American University International Law Review

Volume 22 | Issue 5 Article 3

2007

Enforcement of Social and Economic Rights

Albie Sachs

PERSONAL DATA PRIVACY TRADEOFFS AND HOW A SWEDISH CHURCH LADY, AUSTRIAN PUBLIC RADIO EMPLOYEES, AND TRANSATLANTIC AIR CARRIERS SHOW THAT EUROPE DOES NOT HAVE THE ANSWERS

EDWARD C. HARRIS*

---

* Visiting Assistant Professor, Chicago-Kent College of Law. I would like to thank Joel Reidenberg for a brief but thought-provoking conversation on the topic of this article. I would also like to extend my most heartfelt appreciation to all of my colleagues who provided thoughtful comments, suggestions and critiques, among them, Richard Warner, Doug Godfrey, Sanford Greenberg, Ron Staudt, Christopher Leslie, Graeme Dinwoodie, Hank Perritt, Mike Pardo (now at University of Alabama) and David Harris and Daniel Steinbock (both at the University of Toledo College of Law). My thanks also go out to my non-lawyer friends and loved ones who provided useful insights from the real world, among them, Margret Harris, Steve Sunner, Ciaran Cooper and Jonathan Rhodes.

I. INTRODUCTION

For several years, legal scholars, policy makers and the business community in the United States have been debating how the law should deal with privacy in personal information. Recent data security breaches in the United States, such as the data thefts at Choicepoint in 2004[1] and CardSystems in 2005[2], have heightened this debate. At the heart of the issue is the question of tradeoffs: do we want more privacy in our data and, as a consequence, less efficiency and higher costs in the flow of data in commerce? Will we tolerate less security as a result of heightened restrictions on the access to our personal data that might be useful in combating crime or terrorism? Thus far, the United States has protected personal data only in an ad hoc, sectoral manner, either regulating specific industries or specific types of information and then, only in reaction to specific data protection problems.[3] As the debate about where the tradeoffs should be made continues, some have looked to the European Union's very different comprehensive statutory approach to data protection through its Data Protection Directive for

1. *See* Tom Zeller Jr., *U.S. Settles with Company on Leak of Consumers' Data*, N.Y. TIMES, Jan. 27, 2006, at C3 (discussing the Federal Trade Commission's $15 million settlement with ChoicePoint, who allowed con artists disguised as lawful businesses to access the records of more than 160,000 consumers).

2. *See* Eric Dash & Tom Zeller Jr., *Mastercard Says 40 Million Files Are Put at Risk*, N.Y. TIMES, June 18, 2005, at A1 (reporting that CardSystems Solutions' security breach compromised over 40 million credit card accounts).

3. *See* Fair Credit Reporting Act of 1970, Pub. L. No.90-321, 15 U.S.C. §§ 1681 et seq. (governing the use of credit information in consumer credit decisions); Privacy Protection Act of 1980, Pub. L. No. 96-440, 42 U.S.C. §§ 2000aa et seq. (governing government access to journalist's work product); Cable Communications Policy Act of 1984, Pub L. No. 98-549, 47 U.S.C. § 551 (governing cable television providers' use of customer information); Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Pub. L. No. 104-191 § 262 (governing the use of personal medical data by health professionals and health insurance providers); Gramm-Leach- Bliley Act of 1999, Pub. L. No. 106-102 15 U.S.C. §§ 6801 et. seq. (governing the handling of financial data by financial institutions); Video Privacy Protection Act of 1988, Pub. L. No 100-618, 18 U.S.C. § 2710 (governing the privacy of video tape rental, purchase, and delivery information); Telephone Consumer Protection Act of 1991, Pub. L. No. 102-243, 47 U.S.C § 227 (governing telemarketers' use of certain consumer information).

guidance.[4] Some have suggested that the European approach might in certain respects serve as a model for a more comprehensive legislative approach to data protection in the United States.[5] This article posits that the European Data Protection Directive ("Directive") has not effectively made the tradeoffs that, on its face, it purports to make. By examining the Directive through the lens of the developing case law of the European Court of Justice ("ECJ") interpreting it, this article shows that the European model is unworkable in making the tradeoffs and is therefore an inappropriate model for any proposed U.S. comprehensive data protection regime. To this end, Part II of this article provides necessary background on the European Union in general and on the Directive in particular. This section will discuss the Directive's salient features, its chief policy objectives and its implementation by the E.U. Member States. Part III then analyzes the developing ECJ case law interpreting the Directive and, through the lens of the cases, discerns what the E.U.'s highest court has and has not done to effectuate the tradeoffs contemplated by the Directive between data privacy, on the one hand, and the free flow of data necessary for commerce and security on the other hand. Part IV discusses that the cases demonstrate that the Directive is an ineffective means for making the tradeoffs and thus Europe has not provided any kind of workable model to determine how much security and data flow should be sacrificed in

4. *See generally* Council Directive 95/46, arts. 1–34, 1995 O.J. (L 281) 31, 38–50 (EC).

5. *See, e.g.*, Marsha Cope Huie et al., *The Right to Privacy in Personal Data: The E.U. Prods the U.S. and Controversy Continues*, 9 TULSA J. COMP. & INT'L L. 391, 405 (2002) ("The sharp European contrast [on data protection] with the United States . . . invites serious study and even emulation"); Ryan Moshell, Comment, *...And Then There Was One: The Outlook for a Self-Regulatory United States Amidst a Global Trend Toward Comprehensive Data Protection*, 37 TEX. TECH L. REV. 357, 368–87 (2005) (suggesting that the United States needs comprehensive data protection legislation and identifying the European Union as one such model); Arnulf S. Gubitz, *The U.S. Aviation and Transportation Security Act of 2001 in Conflict with the E.U. Data Protection Laws: How Much Access to Airline Passenger Data Does the United States Need to Combat Terrorism?*, 39 NEW ENG. L. REV. 431, 472 (2005) (arguing that the United States should attempt to meet European Union standards by adopting stricter privacy standards); Kamaal Zaidi, Comment, *Harmonizing U.S.-E.U. Online Privacy Laws: Toward a U.S. Comprehensive Regime for the Protection of Personal Data*, 12 MICH. ST. J. INT'L L. 169, 171–76 (2003) (identifying the existing influences of the E.U. Directive on U.S. policy).

the name of data privacy. The European approach to data privacy should thus not serve as a model for any potential omnibus legislation in the United States. Finally, this last section posits several suggestions that might help U.S. law makers strike a more meaningful balance between data privacy and the societal necessity of access to personal data. But first, a little background about the current U.S. data protection situation:

