global powers, focusing primarily on the United States. Finally, this section will conclude by weighing the self-regulatory approach's entrenched

179. This issue will be determined by the definition if intelligible form. However, based on the Data Regulation's pro-data subject policies and roll over from the Privacy Directive, it should be safe to assume intelligible form will be determined from the reasonable data subject's perspective. Until this definition is binding, "intelligible form" will be the subject for the European Commission's consideration. *See* Data Regulation, *supra* note 138, art. 11.

effect on an international online privacy regulation, and will ultimately determine the European Union's approach will lead to a global privacy standard based on the effects the Privacy Directive has already had on the global powers and the potential effect the Data Regulation will have.

### A. European Union's Market Effect Creating an International Standard

The European Union began as a method for the Member States to unify their economic interest in the steel industry into an international economy, known as the European Coal and Steel Community.[180] When the original six countries joined together, Belgium, France, West Germany, Italy, the Netherlands, and Luxembourg, these countries were global powers.[181] Soon after the original organization's formation, the Member States recognized the strength of their combined influence and the resulting benefits of a single European market, so they wanted to increase these benefits. This change was accomplished by a name change and expanding the role/power of the organization from an industry-specific decision to an economic-related decision to barriers to entry. By unifying their interests, the European Union has become a force to be reckoned with.

Over the organization's development, the number of Member States grew, and, with the growth, the organization's market and influence grew too. Currently, the European Union sits at the top, as one of the most important, if not the most important economic market in the world.[182] A basic economic principle dictates that businesses operate where the opportunity to make

---

180. *European Communities*, CVCE, http://www.cvce.eu/obj/the_european_communities-en-3940ef1d-7c10-4d0f-97fc-0cf1e86a32d4.html (last visited Mar. 13, 2014).

181. *Treaty Establishing the European Coal and Steel Community, ECSC Treaty*, EUROPA, http://europa.eu/legislation_summaries/institutional_affairs/treaties/treaties_ecsc_en.htm (last visited Mar. 13, 2014).

182. *See* Trade: Committed to Free and Fair Trade, European Union, http://europa.eu/pol/comm/ (last visited Mar. 30, 2013).

money is located,[183] and, to follow the money, companies will continue to make the necessary accommodations to remain in the market, so long as the costs of the accommodations do not outweigh the potential gain/profit.[184] This principle is applicable to the European Union because companies will accommodate and follow the European regulations to maintain their presence in the European Market.

When the European Union established the Privacy Directive, companies followed this basic principle and modified their networks to accommodate the privacy requirements. By placing restrictions on processing data, the European Union also placed restrictions on conducting business in the European Union because, in the online economy, processing data is necessary to complete transactions. Accommodating the Privacy Directive requirements has already limited some companies' profits because they would sell the information for profit and/or use the information to decrease costs by targeting customers that are now restricted under the Privacy Directive.

While the Privacy Directive was immediately applied to European companies and subsidiary companies located in Europe, the privacy accommodations were not as swift for the third countries defined by Article 25. This delay can be attributed to at least three reasons. First, and the most obvious from Article 25, the third countries took their time to adopt the necessary legislation to have "adequate protection." The third countries had to transition and adopt privacy legislation unique to the countries' regulatory structure and ideology.[185] However,

---

183. Depending on the amount of demand for a specific good or service, more businesses for the good and/or service will be drawn to the area.

184. Also, due to the European Market effects other countries are effectively powerless to retaliate against the high privacy protection standards. Shaffer, *supra* note 13, at 8.

185. *See* HEISENBERG, *supra* note 83, at 103. Countries wanted to develop strict standards to ensure its companies could compete in the European Market. *Id.* However, the third country companies are likely able to operate in Europe through a subsidiary formed in the EU. The subsidiary will be an extension of the parent corporation, but the subsidiary would maintain

the third countries wanted to get back into the European Market as fast as possible. To minimize the delay, the countries would essentially copy and paste a Member State's Privacy Directive legislation to acquire the adequate protection label. This desire to enter the European Market as fast as possible and the method to accomplish the goal likely contributed to the domino effect discussed later.[186]

