University of Arkansas at Little Rock Law Review

Volume 36 | Issue 2 Article 3

2014

The Snowden Revelations, the Transatlantic Trade and Investment Partnership and the Divide Between U.S.- EU in Data Privacy Protection

Ioanna Tourkochoriti

THE SNOWDEN REVELATIONS, THE TRANSATLANTIC TRADE AND INVESTMENT PARTNERSHIP AND THE DIVIDE BETWEEN U.S.-EU IN DATA PRIVACY PROTECTION

Ioanna Tourkochoriti[*]

I. INTRODUCTION

The Snowden revelations took place in the midst of negotiations on the Transatlantic Trade and Investment Partnership. The first round of negotiations took place on July 8th in Washington D.C. The Spiegel revealed that the U.S. government had been spying on its European Union "partners."[1] The French and German governments were reported to be outraged, with some parliamentarians calling for a suspension of the talks.[2] The revelations are seen as a strong negotiating tool in the hands of the EU, as there is a significant difference in the protection of data privacy between Europe and the United States.[3] The negotiations are currently through their sixth round.[4]

The Transatlantic Trade and Investment Partnership aims at enhancing trade in goods and services and at increasing investment between the United States and the European Union. If concluded, the scale and breadth of a U.S.-EU free trade agreement would be unprecedented, as the economic relationship between the U.S. and the EU is the largest in the world.[5] Combined, the EU and the U.S. account for approximately 40% of world GDP and 30% of world trade.[6] The development of provisions to aid the use of

---

[*] Wertheim Fellow, Labor and Worklife Program Harvard Law School.

1. Laura Poitras, Marcel Rosenbach & Holger Stark, *Friends or Foes? Berlin Must Protect Germans from US Spying*, THE SPIEGEL (July 1, 2013, 2:58 PM), http://www.spiegel.de/international/world/why-nsa-spying-program-must-be-independently-investigated-a-908726.html.

2. Karen Hansen Kuhn, *Trade Secrets—Draft EU Documents Reveal Trade Agenda with U.S.*, ABOUT EU-USA FREE TRADE & INVESTMENT DEAL, INFO. SHARING & COORDINATION TO STOP TRANSATLANTIC TRADE & INVESTMENT PARTNERSHIP (July 10, 2013, 8:59 AM), http://transatlanticalternatives.wordpress.com.

3. *NSA Leak Shrouds EU-U.S. Trade, Privacy Discussions*, ARMA INT'L (July 24, 2013), http://www.arma.org/r1/news/newswire/2013/07/24/nsa-leak-shrouds-eu-u.s.-trade-privacy-discussions.

4. *See* Memorandum, European Commission, Ensuring transparency in EU-US trade talks: EU publishes negotiating positions in five more areas (May 14, 2014), *available at* http://trade.ec.europa.eu/doclib/press/index.cfm?id=1076.

5. William H. Cooper, *EU-U.S. Economic Ties: Framework, Scope and Magnitude*, CONG. RES. SERVICE (Apr. 2, 2013), *available at* http://www.hsdl.org/?view&did=735058.

6. Bilateral trade in goods and services between the two entities totals $2.7 billion daily. Additionally, $3.7 trillion has been invested in manufacturing facilities, real estate and

electronic commerce in support of trade in goods and services and the movement of cross-border data flows are among these elements of negotiation.[7] Electronic commerce represents 10% of growth in GDP in the world's most developed economies in the last fifteen years. In the United States alone, digital economy represents an estimated 30% of global Internet revenues. According to estimates from the European Commission, over half of the EU-U.S. cross-border trade in services depends on the Internet.[8]

Differences in data privacy and protection between the U.S. and EU have already arisen in the agenda.[9] Senior European data privacy officials have placed preconditions on European participation which would include the United States adopting new privacy protections in multiple areas, including the European Parliament rapporteur on the General Data Protection Regulation, Jan Philipp Albrecht, (Member of European Parliament) and Germany's federal commissioner for data protection, Peter Schaar.[10] These also include addressing inconsistencies in privacy regulations between U.S. states and expanding the coverage of data protection to sectors other than the ones already covered (e.g. healthcare).[11]

Following the revelations, the European Commission made clear that the standards of data protection will not be part of the on-going negotiations for a Transatlantic Trade and Investment Partnership,[12] while the Committee

---

other assets on both sides of the Atlantic. *See* Faegre Baker Daniels, M. Angella Castille, Paul Finlan, Robert J. Kabel & Bradley A. McKinney, *Transatlantic Trade and Investment Partnership (TTIP) Overview*, LEXOLOGY (Aug. 13, 2013), http://www.lexology.com/library/detail.aspx?g=4eecd015-5098-4a01-839c-5e409bdc5d35.