On January 26, 2006, the Federal Trade Commission ("FTC") announced that it had reached a $15 million settlement in its action against U.S. data aggregator and brokerage firm ChoicePoint Inc.[6] The case stemmed from the company's February 2005 revelation that it had inadvertently sold sensitive personal data on about 145,000 consumers to phony companies set up by thieves to acquire the information.[7] The $15 million was apparently the largest civil penalty ever imposed by the FTC.[8] Before this incident, most Americans never even knew that ChoicePoint existed let alone that it was in the business of collecting all manner of data on all U.S. citizens. The ChoicePoint incident was hardly an isolated case. During the past two years, the United States has witnessed an unprecedented number of disclosures by private companies, government agencies and universities that they have somehow allowed the sensitive personal data of millions of Americans to get lost or end up in the wrong hands. The recent well-publicized data security breaches at CitiFinancial,[9] Reed Elsevier subsidiary LexisNexis,[10] Bank of America,[11] DSW Shoe Warehouse,[12]

6. *See* Zeller, *supra* note 1 (identifying $10 million in fines and $5 million in consumer compensation).

7. *See* William Sluis, *Choicepoint Hit by Identity-theft Scam; May Affect 145,000*, CHI. TRIB., Feb. 27, 2005, at Business 3 (reporting ChoicePoint's acknowledgement that the thieves set up fifty accounts and received a variety of consumer data, including names addresses, Social Security numbers, and credit reports).

8. *See* Zeller, *supra* note 1.

9. *See* Tom Zeller Jr., *U.P.S. Loses a Shipment of Citigroup Client Data*, N.Y. TIMES, June 7, 2005, at C1 (reporting that the United Parcel Service lost a box of CitiFinancial's computer tapes with information regarding 3.9 million consumers, but that investigators had failed to identify any theft or data compromise).

10. *See* Tom Zeller Jr., *Another Data Broker Reports a Breach*, N.Y. TIMES, Mar. 10, 2005, at C1 (discussing LexisNexis Group's report of a security breach in which thieves posing as subscribers acquired names, addresses, and Social Security numbers of roughly 30,000 people).

CardSystems,[13] University of California at Berkley[14] and the U.S. Department of Veterans Affairs[15] are a small sampling of incidences that were disclosed to the public in 2005 and 2006. The attention brought on by these data security breaches has largely exposed the previously hidden world of commercial data aggregators and prompted law makers to hold hearings and consider legislative proposals for increased protection of personal data.[16]

---

11. *See* David Wells & Holly Yeager, *Data on 1.2m BofA Customers Go Missing*, FIN. TIMES U.S.A., Feb. 26, 2005, at First Section 1 (following Bank of America's report of missing computer tapes containing personal information of 1.2 million government employees).

12. *See* Associated Press, *Theft Yields 1.4 Million Credit Card Numbers*, N.Y. TIMES, Apr. 19, 2005, at C3 (discussing the DSW Shoe Warehouse security breach where thieves acquired 1.4 million names and corresponding credit card numbers of customers).

13. *See* Dash & Zeller, *supra* note 2 (stating that the CardSystems security breach compromised about 20 million Visa accounts and 13.9 million MasterCard accounts).

14. *See* Ann McDonald, *Security Scramble: High-profile Security Breaches Are Prompting Calls for Stricter Regulations to Better Safeguard Consumer's Personal and Financial Information. What is the Industry's Response?*, COLLECTIONS & CREDIT RISK, May 2, 2005, at 28 (reporting the theft from a university office of a laptop computer containing personal information on nearly 100,000 alumni).

15. *See* David Stout & Tom Zeller Jr., *Vast Data Cache About Veterans Has Been Stolen*, N.Y. TIMES, May 23, 2006, at A1 (reporting the theft of roughly 26.5 million veterans' personal information from a Department of Veterans Affairs employee home).

16. *See* Evan Perez, *Identity Theft Puts Pressure on Data Sellers*, WALL ST. J., Feb 18, 2005, at B1 (noting multiple critiques of the self-regulating focused regime); Tom Zeller Jr., *Data Broker Executives Agree Security Laws May Be Needed*, N.Y. TIMES, Mar. 16, 2005, at C3 (reporting the agreement between ChoicePoint and LexisNexis that new legislation may be necessary to deal with identity theft and to clarify the rules governing data brokers' work); Jonathan Krim, *Parties Split on Data-Protection Bill*, WASH. POST, Nov. 4, 2005, at D4 (observing the partisan divides over a bill that requires consumer notification and security audits in the event of certain data breaches); Tom Zeller Jr., *Breach Points Up Flaws in Privacy Laws*, N.Y. TIMES, Feb. 24, 2005, at C1 (emphasizing the current "patchwork of sometimes conflicting state and federal rules that govern consumer privacy and commercial data vendors"); Michele Heller, *Raft of Bills on Data Security, But Little Clarity*, AM. BANKER, May 4, 2005, at 1 (observing the emergence of a large number of bills in response to public concern over data privacy, most of which will not survive deliberations); Jonathan Peterson, *U.S. Senate Panel Tackles Identity Theft*, L.A. TIMES, Mar. 11, 2005, at Business 1 (following various lawmakers' proposals for new legislation to include tougher security requirements, harsher penalties, and broader notification requirements);

In the United States, protection of personal data is currently governed by a patchwork of legislation that is applicable either to specific industry sectors or to specific types of information.[17] Gaps in protection are purportedly filled by a so-called "self regulatory" scheme.[18] In addition to this legislative patchwork and system of self-regulation, some states (most notably California in 2003) have passed statutes requiring companies to publicly disclose when data security breaches occur.[19] California's statute is credited with making Americans aware of the potential unauthorized exposure of their personal information.[20] This public awareness has given rise to a recent call for more comprehensive consumer protection for personal data.[21]

The national interest in a more comprehensive approach to regulating the use of personal data has naturally led scholars to examine the European approach to protection of personal data.[22] The

---

Byron Acohido & Jon Swartz, *Industry, Congress Develop Tactics to Reduce Online Risks*, U.S.A. TODAY, Nov. 3, 2005, at 2B (discussing how financial industry officials, regulators, and Congress have joined forces to respond to online security risks and balance convenience and security); *Digital Business: In the U.S.*, FIN. TIMES REP., Feb. 22, 2006, at Digital Business 3 (discussing several recent proposals for data privacy legislation in the United States).

17. *See supra* note 3.

18. *See* Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?*, 44 FED. COMM. L.J. 195, 208–09 (1992) (recognizing that, in addition to some ad hoc statutory protection for information privacy, various companies and industries have adopted self-regulatory schemes without individual legal enforcement mechanisms); Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1, 117 (contrasting U.S. efforts to enhance government surveillance capabilities while, at the same time, depending on private industry to advance individual privacy through self regulatory schemes).