The second reason for the delay is the cost of compliance. While the Privacy Directive specifically enumerated the rights of the data subjects and the responsibilities of the individual companies, companies still had to implement the necessary technology to accommodate the Privacy Directive, such as additional security to prevent a breach.[187] Increasing the security could cost a single company millions of dollars annually for one website,[188] and, as the company obtains more protected information, the cost of compliance will continue to increase.[189] Another factor adding to the cost of compliance is the differences between the Member States' privacy legislation. The differences typically provide some citizens more privacy protection than other states and would cost companies more to comply with varying standards.[190] In fact, the costs of

---

some independence such as preventing processing of information obtained within the control of the European Union. Lokke Moerel, *Back 2 Basics: When Does the EU Privacy Directive (and its implementation law) Apply?*, OXFORD, 15-16 (last visited Mar. 14, 2014), http://www.cambridgeforums.com/ww.admin/materials/privacy/Back_to_Basics_WP%2029%20Paper.pdf (last visited Mar. 14, 2014).

186. *See* discussion *infra* Sec. IV.A.

187. *Data Security: A Growing Liability Threat*, ZURICH, (2009), 3-4, http://uszicc.zurichna.com/media/ZHP%20Delivered/files/DODataSecurityWhitepaper.pdf.

188. *See id*. Zeek.com, a small child's site, estimated the accommodations would cost $200,000 annually. Angela Vitale, Note, *The EU Privacy Directive and the Resulting Safe Harbor: The Negative Effects on U.S. Legislation Concerning Privacy on the Internet*. 35 VAND. J. TRANSNAT'L L. 321, 350 (Jan. 2002), http://www.idg.net/crd_idgsearch.

189. Vitale, *supra* note 188, at 351.

190. *See* HEISENBERG, *supra* note 83, at 103. Companies have provided data subjects with equal privacy protection not a result of lawsuits or government threats but protecting their public images. In addition, applying

compliance deter small companies from entering the European market,[191] which monopolizes the market for the multinational corporations.

Finally, companies were reluctant to accommodate the changes because costs may outweigh the benefits of competing in the European Market. Without comprehensive privacy in the United States, companies will consider treating the U.S. market and the European market differently. The companies could provide the privacy protection to the European market and not the United States. However, it would be costly and unpopular for the legislature to treat United States citizens as second class to Europeans.[192] Additionally, the maintenance of two different standards is also costly for companies.[193] In the alternative, treating everybody the same will also cost the companies because they could no longer sell and profit from the information from anybody. With equal treatment, the companies will pass the costs to the consumers, so for non-European companies their goods or services will be more expensive than domestic products.[194]

Regardless of the cause or length of the delay, European-based companies obtained an advantage from the delay. They

---

different privacy standards creates in imperfection in the market that will force a correction to find ways to continue using data subjects' information for profit. *See* Shaffer, *supra* note 13, at 31-33.

191. Privacy Concerns, *supra* note 8.

192. Assey & Eleftheriou, *supra* note 105, at 156. In fact from my experience, companies like Best Buy and Starbucks provided United States citizens with the same protection as citizens in the European Union by giving all subjects the ability to opt-out of some portions. *See Privacy Public*, STARBUCKS, http://www.starbucks.com/about-us/company-information/online-policies/privacy-policy (last visited Mar. 14, 2014); *Privacy Policy*, BESTBUY, http://www.bestbuy.com/site/Help-Topics/Privacy-Policy/pcmcat20440005 0062.c?id=pcmcat204400050062 (last visited Mar. 14, 2014).