7. Jeffrey S. Beckington, *The United States and the European Union Prepare to Negotiate a Trans-Atlantic Trade and Investment Partnership ("TTIP")*, LEXOLOGY (Apr. 15, 2013), http://www.lexology.com/library/detail.aspx?g=6eb0db95-bfa9-4ee2-80f2-972e8de27dc1.

8. *See* Commission Impact Assessment Report on the Future of EU-US Trade Relations, at 8 n.11, COM (2013) 136 final (March 12, 2013).

9. Eric Shimp, *Data Privacy in the Transatlantic Trade Agreement? US-EU Ponder the Way Forward*, LEXOLOGY (Apr. 10, 2013), http://www.lexology.com/library/detail.aspx?g=c5967083-4af2-4ba0-b4c2-f2ae1b4b9674.

10. *Id.* According to the declaration of Peter Schaar, Federal Commissioner for Data Protection and Freedom of Information, "the inspiring idea of a transatlantic comprehensive trade agreement will not only raise economic growth but also advance the efforts for good data protection in the U.S. and in the European Union. Competitive devaluation at the expense of civil liberties and civil rights must not happen!" Peter Schaar, *Transatlantic Free Trade Zone? But Only When the U.S. Provide Improved Data Protection!*, FED. COMMISSIONER FOR DATA PROTECTION & FREEDOM OF INFO. (last visited Feb. 13, 2013), http://www.bfdi.bund.de/EN/PublicRelations/SpeechesAndInterviews/blog/TransatlanticFreeTradeZone.html?nn=408870.

11. Shimp, *supra* note 9.

12. Press Release, European Comm'n, European Commission Calls on the U.S. to Restore Trust in EU-U.S. Data Flows (Nov. 27, 2013), http://europa.eu/rapid/press-release_IP-13-1166_en.htm.

on Foreign Affairs of the European Parliament insists that a separate agreement on strong data privacy protections is necessary.[13] The Commission refuses to negotiate data protection with the United States as in its opinion, this is a "fundamental right" that is not negotiable.[14]

The European Commission has submitted a proposal for a regulation that updates the privacy-law protection to strengthen the existing legal framework, which will increase the gap in data protection even further.[15] EU officials have discussed the need to reform the current arrangement between the U.S. and EU[16]: the 2000 Safe Harbor Agreement.[17] Commentators in the U.S. fear that the proposed EU regulation heightens certain individual rights beyond levels that U.S. information-privacy law recognizes and centralizes power in the European Commission in a way that destabilizes the current equilibrium.[18]

The existing legal instrument in the European Union is the 1995 Data Protection Directive ("Directive"),[19] which has had great practical impact in shaping other data privacy initiatives within the EU and has proven highly influential outside Europe as well, while also being highly contentious—especially for American business interests.[20] The contention derives from the Directive's qualified prohibition on the transfer of personal data to non-European countries that fail to provide adequate levels of data protection.[21] The fundamental differences between Europe and the United States in the approach to data-privacy regulation concern six distinct variances: their fundamental presumptions; their limits on contractual freedom; their coverage

13. *See Draft Working Document on Foreign Policy Aspects of the Inquiry on Electronic Mass Surveillance of EU Citizens*, at 3 (Apr. 11 2013), *available at* http://www.statewatch.org/news/2013/nov/ep-nsa-surv-inq-working-document-fa-committee.pdf.

14. Memorandum, European Comm'n, Restoring Trust in EU-US Data Flows—Frequently Asked Questions (Nov. 27, 2013), *available at* http://europa.eu/rapid/press-release_MEMO-13-1059_en.htm.

15. *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*, COM (2012) 11 final (Jan. 25, 2012), *available at* http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf [hereinafter Proposed Regulation].

16. Andreas Geiger, *EU Will Ramp Up Data Protection in Wake of Snowden*, THE HILL'S CONGRESS BLOG (Aug. 14, 2013, 7:00 PM), http://thehill.com/blogs/congress-blog/foreign-policy/317061-eu-will-ramp-up-data-protection-in-wake-of-snowden-.

17. *See* Schaar, *supra* note 10.

18. *See, e.g.*, Paul M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966, 1968 (2013).

19. Council Directive 95/46/EC of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 25 [hereinafter Data Protection Directive].