19. *See* CAL. CIV. CODE § 1798.29(b) (2003) ("Any agency that maintains computerized data that includes personal information that the agency does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery . . . .").

20. *See, e.g.*, Marilyn Geewax, *ChoicePoint Scandal Driving Stricter Global Privacy Rules*, PALM BEACH POST, Apr. 9, 2005, at 2F (reporting that ChoicePoint was pressured to apply the California standards of disclosure to all affected consumers).

21. *See supra* note 16.

22. *See* Joel R. Reidenberg, *E-Commerce and Trans-Atlantic Privacy*, 38 HOUS. L. REV. 717, 748–49 (2001) (emphasizing the need to harmonize conflicting U.S.-E.U. information policies); Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STAN. L. REV. 1315, 1315

European Union has had comprehensive data protection legislation in place now for more than ten years (and some individual Member States have had it for much longer).[23] In 1995, two of the principal bodies of the European Union, the European Parliament and the European Council, jointly passed Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.[24] The Directive represents an approach to data protection that differs sharply from the ad hoc, sectoral and self-regulatory American approach and, instead, regulates both the public and private sector, and covers a broad range of actors and activities[25] The Directive required all E.U.

(2000) (arguing that "international cooperation" is "imperative for effective data protection in cyber-space"); Fred H. Cate, *The Changing Face of Privacy Protection in the European Union and the United States*, 33 IND. L. REV. 173, 230–31 (1999) (examining the differing approaches to privacy protection in the United States and the European Union and concluding that neither are adequate in the internet context); Steven R. Salbu, *The European Union Data Privacy Directive and International Relations*, 35 VAND. J. TRANSNAT'L L. 655, 665–70 (2002) (emphasizing that the study of underlying philosophical differences between U.S. and European information privacy laws is a valuable analytical policy tool); Stephen Hinde, *Privacy Legislation: A Comparison of the U.S. and European Approaches*, 22 J. COMPUTERS & SECURITY 378 (2003); *see also* Chuan Sun, *The European Union Privacy Directive and Its Impact on the U.S. Privacy Protection Policy: A Year 2003 Perspective*, 2 NW. J. TECH. & INTELL. PROP. 5, 3–5, 13–15 (2003) (examining the effect of E.U. data privacy practices on U.S. commerce practices); David Raj Nijhawan, Note, *The Emperor Has No Clothes: A Critique of Applying the European Union Approach to Privacy Regulation in the United States*, 56 VAND. L. REV. 939, 975–76 (2003) (concluding that traditional American privacy values prevent the implementation of a European approach in the United States).

23. *See generally* Council Directive 95/46, *supra* note 4, arts. 1–34, 1995 O.J. (L 281) at 38–50; *see also* Gubitz, *supra* note 5, at 434–37 (reviewing the development of E.U. data protection laws within broader international frameworks).

24. *See* Council Directive 95/46, *supra* note 4, art. 1, 1995 O.J. (L 281) at 38 (focusing on natural persons' "right to privacy with respect to the processing of personal data").

25. *Compare supra* note 3 (setting forth U.S. statutes addressing information privacy in specific contexts) *with* Council Directive 95/46, *supra* note 4, art. 2, 1995 O.J. (L 281) at 38 (defining "personal data" as "any information relating to an identified or identifiable person" and defining "processing" as "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or

Member States to pass by 1998 national legislation implementing the provisions of the Directive.[26]

To more fully understand the tradeoffs between data privacy and the free flow of data contemplated by the Directive, it is necessary to first have a brief look at some of the basics of the E.U. system and then some of the salient features and fundamental policy objectives of the Directive.

II. A PRIMER ON THE EUROPEAN UNION AND DIRECTIVE 95/46EC

The European Union consists of three principal bodies and its courts[27]: the Council of the European Union, often referred to as the Council of Ministers (the "Council"); the European Commission (the "Commission"); the European Parliament (the "Parliament"); the European Court of Justice with an attendant Court of First Instance; and the Court of Auditors.[28] As far as the law making function is concerned, as a general matter, laws are enacted in the European Union by the Council and often, but not always, together with the Parliament based on proposals sent to it by the Commission.[29]

---

destruction"). The Directive operates, in part, with respect to each "controller," "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data." *Id.*

26. *See* Council Directive 95/46, *supra* note 4, art. 32, 1995 O.J. (L 281) at 49 ("Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive at the latest at the end of a period of three years from the date of its adoption.").

27. *See* DIRECTORATE-GEN. FOR PRESS & COMMC'N, EUROPEAN COMM'N, HOW THE EUROPEAN UNION WORKS 3–4 (2006), *available at* http://ec.europa.eu/publications/booklets/eu_glance/53/2006-en.pdf (discussing the primary lawmaking E.U. bodies, as well as such institutions such as the Ombudsman and financial and advisory bodies).

28. *See id.* The Council of the European Union should not be confused with the European Council, which creates high level policy guidance at biannual meetings between certain member state leaders. *See* JOHN MCCORMICK, UNDERSTANDING THE EUROPEAN UNION 80 (3d ed. 2005).

29. *See* DIRECTORATE-GEN. FOR PRESS & COMMC'N, *supra* note 27, at 7–8 (describing the decision-making process of the European Union, where in most cases the European Commission proposes new legislation and the Council and Parliament pass the laws, a co-decision procedure giving the Parliament and the Council equal legislative power).

Procedures for enacting laws in the European Union are set forth in the foundational treaties and every piece of E.U. legislation must set forth a specific treaty provision as the "legal basis" for the legislation.[30] The three procedures for adopting legislation at the European level that are set forth in the foundational treaties are "consultation" "assent" and "co-decision" and they basically describe the manner in which the Parliament interacts with the Council and, more specifically, how much legislative power the Parliament shares with the Council.[31] Although the Parliament formerly had limited law making powers, it has managed to increase its power to enact legislation to a point where, in many legislative areas, it now stands on more or less equal footing with the Council.[32] Thus, the Commission sets the legislative agenda and the Council with some level of involvement of the Parliament enacts the law.[33]

It should be kept in mind that the European Union is not a federal system like the United States, but instead a union of sovereign states bound together by treaties under what has been called a system of "pooled sovereignty."[34] The system of pooled sovereignty in part explains the requirement that laws passed at the E.U. level must be based on a provision of one of the foundational treaties that demonstrates the European Union's competence to legislate in a given area.[35] Tied in with this point is the notion of the so-called

30. *See id.* (describing the legal basis requirement as a means of identifying relevant procedural requirements).