193. Assey & Eleftheriou, *supra* note 105, at 156.

194. The increased costs to comply accompanied with low benefits from being in the European Market made companies consider not operating in the European Market. However, excluding the European Market entails additional costs besides the loss of business. The companies must ensure their website is not accessible in the Member States and maintain the prohibition.

had no decision in compliance and continued operating because the scope of the Privacy Directive included all of the processing activities by the European companies. The Privacy Directive caused the delay and gave the first mover advantage to the European companies because third countries businesses could not compete until adequate protection was acknowledged as well as meeting the individual Member States' requirements. However, this is not an egregious advantage because there are numerous subsidiaries from multinational corporations located throughout Europe that each had to comply with the Privacy Directive aside from the other locations of the corporation.[195]

As third countries adopted legislation with adequate privacy protection, the domino theory will apply to other third countries. When the third countries adopted the adequate privacy protection, they protected against the onward transfer by applying the same requirements as the European Union. As more and more countries unconditionally adopt adequate protection legislation to compete in the European Market, smaller countries will adopt the adequate protection legislation for their companies to compete in the third country's market, and, like the Member States, the protection would apply to every company operating in the third country. Other third countries will not want to give business to a regional competitor and possibly allow another country to become the regional economic hegemony.[196] However, the domino effect can only apply if third countries enforce their privacy protection legislation and continue to adopt adequate protection legislation to gain access to the market.

---

195. *See* discussion, *supra* sec. II.D.

196. *See* STEVEN E. LOBELL, THE CHALLENGE OF HEGEMONY: GRAND STRATEGY, TRADE, AND DOMESTIC POLITICS 1-2 (2005). An example would include the United States and Safe Harbor Agreement after Canada acquired the adequate protection status. DONALD C. DOWLING, JR. & JEREMY MITTEN, INTERNATIONAL DATA PROTECTION AND PRIVACY LAW 26 (White & Case 2009), *available at* http://www.whitecase.com/files/Publication/367982-dc9-478e-ab2f-5fdf2d96f84a/Presentatio/PublicationAttachment/30c48c85-a6c4-4c37-84bd-6a4851f87a77/article_IntlDataProtectionandPrivacy Law_v5.pdf.

The domino effect is minimal under the Data Regulation with the adequacy protection accompanying the binding corporate rules. An element of the binding corporate rules requires the rules be enforceable against the corporation. However, the binding corporate rules do not force third countries to develop adequate protection in the entire country. Therefore, the adequate protection requirement of the Privacy Directive created a domino effect in the market toward an international privacy standard, but the Data Regulation will likely negate the domino effect because the privacy protection can be on a company-to-company basis.

### B. European Union Jurisdiction and the Lessor of Two Evils

The scope of the Privacy Directive is expansive toward data processing, which allows enforcement of the Member States laws to extend beyond the European Union boarders.[197] However, this brings about the question of whether the European Union's jurisdiction can reach third countries. The short answer is yes. American lawyers would likely think back to Civil Procedure and ask whether there is personal jurisdiction? A sovereign country can pass any legislation the country wants.[198] For example, while American jurisprudence would give personal jurisdiction to the courts,[199] the United States courts can still only enforce judgments over assets within the United States boarders. So, the issue becomes whether the European Union can enforce legislation within another country? More specifically, can the European Union interfere with another country's

197. For the purposes of this subsection, when I reference the European Union it will refer to the Member States' law enacted for the Privacy Directive requirement.

198. Axel Spies, *Global Data Protection: Whose Rules Govern?,* 12 SEDONA CONF. J. 105, 120 (2011).

199. *See generally* Pavlovich v. Superior Court, 58 P.3d 2 (Cal. 2002) (holding that the defendant must purposefully avail itself with an interactive website), *see also* Asahi Metal Indus. Co. v. Superior Court of Cal., 480 U.S. 102 (1987) (requiring a purposeful instead of a passive act to establish personal jurisdiction).

sovereign right?[200] Typically, countries do not infringe on another's sovereign right to govern. However, countries bind themselves through treaties, agreements, or organizations that allow for enforcement within another country, such as the international treaties over the high seas.[201] The Privacy Directive does not follow the enforcement through international agreement because this enforcement is typically unilateral. This does not mean that countries have not mutually agreed on jurisdiction for the transfer of information.[202] However, the European Union's unilateral enforcement can occur because of Article 25 of the Privacy Directive, which essentially allows the European Union to ban a third country that does not submit to the European Union.[203] The threat is influential because of the European Market's power as discussed above.[204]

While countries may willingly submit to the European Union's law by passing adequate protection legislation, the courts outside of the European Union are not as willing to enforce the Privacy Directive. One purpose of an international agreement or treaty is to establish when to apply another country's laws and choice of law decisions. U.S. courts generally do not weigh economic principles and political agendas when

200. Either the data subject or by an authority, on behalf the data subject, would bring an action, but the suit would began in Europe. This discussion does not consider the multinational corporation that has subsidiaries in Europe. Due to the physical presence, there is no doubt they can enforce against the corporation. This discussion is intended to consider the corporations whose only presence in Europe is virtual.

