2009

Separated by a Common Language?

Yesha Yadav

SEPARATED BY A COMMON LANGUAGE? AN EXAMINATION OF THE TRANSATLANTIC DIALOGUE ON DATA PRIVACY LAW AND POLICY IN THE FIGHT AGAINST TERRORISM

YESHA YADAV*

I. INTRODUCTION

> I don't believe Europeans value privacy more than Americans. And I don't think that Europeans take the threat of terrorism lightly. I do think, though, that there are some historical differences that cause us to look at some of these issues in different ways.[1]

On June 23, 2006, *The New York Times* reported that the Central Intelligence Agency ("C.I.A.") of the United States, together with the U.S. Treasury, secretly accessed a vast database of financial records as part of U.S. intelligence efforts to combat terrorism.[2] The surveillance, which commenced shortly after September 11,

* Yesha Yadav attended Harvard Law School, where she completed her Masters in Law, and the University of Cambridge, where she graduated with M.A. (Hons.) (First Class) in Law and Modern Languages. Whilst at Harvard, she worked as Senior Research Associate and later (Interim) Research Director for the Committee on Capital Markets Regulation (www.capmktsreg.org). Prior to coming to Harvard in 2008, she worked as an attorney at Clifford Chance, London (2004-2008), specializing in its financial regulation and derivatives practice. She is currently working for the Legal Vice-Presidency of the World Bank, in the Insolvency and Creditor Rights and in its Financial Regulation, Markets and Infrastructure units. The author is solely responsible for the content of this paper, and in particular, for all errors and omissions. The views expressed in this paper are solely those of the author and do not represent the views and opinions of the World Bank, or any of the author's present and past employers. The author's contact address is yeshay@gmail.com.

1. Michael Chertoff, U.S. Sec'y of Homeland Sec., Remarks to the Johns Hopkins University Paul H. Nitze School of Advanced International Studies (May 3, 2007) (transcript available at DHS Press Room Archive website).

2. Eric Lichtblau & James Risen, *Bank Data is Sifted in Secret to Block Terror*, N.Y. TIMES, June 23, 2006, at A1.

2001, provided U.S. intelligence services with access to a massive reserve of financial records held by the Society for Worldwide Interbank Financial Communication ("SWIFT"), a Belgium-based provider of messaging services for financial institutions around the world.[3] In addition to the general outcry provoked by this action within the European Union ("EU"), EU officials determined that SWIFT's cooperation with U.S. intelligence agencies was in violation of EU and Belgian data privacy laws.[4]

The SWIFT case illustrates the legal and political conflict between the U.S. and the EU with respect to the sharing of sensitive information. This conflict has intensified during the years following September 11, 2001, as the escalating U.S.-led "War on Terror" has focused considerable international regulatory attention on data-sharing between the U.S. and its allies in their effort to combat terrorism. In light of past conflicts between the U.S. and the EU with respect to airline passenger information, it is unlikely that the SWIFT case will be the last incident in this area.

This paper examines recent controversies in the legal and policy debate between the U.S. and the EU on the sharing of data in the implementation of transatlantic counter-terrorism measures. The nexus between law and policy in this area is particularly close, reflecting the preferences each jurisdiction has in protecting civil liberty and security interests. While the U.S. and the EU offer differing legal frameworks on data privacy, the strategic importance of data in counter-terrorism law and policy necessitates a joint approach. A failure to arrive at such an approach can result in a series of bilateral agreements between the U.S. and individual EU countries, creating unnecessary costs, inconvenience, and uncertainty for both users and processors of data. The haphazard approach in the past, and the continuing failure to come to a proper accord, reflects the tension between civil liberties and the right of the state to erode such entitlements in the face of a terrorist threat. In addition, the failure to come to an accord reflects the uneasiness U.S. and EU lawmakers feel about the compromises they have

3. *See id.*

4. Edwin Jacobs, *SWIFT Privacy: Data Processor Becomes Data Controller*, 12 J. INTERNET BANKING & COM. 1, 3 (2007).

already made. Fortunately, skirmishes over the cross-border transfer of data can encourage both sides to incorporate elements from the differing approaches into their respective policy regimes.

Part II of this paper sets out a factual summary of the recent cases involving the transfer of airline passenger data between the EU and the U.S. This section will also analyze U.S. intelligence authorities' access to the SWIFT database. Part III sets out a discussion of the policies underlying data privacy laws in the U.S. and the EU. Part IV critically examines a proposed solution to the issue, and the policy implications of the steps taken to further legal decision-making in this area. Finally, Part V provides some concluding remarks.

II. OVERVIEW OF KEY CASES

1. Transfer of Passenger Name Record Data ("PNR data")[5]

Pursuant to the Aviation and Transportation Security Act enacted in 2001, all airlines flying into the U.S. are required to provide the Commissioner of Customs with certain data relating to passengers and cabin crew.[6] Furthermore, following the passage of the Enhanced Border Security and Visa Entry Reform Act in 2002, each incoming and outgoing commercial airliner must provide detailed information on each passenger and crewmember to the

5. PNR data is the name given to the detailed travel records that are created by airlines for each passenger. A PNR will usually contain the details of a passenger including her name, address, fare details, forms of payment used, special service requests such as meal preferences, passport details, date of birth and place of birth. A number of airlines host their PNR databases with a central computer reservation system, or global distribution service provider such as Sabre, Galileo, Worldspan or Amadeus. This means that airlines can centrally pool their PNR records with one provider and share the information, if necessary. Increasingly, such database providers allow travel agents and airlines to book rental cars and hotels as well as air travel. The PNR data for each trip remains within the database even in cases where the trip has been cancelled or altered by the passenger. *See* Press Release from Franco Fratlini, Vice President, European Commission, The Passenger Name Record (PNR): Frequently Asked Questions, MEMO/07/294 (July 13, 2007), *available at* http://europa.eu/rapid/pressReleases Action.do?reference=MEMO/07/294&format=HTML&aged=0&language=EN&guiLanguage=en.

6. *See* 49 U.S.C. § 44909(c) (2006).