31. *See id.* The "consultation" procedure requires Parliamentary approval of Commission proposals, and allows Parliament to either reject a proposal or suggest amendments. *Id.* The "assent" procedure, which apples to certain "very important decisions," requires Parliamentary approval of Commission proposals, and allows Parliament to either reject or approve a proposal, but not to suggest amendments. *Id.* The "co-decision" procedure distributes legislative power equally between the Parliament and Council, and includes a "conciliation committee" designed to resolve differences over Commission proposals. *Id.*

32. *See* MCCORMICK, *supra* note 28, at 94 (following the Parliament's growing role in E.U. governance, including more power to amend laws and monitor the activities of other institutions).

33. *See generally* DIRECTORATE-GEN. FOR PRESS & COMMC'N, *supra* note 27, at 7–8 (discussing the decision-making process of the European Union).

34. *See id.* at 3 (explaining that "pooling sovereignty" involves delegating some state decision-making powers on matters of common interest to shared institutions to be made democratically).

35. The requirement to set forth a foundational treaty provision as the legal basis for legislation is also a demonstration of the amount of national sovereignty

"Three Pillars" in the structure of the European Union.[36] The three-pillar structure has its origins in the fact that European Union is really an international organization of sovereign states.[37] Each pillar more or less represents the level of competency that E.U. institutions may have in certain regulatory areas. The first pillar comprises economic union and concerns matters relating to the establishment and functioning of the single internal market, economic expansion and the four basic economic freedoms.[38] The second pillar involves matters of foreign and security policy; while the third pillar relates to matters of police and judicial cooperation in criminal matters among individual Member States.[39] Since the European Union was born out of the idea of a common market, the Member States have delegated considerable sovereignty to E.U. institutions in the area of internal market regulation.[40] With respect to the other two pillars, Member States were less willing to give up national sovereignty in areas of foreign policy, state security and criminal law.[41] Therefore, E.U. institutions are more restricted in regulating in these second and third pillar areas. This is not to say that E.U. governmental bodies cannot act in these areas; it just means that there are significant obstacles to

---

that Member States have delegated to E.U. institutions in particular subject areas.

36. *See* DIRECTORATE-GEN. FOR PRESS & COMMC'N, *supra* note 27, at 5 (tracing the development of the "Three Pillars" to the 1992 Maastricht Treaty on European Union).

37. *See id.* at 3 (observing that "the E.U. is not a federation like the United States. . . . The countries remain independent sovereign nations").

38. *See* PAUL B. STEPHAN ET AL., THE LAW AND ECONOMICS OF THE EUROPEAN UNION 14 (2003) ("[O]nly this pillar comprises truly supranational bodies with an institutional existence that is autonomous of the Member States."). The four economic freedoms, often referred to by the concept "freedom of movement," are the free movement of goods, people, services, and capital within the European Union's common market. *See* Robert F. Rick & Kelly R. Merrick, *Cross Border Health Care in the European Union: Challenges and Opportunities*, 23 J. CONTEMP. HEALTH L. & POL'Y 64, 74 (2006).

39. *See* STEPHAN ET AL., *supra* note 38, at 14–16 (explaining that the first pillar is the European Community, the second is the Common Foreign and Security Policy, and the third is police and judicial cooperation in criminal matters); *see also* DIRECTORATE-GEN. FOR PRESS & COMMC'N, *supra* note 27, at 5 (illustrating the three pillars).

40. *See* STEPHAN ET AL., *supra* note 38, at 14 (observing that only economic pillar created a "truly supranational body").

41. *See id.* (noting that these intergovernmental bodies preserve national sovereignty by requiring the consent of each member state before action is taken).

getting legislation passed at the European level when the European Union is required to use a second or third pillar basis for it.[42]

Once the proper basis for E.U. legislation is determined, the two main forms that legislation is likely to take in the European Union are regulations and directives.[43] A regulation on a specific subject has immediate and direct effect within the Member States whereas directives enunciate the main goals to be achieved by the legislation, but leave it to the individual Member States to best determine how to achieve the goals by their own national implementing legislation.[44] Directive 95/46/EC, as its designation suggests, was passed as the latter type of legislation.[45] While the Directive contains a reasonably specific framework detailing the protection to be afforded to individuals with respect to their personal data, the national governments of the Member States are required to pass their own implementing legislation to give effect to the Directive[46], and the national legislation must be in harmony with and be designed to achieve the objectives of the Directive.[47] The Directive is a first pillar

---

42. In fact, the Second and Third Pillar areas might be characterized more properly as agreement among the sovereign Member States to work in close cooperation rather than a grant of authority to E.U. institutions to regulate on behalf of the Member States. The institutions are more or less used to carry out the agreements struck among the Member States in these areas. *See generally* STEPHAN ET AL., *supra* note 38, at 14–16 (discussing the absence of a permanent institutional framework for cooperation in these two pillars).

43. *See* MCCORMICK, *supra* note 28, at 83 (outlining the five main forms of E.U. law: regulations, directives, decisions, recommendations and opinions).

44. *See id.*

45. Council Directive 95/46, *supra* note 4, 1995 O.J. (L 281).

46. *Id.* art. 32, 1995 O.J. (L 281) at 49 (directing the Member States to bring into force "laws, regulations and administrative provisions necessary to comply with the Directive"). Thus, even though legislative enactments at the E.U. level are ostensibly meant to harmonize the laws of the Member States (and further the aims of the common market), E.U. legislation in the form of a directive seeks also to preserve a measure of state sovereignty among the Member States by leaving it to each Member to decide how best to achieve the goals of a given directive. In spite of one of the main stated purposes behind the Directive being "to coordinate the laws of the Member States so as to ensure that the cross-border flow of personal data is regulated in a consistent manner," *Id.* pmbl. ¶ 8, 1995 O.J. (L 281) at 32, Member States can enact legislation to achieve this in differing ways.