201. *See generally* United Nations Convention on the Law of the Sea, Dec. 10, 1982, 1833 U.N.T.S. 397.

202. *See* Spies, *supra* note 198, at 117. The United States and the European Union agreed on the SWIFT database to stop the funding of terrorism.

203. The European Union likely wants its courts to enforce outside of the territory for its citizens rights. The Privacy Directive is centered on protecting and enforcing the data subject's rights. Enforcement from the European Union gives power to the data subject because it reduces the costs for the data subject. The data subject would not have to pay for litigation outside of the country, which makes it possible for the data subject to enforce his or her rights.

204. *See* discussion *supra* sec. IV.A.

determining the applicable law. The Privacy Directive does not contain a choice of law provision.[205] Therefore, it is not only unclear for courts to determine applicable law, but it is also unclear for everyone else.

This specifically creates a problem when two countries have conflicting law. For example, the United States has disclosure requirements by companies that would be illegal under the Privacy Directive. Therefore, companies that hit this wall must decide between violating the lesser of two evils, unless they obtain informed consent to transfer to someone with adequate protection. The travel industry, such as airplanes and shipping/cruises, is substantially affected by this requirement.[206] When a plane arrives in the United States, the Department of Homeland Security requires a passenger manifest to cross-reference for potential terrorists.[207] However, the company only collected the information for a proof of purchase.[208] By transferring this information to the DHS, the companies would violate the Privacy Directive because this transfer would be for a purpose other than why the company collected the information.[209] Therefore, the company would open itself to penalties from the United States government for not following US law or civil liability from the data subjects.[210] Typically, the penalties and fines imposed by the United States are harsher than some Member States.[211] In addition, United States law requires

---

205. While the Privacy Directive does not have a choice of law provision, the Data Regulation has a choice of law provision in Article 3(3), which allows the Regulation to apply when international public law would apply for a Member State.

206. Movius & Krup, *supra* note 6, at 179.

207. *Id.*

208. *Id.* at 198.

209. *Id.*

210. *Id.*

211. *See generally* Zubulake v. UBS Warburg, LLC, 382 F. Supp. 2d 536 (S.D.N.Y., 2005)(imposing significant penalties on a party for failing to produce discovery documents). Some countries, like France, have imposed criminal penalties for the violation of privacy protection as opposed the United States where criminal penalties generally will not occur in civil

the preservation of data especially when expecting and in the course of litigation.[212] However, under most Member States' data protection law as a result of the Privacy Directive, the data must be destroyed after the purpose of collection and processing has been completed and, therefore, not transferred or available for discovery.

Similar to the manifest requirement, since the September 11th Attacks, the United States allowed the government to obtain more information about potential terrorists under the Patriot Act. The Patriot Act allows the government access to necessary information that is within the United States' jurisdiction by virtue of law or international agreement.[213] While the government can access the information, the numbers suggest the access of European Citizens' information is a considerably small number of the total information accessed.[214] Even if a data subject's personal information was accessed, the subpoenas/warrants are not public and the data subject would rarely know.[215] As a result of the potential access, European companies advertise that the United States government would have access to their information without their consent, and, by selecting a European company, the United States government

---

cases unless you defy a court order. Gareth T. Evan & Farrah Pepper, *Court Holds U.S. Discovery Rules Trump French Law and Hague Convention*, 9 DIGITAL DISCOVERY & E-EVIDENCE 1, 3 (Dec. 1, 2009), *available at* www.gibsondunn.com/publications/Documents/Evans-Pepper-CourtHoldsUSDiscoveryRules.pdf.

212. *See generally* Zubulake, 382 F. Supp. 2d 536; Evan & Pepper, *supra* note 211, at 2.