20. *See* Lee A. Bygrave, *Transatlantic Tension on Data Privacy* 5 (Transworld Working Paper No. 19, 2013), *available at* http://www.iai.it/pdf/Transworld/TW_WP_19.pdf.

21. Data Protection Directive, *supra* note 19, at art. 25.

of privacy protections; their difference in the weighing of values in conflict; their definitions of data protections; and their enforcing authorities. This article will consider each difference, the insight that can be gained in this U.S.-EU divergence, and how those differences affect the flow of data between the U.S. and the EU.

II. ANALYSIS OF THE DIFFERENCES IN THE PROTECTION

As mentioned earlier, there are fundamental differences in the protection of privacy between the U.S. and the EU.[22] This section analyzes these differences in view of understanding what they mean for the transatlantic flow of data.

A. The Fundamental Presumptions

In the United States, the presumption is that processing of personal data is permitted unless it causes harm or is limited by law.[23] The opposite presumption is dominant in the European Union where processing is prohibited unless there is a legal basis that allows it.[24] In the same spirit, the European Court of Human Rights has held that the storage of personal data can constitute an interference with the right to respect for private life under ECHR article 8(1) even if there is no evidence that the data was used to the detriment of the data subject or even at all.[25]

B. The Limits on Contractual Freedom

The EU Directive places legislative limits on the ability to contract around data privacy rules.[26] Although the Directive allows data processing to occur when the data subject consents "unambiguously,"[27] it does not allow a data subject to enter into an agreement that permits a data controller to derogate fundamentally from their basic duties on the basis of article 6 principles relating to data quality[28] and article 12[29] concerning access rights of

---

22. *See supra* Part I.

23. *See* Paul M. Schwartz & Daniel J. Solove, *Reconciling Personal Information in the United States and European Union*, 102 CAL. L. REV. (forthcoming 2014) (manuscript at 6).

24. Data Protection Directive, *supra* note 19, at arts. 5, 6, 7.

25. *See* Amann v. Switzerland, App. No. 27798/95, 2000-II Eur. Ct. H.R. at 22, http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-58497.

26. Data Protection Directive, *supra* note 19, at art. 7.

27. *Id.* at art. 7(a), (b).

28. *Id.* at art. 6 ("1. Member states shall provide that personal data must be: (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

the data subject to the data.[30] The Directive binds the states to outlaw the processing of special categories of personal data such as "data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing data concerning health or sex life"[31] with narrow exceptions.[32] The proposed regulation extends the prohibition to the processing of genetic data, of criminal convictions, and related security measures.[33] Under the Directive, states may legislate that the consent of the data subject does not lift the ban.[34] This proposed regulation maintains relevant legislation in the Member States or enacted by the EU foreseeing such prohibitions.[35]

The U.S. data protection regime affords contract and market mechanisms greater latitude in setting data-privacy standards. It permits a significant degree of contractual "override" of the privacy-related interests of data subjects.

---

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 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 that 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. 2. It shall be for the controller to ensure that paragraph 1 is complied with.").

29. *Id.* at art. 12 ("Right of access. Member States shall guarantee every data subject the right to obtain from the controller: (a) without constraint at reasonable intervals and without excessive delay or expense: - confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed, - communication to him in an intelligible form of the data undergoing processing and of any available information as to their source, - knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15(1); (b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data; (c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.").

30. *See* Bygrave, *supra* note 20, at 6.

31. Data Protection Directive, *supra* note 19, at art. 8.

32. *Id.* at art. 8(2).

33. Proposed Regulation, *supra* note 15, at article 9(1).

34. Data Protection Directive, *supra* note 19, at art. 8(2)(a).

35. Proposed Regulation, *supra* note 15, at art. 9(2)(a).

C. The Coverage of Protection

The Directive is broad in scope and applies to the processing of personal data in both the private and public sectors. The protection afforded is wider in Europe: the EU regime is more restrictive as to the use of data.[36] Any processing of personal data must be fair to the individuals concerned. The principle of proportionality applies here as well, "the data must be adequate, relevant and not excessive in relation to the purposes for which they are processed."[37] The directive provides data subjects with a right to control the use of their personal data.[38] Data subjects are to be informed about the entities that collect their personal information, how it will be used and to which third parties it will be transferred.[39] Subjects have the right to verify the accuracy and the lawfulness of the processing, and to know the logic involved in the automatic processing of data that concerns them.[40] According to the new regulation, the collection and processing of personal data must be for "specified, explicit and legitimate purposes."[41]