Immigration and Naturalization Service.[7] U.S. authorities have the right under U.S. law to access a large amount of passenger data collected in the reservation and departure control systems ("DCS"),[8] and share it with federal agencies for the purposes of fighting terrorism.[9] Such information not only includes basic PNR data, but also other information such as credit card numbers, bank details, telephone number, dietary preferences (which may potentially reveal details about a passenger's religious or ethnic origins), history of preceding and/or planned travel, and medical conditions or contact details for emergency contact persons.[10]

Provision of such detailed and comprehensive information by European airlines and database providers to U.S. authorities was considered by European authorities to be incompatible with Directive 95/46/EC on the protection of individuals with regard to the processing and free movement of such data.[11] In particular, there was concern that U.S. demands would violate this Directive

7. *See* 8 U.S.C. § 1221 (2006).

8. *See* 49 U.S.C. § 44909(c). The DCS contains the passenger name record for all passengers irrespective of whether the passenger is landing or leaving from the U.S. *See* Jacobs, *supra* note 4.

9. *See* 19 C.F.R. § 122.49(a) (2009). It should be noted that European authorities, in the wake of the 2004 Madrid bombings, instituted measures to require air carriers to supply Advance Passenger Information ("API data") to Member State border control authorities. *See* Council Directive 2004/82, 2004 O.J. (L 261) 24 (EC). However, the scope of the information-sharing requirement is more limited under this Directive. *See id.* art. 3(2). API data forms only one part of the PNR record and extends to cover the passenger's name, date of birth, passport number and point of embarkation. In addition, the Directive requires API data to be destroyed after 24 hours unless it is needed for either the exercise of statutory functions, or for law enforcement purposes. *See id.* art. 6(1). In contrast, PNR data is a great deal more detailed, covering such items as payment information, dietary preferences, airlines' or travel agents' remarks about a passenger, baggage information, and may be retained for a number of years under U.S. law.

10. Electronic Privacy Information Center, EU-US Airline Passenger Data Disclosure, http://epic.org/privacy/intl/passenger_data.html (last visited Sept. 9, 2009).

11. *See* Article 29 Data Prot. Working Party, *Opinion 6/2002 on Transmission of Passenger Manifest Information and Other Data from Airlines to the United States*, § 2, 11647/02/EN, WP 66 (Oct. 24, 2002) [hereinafter Working Party, *Opinion 6/2002*], *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs /wpdocs/2002/wp66_en.pdf. *See generally* Council Directive 95/46, 1995 O.J. (L 281) 31 (EC).

by mandating that data, originally collected for a commercial purpose, would be used for a secondary purpose, namely for gathering intelligence for counter-terrorism efforts.[12] In addition, the Directive prohibits the transfer of data to countries outside of the EU if these countries do not provide an "adequate level of protection" for the data.[13] The U.S., considered as lacking a comprehensive regulatory framework for data privacy (discussed further below), was *prima facie* deemed to lack an "adequate level of protection."[14] However, transfers of personal data between the U.S. and the EU could still take place within a bilaterally negotiated agreement, or with the consent of the subject whose data was subject to the transfer.[15] Finally, there was concern that once data was provided to the U.S., European data privacy authorities would no longer be able to exercise control over the management of the data[16] and that the data itself was then liable to be treated without a sufficiently robust standard of protection.[17]

Accordingly, the legal demands made by U.S. authorities on European airlines regarding detailed passenger data necessitated joint regulatory and political action to ensure compatibility with the Directive.[18] Consequently, EU and U.S. authorities came to a

12. *See* Working Party, *Opinion 6/2002*, *supra* note 11, § 2.4.

13. Council Directive 95/46, *supra* note 11, art. 25(1). "Adequacy" is measured in relation to the individual data transfer, taking into account a variety of circumstances, including "purpose and duration" of the processing, the security measures in place for protecting the data, and the rule of law of the country of transfer. *Id.* art. 25(2).

14. *See* Working Party, *Opinion 6/2002*, *supra* note 11, § 2.5.

15. *See* Council Directive 95/46, *supra* note 11, art. 26.

16. *See generally* Article 29 Data Prot. Working Party, *Opinion 4/2003 on the Level of Protection Ensured in the US for the Transfer of Passengers' Data*, 11070/03/EN, WP 78 (June 13, 2003), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp78_en.pdf.

17. *See* Working Party on the Prot. of Individuals with Regard to the Processing of Personal Data, *Opinion 1/99 Concerning the Level of Data Protection in the United States and the Ongoing Discussions between the European Commission and the United States Government*, ¶ 1, 5092/98/EN/final, WP 15 (Jan. 26, 1999), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1999/wp15en.pdf.

18. *See* Caitlin Friedemann, *Council Decision Regarding Agreement Between the European Community and the United States on the Use of Passenger Name Record Data*, 11 COLUM. J. EUR. L. 207 (2004/2005) (discussing the regulatory

provisional agreement in May 2004, in which the European Commission, likely submitting to political pressure and without the support of the European Parliament, declared that U.S. data privacy laws could be considered "adequate" for the purposes of protecting the transfer of airline data and subsequent data collection by U.S. authorities.[19] However, following protests by the European Parliament and a subsequent legal challenge to its validity, this agreement was held to be null and void by the European Court of Justice. In July 2007, a revised agreement was concluded to ensure that U.S. authorities agreed to conditions for protecting data gathered from EU airlines.[20]

The July 2007 agreement between the U.S. and the EU (the "PNR Agreement") permits the transfer of airline data on the basis of assurances given by the Department of Homeland Security for the processing and handling of such data.[21] Accordingly, it has been agreed that the data shall be used and shared for limited, defined purposes, i.e., "combating: (1) terrorism and related crimes; (2) other serious crimes . . . that are transitional in nature; and (3) flight from warrants or custody."[22] The PNR data may also be used "where necessary for the protection of the vital interests of the data subject or other persons, or in any criminal judicial proceedings, or as otherwise required by law."[23] Sharing of PNR data between law enforcement and intelligence bodies may be undertaken only on a limited and proportionate basis.[24] Moreover, the transfer of the data

---

and legislative developments).

19. *See id.*

20. *See* Council Decision 2007/551, 2007 O.J. (L 204) 16 (EU); *see also* Franziska Boehm, *Confusing Fundamental Rights Protection in Europe: Loopholes in Europe's Fundamental Rights Protection Exemplified on European Data Protection Rules* (Univ. of Luxembourg Faculty of Law, Econ. and Fin., Law Working Paper Series, Paper No. 2009-01), *available at* http://ssrn.com/abstract=1348472.