213. *See generally* Societe Natioanle Industrielle Aerospatiale v. U.S. Dist. Court for the S. Dist. of Iowa, 482 U.S. 522 (1987) (holding a U.S. may compel production of document within the possession, custody, or control of an entity under U.S. jurisdiction). However, the courts have considered a list of factors to compel production, namely U.S. government concern, which will outweigh foreign interests. *See generally* United States v. Bank of Nova Scotia, 691 F.2d 1384 (11th Cir. 1982).

214. *See* Steven C. Bennett et al., *Storm Clouds Gathering for Cross-Border Discovery and Data Privacy: Cloud Computing Meets the U.S.A Patriot Act*, 13 SEDONA CONF. J. 235, 245 (2012).

215. *See id.*

could not access the personal information for the European company to gain additional business.[216] However, under the Privacy Directive, Member States can create exceptions for data access for investigating criminal offenses and national security, including terrorism.[217] Even the data subject's information would not be shielded from the European Union for national security issues.[218] Therefore, the Patriot Act actually does not violate the Privacy Directive, and it is similar to legislation passed by Member States for national security issues. While the European Union does have influence to enforce the Privacy Directive exterritorialy, the document does not provide guidance when the privacy legislation would apply over other countries' laws.

### C. Self-Regulation as a Virus to an International Standard?

While the Directive can begin an International Privacy Policy, the Data Regulation is a better model specifically for the United States.[219] In the United States, state governments have already taken the lead to develop personal data privacy protection policy and, if legislated in mass, have the same potential of fragmentation as the European Union saw under the Privacy Directive. Therefore, the Data Regulation is a better example because it provides a centralized government the opportunity to provide uniform policy, regulation, and enforcement for other

---

216. "[F]rom 2006-2009, 1755 'delayed-notice' search warrants were issued. Of those, 1619 (92%) were issued for drug-related investigations, 122 (about 7%) for fraud; and 15 (less than1%) for terrorism related investigations." *Id.*

217. Privacy Directive, *supra* note 54, art. 3(b).

218. *See id.* at 246-47.

219. One author believes implementation in the United States would not see the slow process of technology development "because the area of free data transferability would be greatly expanded" with two of the largest markets working together. Kevin J. O'Brien, *Cloud Computing Hits Snag in Europe*, NY TIMES, (Sept. 19, 2010), *available at* http://www.nytimes.com/2010/09/20/technology/20cloud.html?pagewanted=all&_r=0.

sovereign entities. This is especially important for an issue like the Internet because it can span multiple jurisdictions within the United States.

While the European Union's implementation of the Data Regulation would provide a good model for the United States' regulatory scheme, the United States' current approach, self-regulation, can make transition difficult, if not impossible. History provides examples of industries that have gone from little to no regulation to complete regulation of the industry by the government. For example, during the Prohibition era of the 1920s, the government proactively banned the sale of alcohol throughout the country. However, alcohol sales during Prohibition were more rampant than before the regulation because money could be made from bootlegging. The enforcement of Prohibition was generally unsuccessful because the regulation created a black market and prevented government oversight of a potentially harmful industry. The United States' approach is similar to alcohol enforcement before prohibition, a patchwork of law regulating the industry. The self-regulatory approach could be a virus to the world of privacy standards like the Pre-Prohibition regulation because there is too much money to be made with personal data. Therefore, a sudden increase in privacy regulation would likely make transition difficult and create an issue for enforcement.[220]

A change from the United States' privacy approach could look similar to the beginning of Prohibition. However, a change in the United States' privacy approach will have an easier transition, similar to the change in regulation for the banking industry during the New Deal. Before the New Deal legislation, the banking industry was predominantly unregulated, except for some self-regulation. These business practices led to the Crash of 1929, contributing to the Great Depression. As a part of the New

220. Another key difference between creating a privacy regulation and Prohibition is Prohibition completely banned the transaction. Whereas a privacy regulation would place limitations how to acquire and use the information. However, a full scale and immediate regulation would still create an enforcement issue.