In contrast, U.S. law contains only limited sector-specific protections for sensitive information.[42] It does not generally restrict automated processing. U.S. law allows companies to try new kinds of data processing. This promotes innovation but might lead to new ways to violate privacy.[43] The result of the sector-by-sector approach in the U.S. makes technology companies a powerful voice in favor of the regulatory status quo. The consumer data privacy framework consists of industry best practices, FTC enforcement, and a network of chief privacy officers and other privacy professionals who develop privacy practices that adapt to changes in technology and business models and create a growing culture of privacy awareness within companies.[44]

---

36. *See supra* notes 28–29.
37. Data Protection Directive, *supra* note 19, at § 28.
38. *See id.* at arts. 7, 11, 14.
39. *Id.* at art. 11.
40. *Id.* § 41 (Considerations of trade secrets or intellectual property and copyright protecting software cannot result in the data subject being refused all information.).
41. *Id.* at art. 6(1)(b).
42. For a general presentation, see Schwartz, *supra* note 18, at 1974.
43. *See id.* at 1978.
44. *See* THE WHITE HOUSE, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (Feb. 23, 2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf [hereinafter Consumer Data Privacy].

D. The Difference in the Weighing of Values in Conflict

When privacy conflicts with other rights such as freedom of expression, the balancing of European enforcement mechanisms (data-protection authorities and courts) weighs mostly in favor of protecting privacy.[45] In the U.S., however, when privacy claims are weighed against First Amendment rights, most often the latter win out.[46] Recently, the United States Supreme Court struck down a Vermont law that barred pharmacies from disclosing information to "data miners."[47] Pharmacies receive "prescriber-identifying information" when processing prescriptions and sell the information to "data miners" who produce reports on prescriber behavior and lease their reports to pharmaceutical manufacturers.[48] "Detailers" employed by pharmaceutical manufacturers then use the reports to refine their marketing tactics and increase sales to doctors.[49] Vermont's Prescription Confidentiality Law provided that absent the prescriber's consent, prescriber-identifying information may not be sold by pharmacies and similar entities, disclosed by those entities for marketing purposes, or used for marketing by pharmaceutical manufacturers.[50]

For the Court, the law enacted a content- and speaker-based restriction on the sale, disclosure, and use of prescriber-identifying information forbidding sale subject to exceptions based in large part on the content of a purchaser's speech. It then barred pharmacies from disclosing the information when recipient speakers will use that information for marketing. Finally, it prohibited pharmaceutical manufacturers from using the information for marketing.[51]

The statute disfavored marketing, i.e. speech with a particular content, as well as particular speakers, i.e. detailers engaged in marketing on behalf of pharmaceutical manufacturers, and is thus subject to heightened judicial scrutiny.[52] For the Court, assuming that physicians have an interest in keeping their prescription decisions confidential, Vermont's law is not drawn to serve that interest, as pharmacies may share prescriber-identifying information for any reason except for marketing. The State's interest in burdening detailers' speech thus turns on nothing more than a difference of opinion.[53]

---

45. *See, e.g.*, Von Hannover v. Germany, 2004-VI Eur. Ct. H.R.
46. *See, e.g.*, Jackson v. Playboy Enterprises, 574 F. Supp. 10, 14 (S.D. Ohio 1983).
47. *See* Sorrel v. IMS Health Inc., 131 S.Ct. 2653, 2672 (2011).
48. *Id.* at 2659–62.
49. *Id.*
50. *Id.* at 2660.
51. *Id.* at 2665.
52. *Id.* at 2666.
53. *Sorrel*, 131 S.Ct. at 2672.

This argument would not be popular in the European conception where a concept of privacy as articulated in different spheres that are not overlapping is dominant. Revelation of one piece of information to one sphere does not necessarily mean that this information is public. Thus the state is legitimized to limit specific disseminations of information available in one domain. Similar data in the European Context are considered sensitive as relating to medical privacy and thus under the scope of the EU Directive.

E. The Definition of the Protected Data

The European Union protects information that is identifiable to a person, whereas the United States protects information that is actually liked to an identified person.[54] The EU Directive defines "personal data" as "any information relating to an identified or identifiable natural person . . . ; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."[55]

The EU approach is over-inclusive, whereas the U.S. is under-inclusive.[56] This is because whether information can be re-identified depends upon technology and corporate practices that permit the linking of de-identified data with already identified data.[57] As additional pieces of identified data become available, it becomes easier to link them to de-identified data because there are likely to be more data elements in common.[58]