47. *Compare* Bundesdatenschutzgesetz [BDSG] [Federal Data Protection Act], Jan. 14, 2003, BGBl. I at 66, last amended by Gesetz, Aug. 25, 2006, BGBl. I at 1970 (F.R.G.), *available at* http://www.bfdi.bund.de/cln_029/nn_946430/EN/DataProtectionActs/Artikel/Bun

E.U. law since it was passed on the basis of Article 95 of the Treaty of the European Community ("EC Treaty") which provides that "[t]he Council shall,... adopt the measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market."[48]

The preamble and Article 1 of the Directive state that the dual purposes of the Directive are to (1) provide citizens with protection of their fundamental right to privacy with respect to the processing of personal data and (2) ensure that free flow of data between Member States is not restricted or prohibited due to differing levels of protection afforded to personal data in the Member States.[49] The Directive thus seeks to balance the E.U. citizens' privacy interests in personal data against the public need for the flow of personal data; the Directive therefore seeks to tradeoff some level of data flow for data privacy.[50]

---

desdatenschutzgesetz-FederalDataProtectionAct,templateId=raw,property=publicationFile.pdf/Bundesdatenschutzgesetz-FederalDataProtectionAct.pdf (executing Germany's obligations under the Directive), *with* Law No. 2004-801 of Aug. 6, 2004, Journal Officiel de la République Française [J.O.] [Official Gazette of France], Aug. 7, 2004, p. 14063 (Fr.), *available at* http://www.cnil.fr/fileadmin/documents/uk/78-17VA.pdf (executing France's obligations under the Directive), *and* Upper House of the Dutch Parliament, *Personal Data Protection Act*, WWW http://www.dutchdpa.nl/downloads_wetten/wbp.pdf (consulted Mar. 22, 2007) (executing Holland's obligations under the Directive), *and* Data Protection Act, 1998, c. 29, § tbd (Eng.) (executing the United Kingdom's obligations under the Directive).

48. *See* Consolidated Version of the Treaty Establishing the European Community art. 95, *reprinted in* Consolidated Versions of the Treaty on European Union and of the Treaty Establishing the European Community, 2002 O.J. (C 325) 33, 369 (EC) [hereinafter E.C. Treaty]; *see also* Council Directive 95/46, *supra* note 4, pmbl., 1995 O.J. (L 281) at 32 (citing Article 100a of the E.C. Treaty, now renumbered as Article 95, as the basis on which the Directive was adopted); Treaty Establishing the European Community art. 100a, O.J. (C 340) 173, *available at* http://www.hri.org/docs/Rome57/Part3Title05.html#Art100a (demonstrating that Article 100a in the 1957 E.C. Treaty is the same language as Article 95 in the 2002 version of the E.C. Treaty).

49. Council Directive 95/46, *supra* note 4, pmbl. ¶¶ 3, 7, 8, 9, art. 1, 1995 O.J. (L 281) at 31–32, 38.

50. *Id.* pmbl. ¶ 3 (recognizing that while the "free movement of goods, persons, services, and capital" depends on the free flow of information, "fundamental rights of individuals should be safeguarded").

The Directive's broadly defined terms give it broad application. Among its key terms are "personal data," "processing of personal data" and "controller." The Directive applies to all "personal data" which is "any information relating to an identified or identifiable natural person" and "an identifiable person is one who can be identified, directly or indirectly, in particular or by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."[51] "Processing of personal data" is defined as "any operation or set of operations which is performed upon personal data, whether or not by automatic means" and the definition lists as examples "collection, recording, organization, storage, adaptation or alteration . . . use, disclosure by transmission, dissemination" as well as other processes.[52] The Directive applies to all "controllers" who are defined as "natural or legal person[s], public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data."[53] In defining the scope of the Directive, Article 3 states that it "shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system."[54]

Specifically excluded from the scope of the Directive is the processing of personal data that is done (1) in the course of activities falling outside the scope of European Community law, and activities relating to public and state security and criminal matters (i.e., typically second and third pillar matters) and (2) "by [a] natural person[] in the course of purely personal or household activity."[55] Thus, the Directive applies to a wide variety of personally identifiable information, it applies to both public and private sector actors, applies to a broad range of processing activities, but excludes activities generally related to public security or criminal matters and to household activities such as an individual keeping an address book.

---

51. *Id.* art. 2(a).
52. *Id.* art. 2(b).
53. *Id.* art. 2(d).
54. *Id.* art. 3(1).
55. *Id.* art. 3(2).

One scholar has identified eight basic principles in the Directive which demonstrate its far-reaching, individual rights centered and comprehensive approach.[56] These human rights centered principles as well as the competing goal of the Directive in ensuring that the

---

56. *See* Cate, *supra* note 22, at 185–86. First, the "Purpose Limitation Principle," *id.*, requires that personal data be collected only for "specified, explicit and legitimate purposes" and not used in ways that are inconsistent with those purposes or stored longer than necessary to accomplish those purposes. Council Directive 95/46, *supra* note 4, art. 6(1)(b), 1995 O.J. (L 281) at 40. Second, the "Data Quality Principle," Cate, *supra* note 22, at 185, requires that personal data be kept "accurate" and "up-to-date." Council Directive 95/46, *supra* note 4, art. 6(d), 1995 O.J. (L 281) at 40. Third, the "Data Security Principle," Cate, *supra* note 22, at 185, requires that appropriate measures be implemented to protect personal data from "accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access . . . and against all other unlawful forms of processing." Council Directive 95/46, *supra* note 4, art. 17(1), 1995 O.J. (L 281) at 43. Fourth, the "Special Protection for the Sensitive Data Principle," Cate, *supra* note 22, at 185, prohibits the processing of personal data "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and . . . data concerning the health or sex life" unless one of the enumerated exceptions applies. Council Directive 95/46, *supra* note 4, art. 8, 1995 O.J. (L 281) at 40. Fifth, the "Transparency Principle," Cate, *supra* note 22, at 185–86, requires that the data subject be informed of the fact that her data is being processed, who is doing the processing and for what purpose and provides for the data subject's right of access to the data and the ability to rectify erroneous data. Council Directive 95/46, *supra* note 4, pmbl. ¶ 38, arts. 10, 11,12, 1995 O.J. (L 281) at 35,40–41. Sixth, the "Data Transfers Principle," Cate, *supra* note 22, at 186, prohibits controllers from transferring personal data (which they are authorized to process) to third parties without first obtaining the consent of the data subject and prohibits the transfer of data across borders to third countries lacking an "adequate level of protection." Council Directive 95/46, *supra* note 4, pmbl. ¶¶ 34, 35, arts. 8(1)d, 14(b), 25(1), 1995 O.J. (L 281) at 34, 35, 41, 43, 45. Seventh, the "Independent Oversight Principle," Cate, *supra* note 22, at 186, is manifest through the supervisory authorities created in each Member State empowered to investigate and audit data processing activities and bring enforcement proceedings against non-compliant processors. Council Directive 95/46, *supra* note 4, art. 28 1995 O.J. (L 281) at 47. The Working Party set up by Article 29 also provides independent oversight in that it is empowered to render interpretations of the Directive. *Id.* art. 29, 1995 O.J. (L 281) at 48. Eighth, the "Individual Redress Principle," Cate, *supra* note 22, at 186, provides individuals with the right to access and demand erasure or correction of inaccurate data, the right to judicial remedies including damages awards against controllers and also obligates Member States to "lay down the sanctions to be imposed in case of infringement." Council Directive 95/46, *supra* note 4, arts. 6(d), 12, 22, 23, 24, 28, 1995 O.J. (L 281) at 40, 42, 45, 47. The supervisory authorities established by Article 28 may also hear claims brought by any person for a breach of obligations under the Directive. *Id.* art. 28 1995 O.J. (L 281) at 47.