Deal legislation, the government heavily regulated the industry, a complete turnaround in the regulator scheme before the crash. However, the New Deal regulation did not completely stop the business practices that led to the crash immediately, as there was a progressive approach with targeted regulations for specific practices. A transition to a comprehensive privacy regulation would be similar to the banking regulation in the New Deal as the federal and state governments adopt more industry specific privacy protection.

As a likely effect of the Privacy Directive, the federal and state governments have considered legislation to create comprehensive privacy standards,[221] with some state governments actually passing such legislation.[222] To this date the federal government has considered but not passed comprehensive privacy protection, such as the Privacy Act of 2005.[223] In 2012, President Obama put forth the Consumer Privacy Bill of Rights "that would give Americans many of the baseline protection that the [E.U. Data Regulation] proposes to reinforce."[224] However, Congress has only considered the legislation.

State governments have also increased privacy standards, specifically California, Nevada, and Massachusetts to name a few.[225] Beginning in 2002, California enacted a breach

---

221. *See* Personal Data Privacy and Security Act of 2005, S. 1332, 109th Cong. (2005).

222. *See* Cal. Civ. Code § 1798.82 (West 2014); *see* S. 227, 75th Reg. Sess. (Nev. 2009); *see* MASS. ANN. LAWS ch. 93H, §§ 1-6 (West 2014).

223. Privacy Act of 2005, S. 116, 109th Cong. (2005). The Privacy Act responds to the public concern of "the threat of identity theft posed by the improper use of data." *Id*.

224. Natasha Singer, *Data Protection Laws, an Ocean Apart*, N.Y. TIMES, (Feb. 2, 2013), *available at* http://www.nytimes.com/2013/02/03/technology/consumer-data-protection-laws-an-ocean-apart.html.

225. Vermont, Minnesota, and North Dakota have also adopted legislation that includes principles from the Privacy Directive, while other states have adopted provisions requiring opt-in or opt-out collection. *See* Tallman, *supra* note 104, at 760.

notification law.[226] Then in 2010, Nevada and Massachusetts continued the privacy protection. Nevada required encryption of personal information outside of the company's system.[227] However, Massachusetts has the strongest and farthest-reaching regulation out of the states, disregarding the industry specific regulation.[228] Massachusetts's regulation incorporates the principles and policy in the Privacy Directive and the Data Regulation.[229] Massachusetts requires written security programs and a specific employee responsible for the implementation of the program. Violation of the Massachusetts regulation would place the company in violation of consumer protection laws with $5,000 per violation penalty plus reasonable costs for investigation and litigation.[230] Even though Massachusetts is just one state, the regulation from one state can affect the rest of the country, considering the market effect discussed above.[231] Companies that conduct business in Massachusetts will have to determine if the costs of compliance will outweigh the revenue in the market and consider adopting the strictest standard nationally which would provide the spillover benefits to the rest of the country.

As a result of the state governments' recognition and increase of privacy protection, the transition away from self-regulation is even more possible and easier because the states have done the grunt work, measuring pushback and enforcement issues. In addition, by creating the overall structure in legislation, the administrative agency will be able to increase the regulation progressively through rulemaking and adjudication, like agencies

---

226. California Data Protection Act, Cal. Civ. Code § 1998.82 (West 2014).

227. 2009 Nev. Stat. 1604.

228. Mass. Gen. Laws ch. 93H., §§ 1-6 (2010).

229. *See Penalties For Mass. Personal Information Law Violation - 201 CMR 17.00*, ALERTBOOT (Jan. 21, 2009), http://www.alertboot.com/blog/blogs/endpoint_security/archive/2009/01/21/penalties-for-mass-personal- information-law-violation-201-cmr-17-00.aspx.

230. The regulation also gives individuals the right to bring civil negligence suits from the mishandling of data.

231. *See* discussion *supra* sec. IV.A.

currently regulate. However, until the federal government steps-in to provide a minimum level of regulation, self-regulation will still exist in the country and throughout the world.[232] Once the federal government does step in to regulate, the domino theory would likely apply, and the third countries would follow the United States' privacy standards to conduct business in the United States. With two of the world's largest markets establishing similar privacy standards, a global privacy standard would soon exist.