F. Enforcing Authorities

In implementing the Directive, the EU member states have established independent authorities that monitor and enforce the data privacy laws.[59] Independent authorities are empowered to contribute to the consistent application of the Directive throughout the Union.[60] These authorities conduct investigations, either following a complaint by a data subject, or on their own initiative.[61] They monitor relevant developments insofar as they have an impact on the protection of personal data.[62] Data Controllers may process

54. *See* Schwartz & Solove, *supra* note 23, at 5.
55. *See* Data Protection Directive, *supra* note 19, at art. 2(a).
56. Schwartz & Solove, *supra* note 23, at 18.
57. *Id*.
58. *Id*.
59. *See* Data Protection Directive, *supra* note 19, at art. 28.
60. *See id.*
61. *See id.* at art. 28(3).
62. *See id.*

personal data once they have notified the relevant Data Protection Authority.[63] They also approve corporate binding rules that are obligatory for the transfer of data abroad and participate in the activities of the European Data Protection Board.

In the U.S., the Federal Trade Commission (FTC) has been granted some of these same powers.[64] During the last two decades the FTC has played an increased role in protecting privacy. There are, nevertheless, limits on the scope of its activities. For example, it does not have jurisdiction over all companies,[65] and its enforcement has not extended to even the narrow range of Fair Information Practices used in the United States.[66] The agency concentrates on "notice and choice."[67] The FTC has prompted the members of the online advertising industry to develop self-regulatory principles based on Fair Information Practice Principles.[68] The FTC has maintained that the use or dissemination of personal information in a manner contrary to a posted privacy policy is a deceptive practice under the FTC Act.[69] The Gramm-Leach-Bliley Act of 1999[70] requires the FTC and other agencies to establish security standards for nonpublic personal information.[71] In the public sector in the U.S., seventy Inspectors General conduct, coordinate, and supervise audits and investigations of their respective agencies for issues concerning data privacy. Congressional Committees

---

63. *See id.* at art. 18.

64. *See* 15 U.S.C. § 45 (2000).

65. Exempt from the FTC's jurisdiction are many types of financial institutions, airlines, telecommunications carriers and other types of entities. *See id.* § 45(a)(2).

66. Paul M. Schwartz, *supra* note 18, at 1977–78.

67. FED. TRADE COMM'N, *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress* (May 2000), *available at* http://www.ftc.gov/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission.

68. Jon Leibowitz, FED. TRADE COMM'N, *Self-Regulatory Principles for Online Behavioral Advertising* (Feb. 2009), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadleibowitz.pdf. Fair Information Practices define the core obligations for public or private entities that process personal information. *See* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 915–17 (Vicki Been et al. eds., 4th ed. 2011).

69. 15 U.S.C. § 45 (2000).

70. *Id.* §§ 6801–6809 (2006).

71. *Id.* § 6801(b). The FTC issued regulations according to which financial institutions "shall develop, implement and maintain a comprehensive information security program" that is appropriate to the "size and complexity" of the institution, the "nature and scope" of the institution's activities and the "sensitivity of any customer information at issue." 16 C.F.R. § 314.3(a) (2006). An "information security program" is defined as "the administrative, technical, or physical safeguards you use to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information." *Id.* § 314.2(c) (2006).

have oversight role with respect to the executive branch, including privacy and data protection issues.[72]

III. AN INTERPRETATION OF THE DIVERGENCE

The difference in the data protection is profoundly a difference in the understanding of the role of the state. In Europe, the mission of the state is considered to be to realize citizens' liberty.[73] According to this conception, the state will assure that the citizens will have the necessary preconditions for the exercise of their liberty. This conception of the state often leads to paternalism and the negation of the individual to decide for herself. The possibility allowed by the Directive for statutory limitations of the right to contract out data protection reflects this philosophical attitude. This conception is motivated by the idea that there are inequalities of power within civil society and the state is legitimized to intervene in order to protect the most vulnerable. Data privacy regulation is an important element towards allowing the individual to define for herself how she will realize her liberty. This conception can be summarized in the phrase from the case law of the European Court of Human Rights—that there are "positive obligations inherent in an effective respect for private or family life. These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves."[74] Privacy is understood as a right that extends beyond a negative interest in protecting secret information, to a positive right of personal development and information self-determination and affirmative obligations of the state to secure data protection interests effectively.[75]

In the U.S., the reverse presumption is dominant: the state will intervene to regulate only specific aspects of human activity. Privacy against the state is protected in its form of self-determination, in cases like abortion,[76]

---

72. *See* Solove & Schwartz, *supra* note 23.

73. *See* Ioanna Tourkochoriti, *The Burka Ban: Divergent Approaches to Freedom of Religion in France and in the U.S.A.*, 20 WM. & MARY BILL RTS. J. 791, 809 (2012).