21. *See* Council Decision 2007/551, *supra* note 20.

22. Letter from Michael Chertoff, Sec'y of Homeland Sec., to Luis Amado, President of the European Council, regarding DHS Policies on the Processing and Transfer of Passenger Name Record (PNR) Data by Air Carriers (July 23, 2007) § I, *available at* https://www.dhs.gov/xlibrary/assets/pnr-2007agreement-usltrtoeu.pdf.

23. *Id.*

24. *See id.* § II.

to third-party countries may, with the exception of emergency cases, only be carried out after determining the reasons for requesting such access and on assurances that such data will be adequately protected.[25] Further, sensitive data (disclosing, *inter alia*, religious beliefs or ethnic origins, political and philosophical beliefs) is filtered and not retained, unless the data is required for an exceptional use.[26] The filtered PNR data collected by the U.S. can be retained for an initial period of seven years, after which, it may be accessed only with special permission.[27] Under the agreement, the Department of Homeland Security may electronically access the airline databases within the European Union in advance of the airlines transfering the data to the U.S.[28] The agreement underscores the importance of a "push" system, whereby the data transferred to the U.S. is filtered for appropriateness, rather than a "pull" system (which may still be operated until such time as airlines can use "push" technology) that absorbs all data before filtering it.[29]

2. SWIFT and the Transfer of Financial Data

SWIFT provides messaging services between financial institutions for the transmission of data relating to financial transactions worldwide. Structured as a not-for-profit industry-owned co-operative under Belgian law,[30] SWIFT has a number of offices in countries around the world, including the U.S. It is overseen by a board of the world's major banks, including several central banks, such as the U.S. Federal Reserve, the Bank of

25. *See id.*

26. *Id.* § III.

27. *Id.* § VII.

28. *See* Agreement on the Processing and Transfer of Passenger Name Record (PNR) Data by Air Carriers to the United States Department of Homeland Security (DHS), U.S.-EU, July 26, 2007, https://www.dhs.gov/xlibrary/assets/pnr-2007agreement-usversion.pdf.

29. *See* Letter from Michael Chertoff to Luis Amado, *supra* note 22, § VIII (discussing "push" and "pull" systems in the context of PNR data transfers).

30. SWIFT – Governance at SWIFT, http://www.swift.com/about_swift/company_information/governance/governance_at_swift.page? (last visited Sept. 9, 2009).

England, the Bank of Japan and the European Central Bank.[31] SWIFT provides a routing mechanism for banking data, rather than operating as a bank and does not hold accounts.[32] It is estimated that SWIFT is responsible for providing messaging services for approximately six trillion dollars in financial transactions daily.[33]

In light of its importance to the worldwide banking infrastructure, the data held by SWIFT was considered by the C.I.A. and the U.S. Treasury to be a particularly valuable source of financial intelligence in U.S. counter-terrorism efforts.[34] SWIFT data had the potential to provide widespread international coverage as well as, if required, an understanding of the patterns of financial transactions taking place within U.S. borders.[35] *The New York Times* reported that U.S. intelligence authorities had initially considered taking action to monitor the SWIFT database in secret, but eventually chose to compel access to the database by serving SWIFT with broad administrative subpoenas under the U.S. Terrorist Finance Tracking Program ("TFTP").[36] The subpoenas served on SWIFT were reviewed only by U.S. Treasury officials, in consultation with the Justice Department, but were not reviewed by any judicial body.[37] Given SWIFT's nature as a bank messaging service rather than a bank, officials concluded that SWIFT did not benefit from protection under banking secrecy laws.[38] The subpoenas required that SWIFT provide the C.I.A. and the U.S. Treasury with specified financial records maintained by its U.S. operations center as collected in the course of its everyday

31. SWIFT – Oversight at SWIFT, http://www.swift.com/about_swift/company_information/governance/oversight_of_swift.page? (last visited Sept. 9, 2009).

32. SWIFT – Company Information, http://www.swift.com/about_swift/company_information/index.page?lang=en (last visited Sept. 9, 2009).

33. *See* Courtney Shea, Note, *A Need for Swift Change: The Struggle Between the European Union's Desire for Privacy in International Financial Transactions and the United States' Need for Security from Terrorists as Evidenced by the SWIFT Scandal*, 8 J. HIGH TECH. L. 143, 152-53 (2008).

34. *See* Lichtblau & Risen, *supra* note 2.

35. *See id.*

36. *See* Lichblau & Risen, *supra* note 2; Shea, *supra* note 33, at 151.

37. *See* Lichblau & Risen, *supra* note 2.

38. *See id.*

operations.[39]

Notwithstanding the status of SWIFT as a messaging service, the C.I.A. and U.S. Treasury subpoenas enabled access to information regarding the bank accounts and financial details of individuals and companies, including U.S. persons.[40] SWIFT data obtained under the program included identifying information on the payer and the payee of transactions, including their names, bank account numbers, addresses, national identification numbers and other personal data.[41] Whilst safeguards were said to have been put in place to limit undue monitoring of transactions relating to U.S. persons, as well as to limit the scope of surveillance to searches based on intelligence leads, the extent of the access may nevertheless be considered significant, particularly given the limited legal review to which the subpoenas had been subject.[42]

The EU Privacy Commission and the Belgian Data Privacy Commissioner's initial findings deemed SWIFT in breach of its data privacy obligations because it allowed U.S. authorities a disproportionate level of access and failed to inform the EU Privacy Commission and the Belgian Data Privacy Commission of its disclosures to the C.I.A and the U.S. Treasury.[43] The Article 29 Working Party, the EU's advisory body on matters relating to data privacy law, stated that "the hidden, systematic, massive and long-term transfer of personal data by SWIFT to the UST in a confidential, non-transparent and systematic manner for years constitutes a violation of the fundamental European principles as regards data protection and is not in accordance with Belgian and European law."[44] Indeed, the mere fact of having an operating

39. Notice: Publication of U.S./EU Exchange of Letters and Terrorist Finance Tracking Program Representations of the United States Department of the Treasury, 72 Fed. Reg. 60054, 60055 (Oct. 23, 2007) [hereinafter U.S./EU Exchange of Letters].

40. *See* Lichtblau & Risen, *supra* note 2.

41. *See* U.S./EU Exchange of Letters, 72 Fed. Reg. at 60057.