free flow of data is not inhibited within the Union are enshrined in some of the Directive's most important provisions. In addition to Article 2's broad definitions of "personal data," "processing of personal data," and "controller" mentioned above,[57] Article 2 broadly defines what constitutes the "data subject's consent."[58] Article 6 enshrines the data quality principle by detailing the conditions in which the data must be maintained (e.g., kept "accurate," "up-to-date," "relevant" and "not excessive") and manner in which processing may take place.[59] Article 7 defines the criteria for making data processing legitimate, the most important of these criteria being when the data subject has provided "unambiguous[]... consent" to the processing.[60] Article 8 places special restrictions on the processing of certain special categories of data typically referred to as sensitive data.[61] Data such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership and data relating to health or sex life are considered to be particularly sensitive and worthy of a higher degree of protection.[62] Articles 10 and 11 detail the information that must be provided by the controller to the data subject about her data and its processing.[63] Article 12 provides for the data subject's somewhat qualified right to access her personal data and to demand erasure or correction of it.[64] Article 13 sets out the right of Member States to be exempt from certain of the provisions of the Directive when necessary for reasons of national or public security, defense, criminal matters, to protect an important economic interest.[65] Article 14 gives the data subject certain rights to object to the processing of her data.[66] Articles 22, 23, and 24 detail

57. Council Directive 95/46, *supra* note 4, art. 2, 1995 O.J. (L 281) at 38.

58. *See id.* art. 2(h), 1995 O.J. (L 281) at 39 ("[T]he data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.")

59. *Id.* art. 6, 1995 O.J. (L 281) at 40.

60. *Id.* art. 7, 1995 O.J. (L 281) at 40.

61. *Id.* art. 8, 1995 O.J. (L 281) at 40.

62. *Id.*

63. *Id.* arts. 10, 11, 1995 O.J. (L 281) at 41–42 (providing that, for example, the data subject must be provided with information regarding the identity of the controller, the processing purpose, and possible further recipients of the data).

64. *Id.* art. 12, 1995 O.J. (L 281) at 42.

65. *Id.* art. 13, 1995 O.J. (L 281) at 42.

66. *Id.* art. 14, 1995 O.J. (L 281) at 42–43.

the judicial remedies, liability and sanctions available for noncompliance with the Directive.[67] Finally, Article 25 deals with the transfer of data to third countries, i.e., non-E.U. Member States.[68] This provision specifically prohibits the transfer of data to third countries that do not provide an "adequate" level of protection.[69] Article 25 also specifies how the adequacy of protection in a third country is to be assessed, and that the Commission is to undertake this assessment and what can be done in light of the Commissions findings on adequacy.[70]

While the above rendition of the Directive's salient features suggests that the European legislators have determined precisely the point at which the tradeoff between privacy and free flow of data is to be made, the Directive's seemingly straightforward approach is deceptive. Two recent European Court of Justice decisions on the subject of the Directive illustrate that, when applied to real facts, the Directive cannot effectively make the tradeoffs it portends.[71]

Well, to be fair, there was a case decided on the subject of the Directive a few months prior to the first of the two case alluded to above.[72] This first ECJ case dealing with the Directive seemed to achieve the tradeoffs. But, this initial case was easy. Its facts involved the least tension between privacy and data flow. It is therefore briefly discussed here to provide a backdrop and to act as a foil for the latter two cases. The two subsequent (and more celebrated) cases involved facts that more clearly demonstrate the tensions between the competing goals of data privacy and data flow. The Court's formulaic and forced findings in the two latter cases expose the flaws in the Directive's capacity to effectuate the tradeoffs its language so clearly sets out.

---

67. *Id.* arts. 22, 23, 24, 1995 O.J. (L 281) at 45.
68. *Id.* art. 25, 1995 O.J. (L 281) at 45–46.
69. *Id.* art. 25(4), 1995 O.J. (L 281) at 46.
70. *Id.* art. 25, 1995 O.J. (L 281) at 45–46.
71. Case C-101/01, Lindqvist, 2003 E.C.R. I-12971, 1 C.M.L.R. 20 (2004); Joined Cases C-317 & 318/04, Eur. Parliament v. Council of the Eur. Union (*PNR*), 2006 E.C.R. I-4721, 3 C.M.L.R. 9 (2006).
72. Joined Cases C-465/00, C-138 & 139/01, Rechnungshof v. Rundfunk, 2003 E.C.R. I-4989, 3 C.M.L.R. 10 (2003).

III. THE ECJ CASES INTERPRETING THE DIRECTIVE

Each of the three ECJ cases provides a window through which to examine whether the Directive makes the appropriate tradeoff between data privacy and the free flow of data. The first two cases discussed below, *Rundfunk* and *Lindqvist*, relate primarily to the tradeoff between data privacy for individuals and the need for free flow of data in society for use by the public and commercial actors. The third case involves the tradeoff between data privacy and the free flow of data to public authorities for security purposes, for example, the use of personal data to track the movements of suspected criminals or terrorists. While *Rundfunk* shows how the tradeoffs under the Directive *should* work, the latter two cases which involve less straightforward circumstances illustrate that the broadly applicable tradeoffs contemplated by the language of the Directive cannot be realized in any practical way.