74. *See* X. & Y. v. The Netherlands, App. No. 8978/80, Eur. Ct. H.R. (1985). The case has been characterized as a "landmark" stressing the importance of security measures in the protection of personal data in a manner that ought not to leave any uncertainties for the governmental actors. *See* Jari Råman, *European Court of Human Rights: Failure to Take Effective Information Security Measures to Protect Sensitive Personal Data Violates Right to Privacy*—I v. Finland*, no. 20511/03, 17 July 2008*, 24 COMPUTER L. & SECURITY REP., no. 6, 562–64 (2008).

75. Nadezhda Purtova, *Private Law Solutions in European Data Protection: Relationship to Privacy and Waiver of Data Protection Rights*, 28 NETH. Q. HUM. RTS. 179, 179–98 (2010).

76. *See* Planned Parenthood of Southeastern Pennsylvania v. Casey, 505 U.S. 833, 839–40 (1992); Roe v. Wade, 410 U.S. 113, 152 (1973).

freedom against self-incrimination (Fifth Amendment), and freedom from unreasonable searches and seizures (Fourth Amendment). Privacy is protected in the U.S. in such a way that creates a sphere of inviolability concerning personal decisions. In this sense, it conforms with the logic that the state must intervene within civil society as little as possible. This is potentially why the state is not as willing to intervene in order to protect violations of informational privacy coming from within civil society, whether it is the press or other corporations handling data privacy. Informational privacy is not considered to be a value with enough importance to be protected by violations coming within civil society.[77] According to the conception dominant in the U.S., the state will arbitrate differences and will intervene in order to protect negative liberty, liberty against the state.[78]

IV. WHERE THE DIFFERENCE AFFECTS THE FLOW OF DATA BETWEEN EUROPE AND THE UNITED STATES

The disjunction between the U.S. and EU definitions raises problems regarding international transfers of personal data. There is a complex legal structure for judging the permissibility of these transfers under EU law.[79] The Directive permits transfers to "third countries," that is countries outside of the EU only if they have an "adequate level of protection."[80] The determination of adequacy is made at the member state level by the supervisory authority, which is required to inform the European Commission.[81] The Commission can also decide that a third country does not ensure an adequate level of protection and block any transfer of data to this Country.[82] The European Commission may "enter into negotiations" with countries with inadequate data protection "with a view to remedying the situation."[83] The directive already provides for the law of an EU state to apply outside the EU in certain circumstances—most notably where a data controller based outside the EU uses equipment located in the state to process personal

77. *See* Ioanna Tourkochoriti, Freedom of Expression and the Protection of Human Dignity and Privacy in the French Legal Order and the Legal Order of the United States: A Study on Two Different Constitutional Precomprehensions (Sept. 24, 2010) (unpublished Ph.D. dissertation, École des Hautes Études en Sciences Sociales) (on file with author).

78. *See id.*

79. Data Protection Directive, *supra* note 19, at art. 25, 26.

80. *Id.* at art. 25(1).

81. *Id.* at art. 25.

82. *See id.* at art. 25(3), (4) ("The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure and adequate level of protection. . . . Member States shall take the measures necessary to prevent any transfer of data to [this country].").

83. *Id.* at art. 25(5).

data for purposes other than merely transmitting the data through that state.[84] Issues have come up with Google's apparent absence of respect for EU data-privacy law, although it maintains servers in European Countries.[85] As recently as last year, the French Data Protection Supervising Authority issued a report stating that Google currently provides insufficient information to its users on its personal data processing operations, that it does not provide user control over the combination of data across its numerous services, and that it does not provide retention periods.[86]

Generally, the EU does not consider the U.S. to provide adequate privacy protection.[87] U.S. law does not limit a company's data exports to other countries. Negotiations between the U.S. and EU have resulted in mechanisms that oblige U.S. companies to meet the "adequacy" requirement of the Directive.[88] The Safe Harbor, Model Contractual Clauses and Binding Corporate Rules are some of these mechanisms.[89] The Safe Harbor negotiated between the EU Commission and the U.S. Department of Commerce went into effect in 2000.[90] A member state does not need to make a prior approval of a data transfer to the U.S. To join the Safe Harbor, a company must self-certify to the Department of Commerce that it has complied with the seven principles and related requirements that have been deemed to meet the EU's adequacy standard.[91] Among these principles are "notice" and "choice." Its

---

84. *Id.* at art. 4(1)(c).