42. *See* Lichtblau & Risen, *supra* note 2.

43. *See* Jacobs, *supra* note 4, at 3.

44. Article 29 Data Prot. Working Party, *Opinion 10/2006 on the Processing of Personal Data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)*, at 26, 01935/06/EN, WP 128 (Nov. 22, 2006) [hereinafter Working Party, *Opinion 10/2006*], *available at* http://ec.europa.eu/

center in the U.S. could be considered a breach of data protection principles by placing SWIFT within the technical reach of U.S. subpoenas.[45] Indeed, the mere fact of having an operating center in the U.S. could be considered a breach of data protection principles by placing SWIFT within the technical reach of U.S. subpoenas.[46]

As with the PNR data, high-level political discussions culminated in an *ad hoc* compromise, which secured the conditions under which SWIFT could continue to provide access to its database. The compromise describes (i) the legal authority of the U.S. to issue subpoenas allowing for the collection and subsequent use of the data; (ii) arrangements for the handling and processing of the data, specifying that the data may only be used for the purposes of counter-terrorism, may only be handled by persons with designated authorized status to access and use SWIFT data, and must be stored under secure conditions; and (iii) provisions to review the arrangements in place and the appointment of an "eminent European" to conduct regular oversight of the arrangements.[47] However, the European Parliament recently voted to reject the compromise for failing to include sufficiently robust privacy and data protection guarantees.[48] Consequently, EU officials and the U.S. Treasury will need to negotiate another solution to share European bank transfer records. This turn of events is evidence of the continued tension between protecting civil liberties and security interests.

3. Implications for a Wider Solution

The PNR data and SWIFT cases highlight the practical implications of the incompatibility between the EU and U.S. data

---

justice_home/fsj/privacy/docs/wpdocs/2006/wp128_en.pdf.

45. *See id.* at 9.

46. *See Id.*

47. *See* U.S./EU Exchange of Letters, *supra* note 41, at 60058-63.

48. *See* EUROPA Press Release, The European Parliament Votes Against the EU-US Provisional Agreement on Transfer of Bank Data for Counter-Terrorism Purposes: Commission Reaction (Feb. 11, 2010), *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/152; see also Constant Brand, *MEPs Threaten to Derail EU-US Data-Transfer*, EUROPEANVOICE, Feb. 2, 2010, http://www.europeanvoice.com/article/meps-threaten-to-derail-eu-us-data-transfer-deal/67037.aspx.

protection laws and policies. In particular, the cases illustrate a largely reactive position adopted by both regulatory authorities. Notwithstanding the strategic importance of sound data collection in their counter-terrorism policies, the U.S. and the EU took remedial actions only after the issues were identified as politically and legally problematic.

Furthermore, the *ad hoc* solutions that were formulated are limited to the discrete problems they were designed to control. The solutions imposed a broad, negotiated legal and policy compromise, without establishing a detailed framework to manage different situations, or rules and principles for dealing with other categories of data that may necessitate regulation going forward.[49] While the urgency of each situation may have necessitated a speedy and expedient solution to ensure that otherwise "blameless" service providers, such as airlines and SWIFT, could continue to operate, the failure to arrive at a global response reflects an underlying unease at the EU level. Indeed, as detailed above, the SWIFT compromise now requires further discussions and re-negotiation between EU and U.S. authorities following its repudiation by the European Parliament. This unease is not only due to the divergence in approaches to data privacy regulation by the U.S. and the EU, but is also a result of the tenor of U.S. national security laws and policies, and the potential impact such measures have on the protection afforded to EU data abroad.

Indeed, as set out above, the Article 29 Working Party condemned the transfer of data by SWIFT to the U.S. in very strong terms.[50] The Working Party's criticism is further echoed by experts. By way of illustration, expert testimony before the Article 29 Working Party and the European Parliament's LIBE Committee on Civil Liberties, Justice and Home Affairs, contended that U.S. assurances on data protection could be circumvented by using various legislative tools, such as national security letters or court orders, that are available to intelligence agencies.[51] These orders

49. There are, however, proposals for creating such principles. *See* discussion *infra* Part III.

50. *See* Working Party, *Opinion 10/2006*, *supra* note 44.

51. *See* Written Testimony of Edward Hasbrouck, The Identity Project, before the LIBE Comm. of the European Parliament and the Art. 29 Working Party,

would not have to be disclosed to the database operators, or airlines, for reasons of national security; furthermore, they may also be unreviewable under the "state secrets privilege."[52]

In light of the practical difficulties of checking compliance with, and enforcing the terms of, agreements involving U.S. intelligence agencies, the EU has instead chosen to grant the U.S. access only to limited types of data (e.g., PNR data, SWIFT's database). This approach permits the EU to retain political leverage and control over access to other types of data, including the vast databases containing personal information such as credit card usage, Internet searches, employment history and the like. On the one hand, such leverage may enable the EU to exert some influence in the evolution of the U.S. data privacy framework. On the other hand, this creates legal uncertainty for service providers and individuals whose data may be at risk. In any event, in the absence of a jointly negotiated solution, the U.S. can unilaterally engage individual countries for access to data[53] in addition to pursuing access through secret administrative subpoenas when service providers are located within the U.S.

III. DATA PRIVACY LAW AND POLICY IN THE EU AND THE U.S.

1. Possible Reasons for Divergence

The cases discussed above reflect an underlying divergence in approach to data privacy and policy between the U.S. and the EU. Commentators have suggested that this outcome is puzzling, given that the evolution of data privacy law in both regions has taken

---

Transfers of PNR Data from the E.U. to the U.S. (Mar. 26, 2007), http://www.hasbrouck.org/IDP/IDP-PNR-26MAR2007.pdf.