A. *RECHNUNGSHOF AND OTHERS V. ÖSTERREICHISCHER RUNDFUNK AND OTHERS*

Rundfunk evolved from two cases pending in Austrian national courts involving basically the same issues and which the ECJ consolidated for review.[73] The case involved the application of an Austrian statute that required certain public bodies that are subject to the control of the Rechnungshof (the Court of Auditors) to disclose salaries and pensions over a certain amount paid by the public bodies to employees and pensioners.[74] Along with the salary and pension information, the statute also required disclosure of the names of the persons receiving the remuneration.[75] The Court of Auditors was then to prepare an annual report that was to be transmitted to the upper and lower houses of the Austrian Federal Parliament and to the provincial assemblies and also made available to the general public.[76] Several public bodies subject to the statutory obligations (local and regional authorities, a public broadcasting corporation and a statutory

73. *Id.* at 285–86 (recounting the procedural posture of the case).
74. *Id.* at 286.
75. *Id.* at 287.
76. *Id.* at 286–87.

professional body) provided the Court of Auditors with less than full disclosure of the information.[77] These bodies either failed to communicate the data, communicated it in an anonymized form, or refused to give access to the information or made such access subject to conditions that the Court of Auditors was unwilling to accept.[78] The Court of Auditors then brought proceedings before the Austrian Federal Constitutional Court against the public bodies seeking a declaratory ruling that the Court of Auditors indeed has the jurisdiction to decide what information is to be disclosed.[79] The Austrian Constitutional Court recognized that the legislature's intent in making the salary and pension data public was to provide the general public with "comprehensive information" and that "... through this information, pressure is brought to bear on the bodies concerned to keep salaries at a low level, so that public funds are used thriftily, economically and efficiently."[80] The Constitutional Court also recognized, however, that the public disclosure of personal data involves important fundamental rights under Community law, namely, rights to protection of personal data under the Directive and right to respect for private life under the European Convention for the Protection of Human Rights and Fundamental Freedoms ("ECHR").[81] The Constitutional Court therefore stayed these proceedings and referred several questions to the ECJ for preliminary ruling.[82]

At roughly the same time as the above case was pending, two employees of Österreichischer Rundfunk ("ÖRF"), a public broadcasting company subject to the disclosure requirement, brought

77. *Id.* at 286, 289.
78. *Id.* at 289.
79. *Id.*
80. *Id.* at 287.
81. *Id.* at 288–90 (citing multiple provisions of the Directive, which imports standards from the Convention for the Protection of Human Rights and Fundamental Freedoms); *see* Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Nov. 4, 1950, Europ. T.S. No. 5 [hereinafter ECHR] (providing that "everyone has the right to respect for his private and family life, his home, and his correspondence," and that this right shall only be interfered with "in the interests of national security, public safety, or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others").
82. *See Rundfunk*, 3 C.M.L.R. at 290.

proceedings against their employer to prevent ÖRF from disclosing their salary information.[83] The highest regional court in Vienna determined that the Austrian statue was consistent with both fundamental rights to privacy and the Directive even where the statute requires the communication of the salary information along with the names of the recipients.[84] The employees appealed to the Austrian Supreme Court. That court also stayed the proceedings and referred essentially the same questions for a preliminary ruling to the ECJ as did the Austrian Federal Constitutional Court.[85]

In essence, the questions put before the ECJ were:

(1) Does the Directive even apply to the situations before the Court?

(2) Assuming that the Directive does apply, does it preclude national legislation of the sort at issue which requires certain public bodies to disclose personal information on salaries and pensions which includes the names of the recipients?

(3) If the answer to the above question is at least partially yes, are the provisions of the Directive that preclude the national legislation "directly applicable" in the sense that they may be directly relied on by individuals before national courts to oust the application of the precluded legislation?[86]

On the first question, the ECJ held that the Directive indeed applies to the processing of personal data as required by the Austrian legislation.[87] The Court found that the applicability of the Directive cannot rest on a cases-by-case determination of whether specific situations at issue have a sufficient link with the free movement

83. *See id.*

84. *See id.* at 291.

85. *See id.* at 290–91 (referring explicitly to the parallel proceedings).

86. *See id.* at 292, 294, 301 (asserting that, in order to answer the final two questions, the ECJ would first have to presuppose that the Directive is applicable in the proceedings, a disputed proposition in the proceedings).

87. *See id.* at 293–94.

within the European Union[88] i.e., a sufficient link with the functioning of internal European market, to justify the application of Community law instead of or in derogation of the law of an individual Member State.[89] The Court further found that the exceptions under Article 3(2)[90] (i.e., data processing done in connection with certain activities of the state or by individuals in the course of purely household activities) did not apply to exclude the situation from the scope of the Directive.[91]

On the second question, the ECJ held that the Directive does not preclude the national legislation at issue provided that it is shown that the wide disclosure requirements under the statute of not merely income amounts but also of names is necessary for and appropriate to the objective of proper management of public funds as contemplated by the Austrian legislature.[92] The Court, however, left it for the Austrian national courts to decide whether the disclosure requirements were necessary to achieve the legislature's objective.[93] In its analysis on this point, the ECJ also discussed at length the relationship between the Directive and provisions of the ECHR, specifically, Article 8's guarantee[94] of the respect for the private life

88. "Free movement" is a term that generally describes the unrestricted movement of goods, people, services and capital, etc., within the single, common, internal market of the European Community. *See* E.C. Treaty, *supra* note 48, art. 3(1)(c), 2002 O.J. (C 325) at 40; *see also* discussion *supra* note 38 (listing the four economic freedoms often referred to as the "freedom of movement" concept).

89. *See Rundfunk*, 3 C.M.L.R. at 293. Recall that the Directive was enacted on the basis of Article 95 of the EC Treaty, which has as its purpose the establishment and function of the internal market; therefore, the Directive is a First-Pillar market-related law. *See supra* note 48 and accompanying text.

90. *See* Council Directive 95/46, *supra* note 4, art. 3(2), 1995 O.J. (L 281) at 39.

91. *See Rundfunk*, 3 C.M.L.R. at 294 (finding that the processing of personal data at issue (1) did not concern the exercise of an activity outside the scope of Community Law, such as those found in Titles V and VI of the Treaty on European Union; and (2) did not concern public security, defense, State security, or State criminal law activities).

92. *See id.* at 301 (analyzing Articles 6(1)(c), 7(c), and 7(e) of the Directive).

93. *See id.* at 300 (noting the legislation's objective of keeping salaries within reasonable limitations).

94. *See* ECHR, *supra* note 81, art. 8 (guaranteeing everyone the right to "respect for his private and family life, his home, and his correspondence," and allowing only carefully limited interference by public authorities).

of the individual.[95] Here, the Court weighed the "existence of an interference with private life" against "a justification of the interference" and then determined that if the Austrian statute at issue was incompatible with ECHR Article 8's respect for private life, it must necessarily also be incompatible with the provisions of the Directive.[96] The ECJ then concluded that the above balancing test applies under the Directive.[97]

On the third issue, the ECJ determined that, although the Directive confers a certain amount of leeway in the implementation of some of its provisions, the provisions of the Directive[98] that were invoked in this case state unconditional obligations and therefore may be relied on by individuals in national courts to oust the application of national laws that are contrary to these provisions.[99] Thus, if on remand the Austrian courts were to determine that the disclosure requirements were not necessary to achieve the legislature's objectives, the

95. *See Rundfunk*, 3 C.M.L.R. at 297–300 (explaining that, before applying the applicable provisions of the Directive, the ECJ must first decide whether the legislation at issue interferes with private life, and if so, whether that interference is justified based on Article 8 of the ECHR).