85. *See Google: The Beginnings of a Dialog,* ARTICLE 29 WORKING PARTY (Sept. 16, 2008), *available at* http://ec.europa.eu/justice/policies/privacy/news/docs/pr_16_09_08_en.pdf. In 2011, the U.S. FTC had found that Google was not abiding by the U.S.-EU Safe Harbor or other privacy programs. *See id.*

86. Press Release, Comm'n Nationale de l'Informatique et des Libertés, Google's New Privacy Policy: Incomplete Information and Uncontrolled Combination of Data Across Services, (Oct. 16, 2012), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/otherdocument/files/2012/20121016_press_release_google_privacy_cnil_en.pdf.

87. *See, e.g.*, Press Release, European Comm'n, European Commission Calls on the U.S. to Restore Trust in EU-U.S. Data Flows, (Nov. 27, 2013), *available at* http://europa.eu/rapid/press-release_IP-13-1166_en.htm.

88. *See* U.S. DEP'T OF COM., *Safe Harbor Privacy Principles* (July 21, 2000), http://export.gov/safeharbor/eu/eg_main_018475.asp.

89. Lothar Determann, DETERMANN'S FIELD GUIDE TO INT'L DATA PRIVACY LAW COMPLIANCE 25–47 (2012).

90. *See Commission Staff Working Document on the Adequacy of the Protection Provided by the Safe Harbor Privacy Principles and Related FAQs Issued by the U.S. Department of Commerce*, 2000 O.J. (215) 7. The safe Harbor decision was taken following an opinion of Article 29 Working Party and an opinion of the Article 31 Committee delivered by a qualified majority of Member States. In accordance with Council Decision 1999/468, the Safe Harbor Decision was subject to prior scrutiny by the European Parliament. *See id.*

91. *See id.* The Department of Commerce reviews Safe Harbor self-certifications and annual recertification submissions that it receives from companies to ensure that they include all the elements required and updates a list of companies that have filed self-certification

substantive standards are closer to the EU protection. U.S. federal agencies regulate and enforce these standards—most notably, the FTC. As a result, the FTC has found violations of this agreement by companies like Google[92] and Facebook.[93]

The proposed regulation has been criticized as carrying a potential for "destabilization of the current status quo" for a number of reasons.[94] The Regulation develops a controversial "right to be forgotten"[95] should a number of conditions apply, and it elaborates stricter requirements before "consent" can be used as a justification for data processing.[96] The right to be forgotten is described as the right of data subjects to have their personal data erased and no longer processed, where the data is no longer necessary in relation to the purposes for which they were collected or otherwise processed, where data subjects have withdrawn their consent for processing, where subjects object to the processing of personal data, or where the processing of their personal data otherwise does not comply with the Regulation.[97] As it stands, this means that at the complaint of a citizen of an EU

---

letters. The FTC intervenes against unfair or deceptive practices, within its powers of consumer protection according to Section 5 of the Federal Trade Commission Act. The FTC committed to review on a priority basis all referrals from EU Member State authorities. *Id.*

92. *See In re* Google Inc., No. 102-3136, 2011 WL 1321658, at *6 (F.T.C. March 30, 2011). Google did not adhere to the US Safe Harbor Privacy Principles of Notice and Choice for using data for purposes different than the one the data subjects had consented to. *Id.* The settlement further requires Google to establish and maintain a comprehensive privacy program and it requires that for the next 20 years, the company have audits conducted by independent third parties every two years to assess its privacy and data protection practices. *Id.*

93. *See In re* Facebook, Inc., No. C-4365, 2012 WL 3518628, at *21 (F.T.C. July 27, 2012). Under the settlement, Facebook is barred from making misrepresentations about the privacy or security of consumers' personal information; required to obtain consumers' affirmative express consent before enacting changes that override their privacy preferences; required to prevent anyone from accessing a user's material more than thirty days after the user has deleted his or her account; required to establish and maintain a comprehensive privacy program in reference to new and existing products and services; and is required every two years for the next twenty years to obtain independent, third party audits certifying that it has a privacy program in place that meets or exceeds the requirements of the FTC order and to ensure that the privacy of consumers' information is protected. *Id.*

94. *See* Schwartz, *supra* note 18, at 1994.

95. *See* Proposed Regulation, *supra* note 15, at art. 17(1) ("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 . . . .").

96. *See id.* at art. 7.