52. *See id.*

53. The U.S. has been criticized for negotiating bilaterally with EU countries, formerly part of the Eastern bloc, which do not benefit from the U.S. visa waiver program. For example, the U.S. signed an accord with the Czech Republic granting visa waiver status to Czech travelers to the U.S., but demanded in return that additional registration forms be filled out. *See Current Affairs: New Agreement Paves Way for Visa-Free Travel to US for Czech Citizens* (Radio Praha radio broadcast Feb. 27, 2008), *available at* http://www.radio.cz/en/article/101320.

place on the basis of common principles.[54] In fact, by signing and ratifying the same multi lateral conventions, such as the 1980 Organization for Economic Co-operation and Development ("OECD") Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data, both regions even agreed to comply with the same principles regarding data privacy.[55] While the U.S. approach is necessarily shaped by the particularities of the federal structure, the EU has sought to adopt and implement a harmonized set of data privacy laws across the twenty-seven Member States, despite considerable differences in their constitutional make-up and regulatory and technological infrastructures.[56] It has been noted that the divergence may be attributable to sharp contrasts in basic cultural legacies.[57] While the EU prefers an approach geared toward harmonization (consistent with the basic jurisprudence underlying the development of the Internal Market within the EU) the U.S. seeks a more decentralized, self-regulatory model.[58]

Furthermore, the historical legacy of the Holocaust provides additional explanation for the differences in this area. The collective memory of the Holocaust marks Europeans as naturally more circumspect with respect to control of their personal data, since it had once been used for singling out members of the Jewish community for persecution.[59] Finally, some commentators identify a tendency within EU communities to place greater trust in central government than in corporations, whereas the opposite applies in the U.S.[60] This tendency within the U.S. leads to a more pronounced emphasis on industry self-regulation, rather than on federal legislation, to control the flow and processing of personal

54. DOROTHEE HEISENBERG, NEGOTIATING PRIVACY: THE EUROPEAN UNION, THE UNITED STATES AND PERSONAL DATA PROTECTION 26 (2005).

55. *Id.* at 8.

56. *Id.* at 9.

57. *The Future of Money: Hearing Before the Subcomm. on Domestic and Int'l Monetary Policy of the H. Comm. on Banking and Fin. Services*, 104th Cong. 32-33 (1996) (statement of Dr. Alan F. Westin, Professor of Public Law and Gov't, Columbia Univ.).

58. *See id.*

59. *See* Bob Sullivan, *'La difference' is stark in EU, U.S. Privacy Laws*, MSNBC, Oct. 19, 2006, http://www.msnbc.msn.com/id/15221111/.

60. *See id.*

data.[61]

As such, while the core foundational principles may once have been the same, their transposition into and interaction with differing regulatory structures in the U.S. and the EU have created a divergent framework. In these two current systems, the normative balance among the different interests involved varies in emphasis. The explosive increase of information on the Internet, automated digital processing, and instantaneous transfers of data across the globe has brought these differences into sharper focus.[62] Furthermore, the differing levels of power granted to law enforcement and intelligence agencies under national security legislation impact the interpretation of data privacy laws and the extent to which privacy rights can be subverted in the interest of state security.

2. Overview of Approaches – European Union

It has been argued that the EU data privacy regime is premised on the primacy of a right to the privacy and proper processing of personal data.[63] Indeed, Directive 95/46 begins by stating that the European Union seeks to "protect [an individual's] right to privacy with respect to the processing of personal data."[64] The Directive may be seen as reflecting the principles set out in the 1948 Universal Declaration of Human Rights,[65] OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data,[66] the 1981 Council of Europe Convention for the Protection of

61. *See id.; see also* HEISENBERG, *supra* note 54, at 26-27, 39.

62. *See* PHILLIP B. HEYMANN AND JULIETTE N. KAYEMM, PROTECTING LIBERTY IN AN AGE OF TERROR 75 (2007).

63. *See* STEPHEN KABERA KARANJA, TRANSPARENCY AND PROPORTIONALITY IN THE SCHENGEN INFORMATION SYSTEM AND BORDER CONTROL CO-OPERATION 136 (2008).

64. *See* Council Directive 95/46, *supra* note 11, art. 1.1.

65. *See* KARANJA, *supra* note 63, at 262, 454.

66. *See* HEISENBERG, *supra* note 54, at 8. The Guidelines endorse eight principles to guide data privacy protection strategies: (1) limitations on data collection; (2) standards for data quality; (3) data purpose specifications; (4) limitations on the use of data; (5) reasonable security safeguard requirements; (6) disclosure of data retained; (7) the ability of an individual to correct inaccurate data; and (8) accountability for compliance for the holder of data. *See* KARANJA, *supra* note 63, at 135.

Individuals with regard to Automatic Processing of Personal Data,[67] as well as Article 8 of the European Convention on Human Rights, which enshrines a basic right of an individual to his private life.[68] The Directive, applying equally to public and private entities,[69] seeks to harmonize data privacy and processing rules and standards across the Member States for personal data.[70]

Directive 95/46 sets out strict conditions for the processing of personal data, so that the use of data is limited to "legitimate purposes and not further processed in a way incompatible with those purposes."[71] For example, personal data is to be processed only with the consent of the data subject, or in "compliance with a legal obligation."[72] The Directive also regulates the transfer of data to third-party countries, requiring that such countries provide an "adequate level of protection" for the data transferred.[73] Under Article 8, the processing of "sensitive" personal data, relating to the religious beliefs, ethnic origin, philosophical views, etc. of a data subject is severely restricted.[74] Articles 16 and 17 of the Directive require data controllers to safeguard the confidentiality of the data.[75] The Directive also prohibits "significant" decisions to be made based on data collected by controllers.[76]

Although, Article 13 of Directive 95/46 permits Member States to restrict the rights granted by this Directive, the scope is limited to purposes such as national security or public defense.[77] However, any such restriction must be a "necessary measure" for the purpose sought.[78] Accordingly, it has been determined that the scope of this exemption must be narrowly construed, and as suggested by the

67. *See* KARANJA, *supra* note 63, at 5 n.8.

68. *See id.* at 86, 135-36.

69. *See* Council Directive 95/46, *supra* note 11, art. 2(e)-(g).

70. *See id.* art. 30.1(a).

71. *Id.* art. 6.1(b).

72. *Id.* art. 7(a), (c).

73. *Id.* art. 25(1).

74. *Id.* art. 8.

75. *See id.* art. 16, 17.

76. *See id.* art. 15(1). This provision may be used in limiting the extent to which profiling is permissible on the basis of data gathered on an individual.

77. *See id.* art. 13(1).

78. *Id.*

words "necessary measure," limited to specific cases.[79] Article 13 is therefore unsuitable as a legal basis for the general surveillance of transferred data by U.S. intelligence authorities.