## V. CONCLUSION

Since the European Union established the Privacy Directive in 1995, the Privacy Directive has had a profound effect on the world by forcing changes in legislation and business practices. Under the Privacy Directive, the Member States passed legislation that adopted the principles and policies within the Privacy Directive by placing restrictions on data processing and expanding the scope of information under the Privacy Directive. While the companies in Europe, including subsidiaries based in Europe, are automatically subject to the Privacy Directive legislation, the Privacy Directive also required third countries to ensure adequate protection, which typically required the third country to adopt the same or similar legislation as the Member States.

However, the Privacy Directive has not completely removed competing approaches to privacy protection, namely the self-regulatory approach that is prominent in the United States. Due to the scale of trade between the United States and European Union, the United States Department of Commerce and the European Union worked out and approved the Safe Harbor Agreement. The companies that self-certify under the Safe Harbor Agreement are eligible to process data in or from the

232. The federal government's involvement could mean preemption to the state government in providing higher standards. *See* Gellman, *supra* note 3, at 147. However, preemption would require legislation to include explicit preemption or imply preemption through field preemption.

European Union by adhering to the seven principles enumerated in the Agreement. The seven principles must be included into the company's privacy policy that can be enforced by the FTC.

Even though countries have complied with the processing restrictions, the Privacy Directive has created hardships and inconsistencies for the third country businesses. The European Union drafted the Data Regulation in 2010 and, after comments, the document will potentially be adopted in 2015. Under the Data Regulation, the principles and policies from the Privacy Directive do not substantially differ between the documents. In fact, the Data Regulation provides more rights to the data subjects, such as the "Right to Be Forgotten" and notification of security breach, in addition to the uniformity issue from different levels of privacy protection among the Member States. The Data Regulation also provides varying methods for compliance such as the binding corporate rules. The binding corporate rules provision is similar to the Safe Harbor Agreement because the provision does not require entire countries to ensure adequate protection, but only individual companies. The provision also provides that the companies draft privacy policies that incorporate the rights, principles, and policies within the Data Regulation. With the Data Regulation almost duplicating the Privacy Directive, this provision provides for essentially uninterrupted processing during the transition between governing documents.

Finally, the Privacy Directive can be considered a step towards an international privacy standard because of the market power of the European Union. Since countries and companies want to be involved in the European market, they will adopt the necessary privacy protection to continue processing data in the European market. By restricting data processing, the European Union can restrict any online transaction within the European Union. The European Union essentially required third countries to adopt similar legislation to the Privacy Directive to enter the European Market. However, once the European Union adopts the Data Regulation, the mandatory requirement to establish adequate protection through adopting privacy legislation has lessened and will likely disappear with the adoption of the Data

Regulation. By lessening the mandatory legislative adoption requirement, privacy protection will likely be on a company-by-company basis. However, with the market effect of the European Union, all businesses will potentially provide privacy protection to its consumers, essentially developing an international standard.

To develop an international privacy standard, the United States must shift away from its self-regulatory approach. Potentially, United States' companies can shift the country away from its approach through enforcement by the European Union. While the European Union can establish and enforce the Privacy Directive, it cannot strong-arm another country's courts to enforce the Privacy Directive. Even with jurisdiction, enforcement through the United States courts is unclear because of the competing government interests and contradicting laws.

However, the Data Regulation, unlike the Privacy Directive, includes a conflict of laws provision to apply the Data Regulation in other countries when public international law would apply.

History has shown that the United States can implement a comprehensive regulatory scheme in an industry that had little to no regulation without much pushback from the industry. In fact, the Data Regulation provides the framework for the United States due to the sovereign relationship between the federal government and state governments. While the federal government has only considered changes to the privacy protection scheme under Presidents Bush and Obama, the state governments have implemented modification to privacy protection that is similar to the principles and protection established in the Privacy Directive that can affect businesses outside of the state. As state governments continue to develop different privacy protection standards, the costs of compliance with all of the different privacy standards may become too costly. Congress must then step in to unify the state laws for the national economy. As the United States develops privacy standards similar to the European Union, the global market will shift to the standards established by two of the largest markets in

the world, in essence creating a global privacy standard for data processing.