97. This right is particularly relevant when the data subject has given their consent as a child when not being fully aware of the risks involved by the processing and later wants to remove such personal data especially on the Internet. However, the further retention of the data should be allowed where it is necessary for historical, statistical and scientific research purposes, for reasons of public interest in the area of public health, for exercising the right of freedom of expression, when required by law or where there is a reason to restrict the processing of the data instead of erasing them. *See id.* at § 53.

member state to the supervising Data Protection authority, this authority can order and enforce any processor for example to erase material that concerns them. The Court of Justice of the EU held recently that this enforcement can go as far as obliging Google to use filters that eliminate links in search results on a person that has opted for erasing their data.[98] For the Court even the operator of a search engine like Google engages in activities that "must be classified as 'processing' within the meaning of Article 2(b) of Directive 95/46".[99]

Other measures that the new regulation imposes are the prior approval of supervising authority for any processing of personal data,[100] the right to object to processing for marketing purposes,[101] and the right not to be subject to "profiling," defined as automated processing intended to evaluate certain personal aspects relating to a natural person or to analyze or predict the natural person's performance at work, economic situation, location, health personal preferences, reliability or behavior, e.g. for use in targeted ads.[102] The Directive foresees as exceptions cases of public security, prevention, investigation, detection and prosecution of criminal offences, in particular economic or financial interest.[103]

The new regulation requires controllers and processors to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected.[104] The regulation also allows for heavy administrative fines: up to five percent of the annual worldwide turnover to enterprises violating its clauses, in case of violation of the aforementioned rights.[105]

There seems to be willingness towards conversion among EU and U.S. officials, as indicated in the joint statement issued in 2012 by Vivian Reding, the European Commission Vice-President, and John Bryson, then U.S. Secretary of Commerce, which expressed a commitment to creating mutual recognition frameworks that protect privacy.[106]

---

98. Case C-131/12, Google Spain SL v. Agencia Espanola de Proteccion de Datos, 2014 EUR-Lex 317 (May 13, 2014).

99. *Id.* § 28.

100. Proposed Regulation, *supra* note 15, at art. 34(1).

101. *Id.* at art. 19(2).

102. *Id.* at art. 20.

103. *Id.* at art. 21(1).

104. *Id.* at art. 30(1).

105. *Id.* at art. 79. The European Commission's initial proposal, before the Snowden revelations, was for fines up to two percent of annual turnover.

106. Press Release, European Comm'n, EU-U.S. Joint Statement on Data Protection by European Commission Vice-President Viviane Reding and U.S. Secretary of Commerce John Bryson, (March 19, 2012), *available at* http://europa.eu/rapid/press-release_MEMO-12-192_en.htm.

The Obama Administration's February 2012 White Paper sets out a consumer privacy bill of rights.[107] It contains a set of fair information practice principles to govern private-sector handling of personal data in commercial contexts. The Fair Information Practice Principles go in some respects further than previous U.S. elaborations of such principles. They include a new principle entitled "respect for context: consumers have a right to expect that companies will collect, use and disclose personal data in ways that are consistent with the context in which consumers provide the data."[108] There is no provision about prohibiting profiling altogether, like the one existing in the EU regulation.[109] According to the White Paper, the Obama administration plans to start a public dialogue with all parties towards elaborating codes of conduct for the industry that the FTC will then enforce.[110] The U.S. prefers this solution, as it is more flexible, rather than enacting rigid legislation, which responds to the existing technology at the moment of enacting legislation and is not easily applicable to later technological advances.[111] It will also enact legislation of a basic set of privacy rights throughout areas of the commercial sector not currently subject to specific Federal data privacy legislation.[112] The FTC and state Attorneys General will have the authority to enforce the Consumer Privacy Bill of Rights.[113] The FTC will have the authority to review codes of conduct against the Consumer Privacy Bill of Rights.[114]

V. CONCLUSION

The differences in the protection of privacy between the European Union and the United States indicate that informational privacy is not a value important enough to legitimize state intervention within civil society for its protection. Although there seems to be willingness for convergence, the profound differences, which reflect a more profound clash of values on the role of the state and its intervention within civil society, show that these efforts will be rather limited. Commentators note, however, that another important actor to influence the international standards in the field is China: if its message runs deeply counter to the Western "privacy paradigm" there

107. *See* Consumer Data Privacy, *supra* note 44, at 9.
108. *Id.* at 15.
109. *See id.*
110. *See id.* at 29.
111. *See id.* at 29–30.
112. *See id.* at 35–37.
113. Consumer Data Privacy, *supra* note 44, at 35–36.
114. *Id.* at 37.

may be even greater coordination and convergence of EU and U.S. regulatory policy in the field.[115]

115. Bygrave, *supra* note 20, at 13.