It is also worth noting that Directive 95/46 does not apply to data collected "outside the scope of [European] Community law," in addition to data collected in the course of operations directed toward defense, state security and criminal law activity of the state.[80] This state criminal law activity exemption falls mostly under the so-called Pillar III of the European Union; Pillar III deals with police and judicial cooperation in criminal matters such as terrorism.[81] However, with respect to PNR and SWIFT data (and, looking forward, presumably data collected by private agents, such as credit card companies and Internet service providers), it can be argued that such data was originally collected for purposes other than national security and law enforcement. This sort of data, such as air travel bookings and financial transactions, can easily be deemed to fall within the scope of Pillar I, and therefore, within the scope of the Directive. In any event, while the Directive does not apply to data collected expressly under Pillar III, on November 27, 2008 the EU approved a framework for regulating private data falling under Pillar III, which framework sets out principles for sharing police and judicial data among EU law enforcement agencies.[82] Under Article 13 of this framework, data transfers to third-party countries may only take place where, *inter alia*, the transmission of data is necessary for the "prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties" and the recipient country can guarantee an adequate level of protection for the data.[83] The civil liberties implications of transferring personal data on criminal and terrorist-related matters may require that the determination of "adequacy"

79. *See* Working Party, *Opinion 6/2002*, *supra* note 11, art. 29.

80. *See* Council Directive 95/46, *supra* note 11, art. 3(2).

81. EUROPA – Glossary – Pillars of the European Union, http://europa.eu/scadplus/glossary/eu_pillars_en.htm (last visited Oct. 8, 2009).

82. *See* Council Framework Decision 2008/977/JHA, Protection of Personal Data Processed in the Framework of Police and Judicial Cooperation in Criminal Matters, 2008 O.J. (L 350) 60 (EU).

83. *Id.* art. 13.

meet a higher threshold. On a related note, in the wake of September 11, 2001, the European Council agreed to authorize additional sharing of data between European agencies.[84] However, the scope of this sharing was restricted to the transfer of data on terrorism and terrorist financing, rather than any broader agreement to share wholesale databases between national authorities or to take unfiltered personal data across borders.[85]

Finally, there is some concern that any system applied to sharing data between the U.S. and EU must also be applied to intra-EU information exchange mechanisms.[86] Such a proposal may have the potential to further erode the limitations on the transfer of data set out in Directive 95/46.

3. Overview of Approaches – United States

By contrast, the U.S. does not provide an overarching legal framework for the protection of personal data.[87] Neither the U.S. Constitution[88] nor the Bill of Rights expressly recognizes a right to privacy, leaving its parameters to be formed incrementally through legal commentary,[89] case law, and specific sectoral legislation granting a right to privacy in certain areas, such as financial

84. *See* European Council, Conclusions and Plan of Action of the Extraordinary European Council Meeting on Sept. 21, 2001, SN 140/01, 2 (EU), *available at* http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/ec/140.en.pdf.

85. *See id.* at 2-3.

86. For an example involving PNR, see *Commission Proposal for a Council Framework Decision on the Use of Passenger Name Record (PNR) for Law Enforcement Purposes*, COM (2007) 654 final (Nov. 6, 2007), *available at* http://ec.europa.eu/commission_barroso/frattini/archive/COM%282007%29654%20EN.pdf.

87. *See* HEISENBERG, *supra* note 54, at 32.

88. In contrast, a number of state constitutions do recognize a right to privacy. *See* National Conference of State Legislatures, Privacy Protections in State Constitutions, http://www.ncsl.org/programs/lis/privacy/stateconstpriv03.htm (last visited Sept. 17, 2009) (consisting of the states Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina, and Washington).

89. In 1890, Judges Samuel Warren and Louis Brandeis argued for the creation of a "right to be left alone." Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1891). Substantiating the formulation, Professor Prosser identified four different components to the right in the context of tort law. William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960).

services and consumer reporting.[90] The U.S. Supreme Court, however, has broadly interpreted the Bill of Rights to include a "reasonable expectation of privacy" in the context of government surveillance, religious activity, political party membership and family relations.[91] Nevertheless, the Court has also held that this limited right does not extend to the transfer of personal data to third parties.[92]

The Privacy Act of 1974, an ostensibly wide-ranging piece of legislation, sets out a broad regime for federal agencies to implement fair information practices.[93] While the Act sets out five principles broadly reflecting the OECD Guidelines, the level of protection that it provides may have largely eroded through the application of broad exceptions and subsequent interpretations (e.g., personal data may be disclosed for "routine use").[94] In the aftermath of September 11, 2001, a number of federal bodies, such as the National Crime Information Center, have been exempted from the Act's provisions.[95] Crucially, the Privacy Act does not provide the opportunity for anyone other than U.S. citizens and permanent residents to seek redress for improper processing of their personal data held by federal agencies, which creates a sticking point in current negotiations between the EU and the U.S.[96]

---

90. *See, e.g.,* Fair Credit Reporting Act, 15 U.S.C. § 1681 (2006); Gramm-Leach-Bliley Act, 15 U.S.C. § 6801-09 (2006).

91. *See, e.g.,* Lawrence v. Texas., 539 U.S. 558, 578 (2003) (right to sexual privacy); Katz v. United States, 389 U.S. 347, 353 (1967) (right to private communications); Griswold v. Connecticut, 381 U.S. 479, 485-86 (1965) (right to marital privacy); NAACP v. Alabama, 357 U.S. 449, 462-63 (1958) (right to private associations). *But see* Paul v. Davis, 424 U.S. 693, 712 (1976) (no right to private, undisclosed arrest).

92. *See* United States v. Miller, 425 U.S. 435, 444-45 (1976) (holding that the right to privacy does not extend to subpoenaed bank records).

93. *See* 5 U.S.C. § 552 (2006). For an example of how the Department of Justice has implemented the Privacy Act, see Exemption of Federal Bureau of Investigation Systems - limited access, 28 C.F.R. § 16.96 (2003).

94. Richard. D. Rasmussen, *Is International Travel* Per Se *Suspicion Of Terrorism? The Dispute Between The United States and European Union Over Passenger Name Record Data Transfers*, 26 WISC. INT'L L.J. 551, 565 (2008).

95. *See* 28 C.F.R. § 16.96(g)(1).

96. *See Final Report by EU-US High Level Contact Group on Information Sharing and Privacy and Personal Data Protection*, Council Document 9831/08,

Accordingly, the U.S. federal court system provides a patchwork of protection, covering certain types of personal data (e.g., under the Fair Credit Reporting Act)[97] and with varying degrees of scrutiny. Notably, PNR data is not specifically recognized as a protected category of data under U.S. laws, and no provisions have been made specifically to restrict its transfer.[98]

Concurrently, a number of legislative measures were passed that cumulatively provide law enforcement and other government agencies considerably greater access to, and sharing of, personal data for surveillance purposes.[99] These measures further limited the extent of oversight and the review of actions taken in data collection for counter-terrorism purposes.[100] To reinforce this point, the Intelligence Reform and Terrorism Prevention Act was created with the explicit purpose of streamlining the collection and sharing of data within the U.S. intelligence infrastructure by promoting an "information sharing environment" that could be extended to areas of the private sector.[101]

4. Possible Significance of Divergences

While both the U.S. and the EU legal systems make some provision for a right to privacy in the case of personal data, and set out legal scenarios in which this right may be subverted to preserve national security, the balance struck diverges fairly markedly.

As set out in Part II, the EU legal regime is premised on the basic inviolability of personal data, so that any processing, transfer or use of such data must occur within codified and legislatively demarcated circumstances. A limitation of Directive 95/46 rights in

---

(May 28, 2008) [hereinafter *Final Report*], *available at* http://ec.europa.eu/justice_home/fsj/privacy/news/docs/report_02_07_08_en.pdf.

97. *See* Fair Credit Reporting Act, 15 U.S.C. § 1681 (2006).

98. *See Final Report*, *supra* note 96, at 3 (discussing EU-U.S. proposed data protection policies).

99. *See, e.g.*, 50 U.S.C. §§ 1861-63 (2006); Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

100. *See* 50 U.S.C. § 1030(g).

101. *See* Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638, 3665 (2004).

the interests of national security must be narrowly construed and handled on a case-by-case basis. While it has been noted that the demands created by the Directive are perceived as cumbersome for businesses,[102] the comprehensive protections provided by the Directive demonstrates a consciousness of the normatively protected position of personal data within the EU legislative framework. Therefore, the Directive's interaction with the U.S. legal system, where the right to privacy for personal data is more limited, may reasonably be assumed to be problematic.

The EU and U.S. legal systems may strike a different normative balance between the right to privacy and the right for the state to monitor, transfer, or retain data for national security reasons. This balance considers factors such as regulatory structure, cultural history, and popular perceptions on the role of government. However, the structure and jurisprudence of an international regime for data sharing for national security purposes is distinct from each of the systems that inform its creation. First, the international transfer of data to another country will likely necessitate a loss of regulatory oversight and control over the data for the transferring jurisdiction.[103] However, this loss may not automatically result in a corresponding gain of legal control to the transferee, because the data does not always relate to subjects and controllers within the transferee's jurisdiction. In addition, service providers that channel the data, such as airlines and SWIFT, may also be subject to a cross-jurisdictional regulatory regime if it is based in the jurisdiction of the transferor or another body. Accordingly, the full range of enforcement and regulatory oversight mechanisms generally available to domestic regulators is unlikely to apply to the international legal regime for the transfer and sharing of data.

Second, the transfer of personal data across borders is likely to add to existing domestic data reserves and thus significantly increase the volume of data that becomes subject to oversight by a transferee jurisdiction. The enforcement limitations of an international regime and the increased volume of data collection make a set of highly prescriptive and exacting standards for data

102. *See* HEISENBERG, *supra* note 54, at 31.

103. *See* Working Party, *Opinion 6/2002*, *supra* note 11, at 8.

protection difficult to implement practically. Concerns over less stringent standards for data transfer may be met with a stricter evidentiary threshold before data is transmitted and either full or partial access is granted.

Notwithstanding the diverging legal regimes, any transatlantic standard will require a new focus. While any consensus to identify the evidentiary thresholds and the level of protection to be provided on transfer may be politically challenging, the continuing global terrorist threat underscores its importance. Furthermore, the absence of codification may diminish the overall credibility of governments to protect their citizens' data in the long run, by placing private actors between conflicting legal regimes. The resulting uncertainty may give way to the possibility of governments acting unilaterally (and secretly) to obtain the desired data.

IV. NEXT STEPS

1. Current Proposal to Reach an EU-U.S. Agreement on Data Privacy

In June 2008, *The New York Times* reported that the U.S. and the EU were close to an agreement on the sharing of personal data between their respective governments for purposes of law enforcement and security.[104] The agreement could potentially provide the legal basis for the transfer of a number of categories of personal data, such as credit card records, Internet-browsing habits, travel, and financial records.[105] However, it seems that negotiations are far from complete. The EU-U.S. High Level Contact Group, an informal body formed to lay the groundwork for a potential resolution to the transatlantic data privacy issue, published a report setting out twelve principles to use as a basis for an accord on data privacy, and submitted this report to the EU-U.S. Summit in June 2008.[106]

---

104. *See* Charlie Savage, *US and Europe Near Accord on Privacy*, N.Y. TIMES, June 28, 2008, at A1.

105. *See id.*

106. *See Final Report, supra* note 96. These 12 principles are listed in Section 2(b): "1. Purpose Specification/Purpose Limitation; 2. Integrity/Data Quality; 3.

However, in addition to the twelve core principles, the report also sets out a number of areas of conflict with the potential to impede progress in this area. These conflicting areas range from the legal nature of the agreement (whether it should be binding, expounded as "soft law," or a political declaration) to the role of reciprocity. The areas identified are politically polarizing, reflecting the underlying normative divergence between the EU and U.S. legal systems.[107] For example, the office of the European Data Privacy Supervisor has observed considerable legal tension in the probable role of private entities in the transfer of information. Considering the role played by SWIFT and the airlines, European authorities have expressed concern about the role of private entities in any new data-sharing regime with public entities. Institutionalizing their position within an information sharing framework may have repercussions for the rest of the EU, where similar intra-EU exchange mechanisms may be demanded on the same terms as those agreed between the EU and the U.S. Thus, notions of privacy in data held by EU private entities become fairly meaningless. Also, any agreement may obscure the debate as to whether a regime should focus on regulating the collection of data from certain types of data controllers, or whether it should concentrate on collecting data generated for certain purposes.[108] It has also been suggested that private entities may be particularly susceptible to pressure exerted by governmental regulatory bodies (e.g., the SWIFT and PNR data cases), such that they may be more

---

Relevant and Necessary/Proportionality; 4. Information Security; 5. Special Categories of Personal Information (sensitive data); 6. Accountability; 7. Independent and Effective Oversight; 8. Individual Access and Rectification; 9. Transparency and Notice; 10. Redress; 11. Automated Individual Decisions; 12. Restrictions on Onward Transfers to Third Countries." *Id.* at 4.

107. *See id.* at 7. These areas are: "1. Consistency in private entities' obligations during data transfers; 2. Equivalent and reciprocal application of privacy and personal data protection law; 3. Preventing undue impact on relations with third countries; 4. Specific agreements regulating information exchanges and privacy and personal data protection; and 5. Issues related to the institutional framework of the EU and US." *Id.*

108. *See Opinion of the European Data Protection Supervisor on the Final Report by the EU-US High Level Contact Group on Information Sharing and Privacy and Personal Data Protection*, 2009 O.J. (C 128) 1, ¶¶ 21-22, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:128:0001:0012:EN:PDF.

amenable to going above and beyond a narrow construction of limitations set out in any agreement in dealing with regulatory bodies. Other points of conflict include ensuring effective avenues of redress for European citizens whose data may have been mishandled by U.S. authorities,[109] definitional uncertainty regarding the use of terms such as "law enforcement," or "public security,"[110] and uncertainty regarding legal assessments of "adequacy" under EU law.[111]

2. Potential Risks with the Proposed Approach

Given the high policy importance of combating the terrorist threat through concerted action, and the strategic value of ensuring proper regulation of data collection to avoid a repeat of the SWIFT and PNR cases, progress made by EU and U.S. regulators toward an accord in this area may be seen as a positive step. Nevertheless, in addition to the areas of uncertainty identified by the High Level Contact Group report, a number of points may be made in respect of the current proposal.

First, while the final text of an agreement remains elusive, the current proposal and debate arguably conflate different types of data into a single category meriting an equal standard of protection. However, it would be more helpful to determine whether certain types of data require a higher standard of review before they are transferred or subject to surveillance. A hierarchy of protection is captured in the category of "sensitive data" in current legislation, but it may be worth considering whether other types of data should be included within a similar bracket. Examples include data pertaining to personal bank accounts, employment and tax information, and information relating to marriage or medical records. While such classifications may be considered arbitrary, this type of approach may be helpful in speeding up the processing and exchange of less sensitive and controversial information. When a category of information has been identified as requiring more robust review, requests from a transferee country/agency should

109. *See id.* ¶ 11.
110. *See id.* ¶ 25.
111. *See id.* ¶ 40.

provide a more substantive justification for the request. Furthermore, such categorization may focus the attention of agencies on the relative sensitivity of particular categories of information, such that information of a certain sensitivity is only requested in circumstances where its retrieval and use can be considered particularly probative.

Second, the tentative agreement appears to be framed by a list of principles on which the new regime is to be based. Although such principles may be seen as necessary to accommodate the divergent legal regimes in the U.S. and the EU, a list of principles may only be useful in providing a political "olive branch" to demonstrate accord between the two blocs, without adding any real substance to an international privacy standard for intelligence collection. Indeed, many of the principles set out in the report of the High Level Contact Group are already reflected to some extent in current legislation and arrangements for SWIFT and PNR data. However, in the absence of clarity on the interaction of the agreement with existing legal regimes, U.S. and EU national security provisions may override the principles. The broad wording of the principles[112] lends the agreement little legal weight. Although difficult to create, clear rules or best practice guidelines would provide more specific operational direction on the application of the principles. Moreover, given the difficulties likely to be faced in enforcing the international agreement, providing detailed rules or best practice guidelines may be more reassuring than relying on observance of principles. This would allow for a clearer way to measure observance of the terms of the agreement by authorities.

Finally, the language of the High Level Contact Group report and the opinion provided by the European Data Protection Supervisor appears to show considerable reluctance in relaxing the existing paradigms related to "adequacy" merely to assure a close fit between the two legal regimes. The creation of an international regime may require negotiating somewhere between the positions taken by each system, without necessarily adopting the architecture of one or the other. While this may be politically unpopular, the implications of failing to reach an accord may be particularly

112. *See Final Report, supra* note 96, at 4.

unpleasant for a number of actors, such as private parties holding the data and the data subjects whose rights may be circumvented through secret, unilateral action. As demonstrated by the case of the Czech Republic, the U.S. may seek to obtain data through bilateral agreements, thus undermining the negotiating position of the EU. It is not suggested that any accord reach for a "lowest common denominator" in protecting the privacy rights of citizens, but it may be helpful to relax assessments of "adequacy" while seeking to expound rules and guidelines that would provide measurable direction to agencies. Furthermore, an agreement may seek to set a high threshold of review before the data is transferred, due to the enforcement limitations of an international accord and the loss of post-transfer control. Unfortunately, as suggested earlier, the aggressive stance recently taken in the area of national security legislation and the apparent precedence given to executive action over the protection of civil liberties may have polarized the position of the EU in this area. It remains to be seen how progress in this area may evolve during the course of the Obama Administration.

IV. CONCLUSION

Current disparities between EU and U.S. laws on data privacy have led to considerable diplomatic and legal unease. Given the tremendous speed and volume of data creation in the digital age, the importance of establishing clear procedures to use such data optimally and lawfully against potential terrorist threats has never been greater. An examination of the current state of play in this area demonstrates the highly charged and politicized nature of the concepts of "data," "privacy," and "national security," such that agreement on how to approach data management does not appear feasible without a broad, overarching political agreement. However, as amply demonstrated by the legally ambiguous positions of European airlines and SWIFT, inaction in this area may lead to the greater danger of abandoning the interests of the very constituencies that regulators are seeking to protect. There is also the potential for opening the door to series of bilateral accords that circumvent EU institutions altogether. While the EU's robust approach to data privacy is laudable, some compromise may be necessary to move forward in establishing a transnational data

privacy framework. At the same time, a U.S. position that more protectively safeguards privacy rights may be beneficial in softening the hard edges of EU data privacy legislation. In light of the broader interests of security and economic prosperity, a proactive agreement, as opposed to reacting to the consequences of inaction, would be more beneficial to all.