96. *See id.* at 298–300 (remarking that the national courts will make the final determination on the compatibility of the legislation at issue with Article 8 of the ECHR).

97. *See id.* at 301 (holding that the national court must "interpret any provision of national law, as far as possible, in the light of the wording and purpose of the applicable directive").

98. *See id.* at 301–02 (referring to Articles 6(1)(c), 7(c) and 7(e)). Article 6(1)(c) of the Directive relates to data quality and states that "Member States shall provide that personal data must be . . . adequate, relevant and not excessive in relation to the purpose for which they are collected and/or further processed," and Articles 7(c) and (e) provide that "Member States shall provide that personal data may be processed only if . . . (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract . . . or (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed." *See* Council Directive 95/46, *supra* note 4, arts. 6(1)(c), 7(c), 7(e) 1995 O.J. (L 281) at 40.

99. *See Rundfunk*, 3 C.M.L.R. at 301–02 (ruling that, wherever the provisions of a directive appear to be "unconditional and sufficiently precise," they may "be relied on against any national provision which is incompatible with the directive or in so far as they define rights that individuals can assert against the State").

Directive could be relied on directly in a challenge to the Austrian legislation.[100]

The ECJ was thus reasonably successful in giving effect to the tradeoffs set out in the Directive by saying that the public disclosure of personal information is permissible under the Directive if it is necessary for the acknowledged legislative purpose.[101] The ECJ instructed the Austrian courts to balance the interests between data privacy and the free flow of data which is needed for an important economic purpose, namely ensuring the efficient use of public funds.[102] The ECJ's further instruction that the proper balance exists only if the disclosure is necessary and appropriate to achieving the stated legislative purpose would seem to dovetail perfectly with the aims of the Directive: protection of the rights of individuals with respect to their personal data and ensuring that the free flow of data is not unnecessarily inhibited.[103] Further, the Court's equating of the balancing of interests under the Directive with the balancing test under the ECHR seems to get at the core of the tradeoffs the E.U. legislators tried to establish in the Directive: the existence of an interference with private life should be balanced against important justifications of that interference.[104] *Rundfunk*, however, was the easy case. The interests at issue in *Rundfunk* make it reasonably easy to balance; a person's income can be considered relatively private information, but when there are compelling reasons for that information to be publicized, privacy should give way to the

100. *See id.* at 302.

101. *See id.* at 299 (finding the legislative purpose to be the maintaining of salaries "within reasonable limits" by guaranteeing "the thrifty and appropriate use of public funds," and defining "necessary" as involving a "pressing social need" where the measure employed is "proportionate to the legitimate aim pursued").

102. *See id.*

103. *See id.* at 300 (holding that the national courts can only conclude that the interference that results from the application of the legislation is justified under Article 8(2) of the ECHR if they find that disclosing the names of the employees is "necessary for and appropriate to the aim of keeping salaries within reasonable limits").

104. *See Rundfunk*, 3 C.M.L.R. at 300 (stating that, if national courts find, after conducting the balancing test of the ECHR, that the legislation is incompatible with Article 8 of the Convention, then they must find that the legislation is also incompatible with Articles 6(1)(c), 7(c), and 7(e) of the Directive).

compelling reasons.[105] The latter two cases present circumstances that are not so straightforward.

B. *BODIL LINDQVIST*

Only several months after its decision in *Rundfunk,* on November 6, 2003, the ECJ handed down its second and more comprehensive decision on the Directive in *Bodil Lindqvist.*[106] The case involved a website set up by Swedish volunteer catechist at a church in the parish of Alseda in Sweden.[107] The church lady, Ms. Bodil Lindqvist, after having recently taken a computer course, had set up a website using her home computer to assist parishioners in obtaining church-related information.[108] It is clear from the facts recited by the Court and from accounts in the press that Ms. Lindqvist put up the website with nothing but the good intention of helping her fellow parishioners get needed information, primarily in preparation for confirmation rituals.[109] She did it on her own time, using her own equipment and was not paid for the task.[110]

---

105. *See id.* at 301.

106. Case C-101/01, Lindqvist, 2003 E.C.R. I-12971, 1 C.M.L.R. 20, 673 (2004); *see also* Jacqueline Klosek, *European Court Establishes Broad Interpretation of Data Privacy Law*, METRO. CORP. COUNS., Mar. 2004, at 22 (providing a brief background on the Directive, a summary of the major facts, and the implications of the ECJ's decision); Dan Tench, *You Can't Print That: Thanks to European Privacy Rulings, the British Media May Find It Harder and Harder to Prove Stories and Images Are in the Public Interest*, GUARDIAN (London), Jan. 5, 2004, at Media 1 (arguing that the decision represents the forefront of a broader shift in European privacy protection soon to be applied to the British media); Andre Fiebig, *The First ECJ Interpretation of the Data Privacy Directive*, MONDAQ BUS. BRIEFING, Dec. 2, 2006, *available at* 2003 WLNR 10746524 (summarizing the case and interpreting its holdings); Andre Fiebig, EIU VIEWSWIRE SWEDEN, *Sweden Regulations: ECJ Rules on Data Privacy Directive Case*, Jan. 14, 2004, *available at* 2004 WLNR 13985779 [hereinafter Fiebig, *Sweden Regulations*].

107. *Lindqvist*, 1 C.M.L.R. at 681.

108. *Id.*

109. *Id.* at 686 (noting that Mrs. Lindqvist set up the website "without any intention of economic gain," only "as an ancillary activity to her volunteer work"); *see also* Tench, *supra* note 106 (stating that her efforts "seemed harmless" and that she removed the controversial material immediately upon complaint).

110. *Lindqvist*, 1 C.M.L.R. at 692.

On the site, the church lady included information about herself and information relating to about 18 of her colleagues at the church.[111] Although some of the church lady's colleagues were identified by only first names, in some cases last names were also used.[112] She also included other information about her colleagues such as their jobs and hobbies and in some cases family circumstances and telephone numbers were also posted.[113] In the case of one of her colleagues, the church lady also posted information about that person having injured her foot and that she was currently on half-time medical leave.[114] According to the Court, all of this information was conveyed in a "mildly humorous manner" and some news outlets reporting on the case had referred to the website as "gossip."[115] Apparently, Lindqvist did not discuss the postings with her colleagues or obtain their consent prior to posting the information.[116] Shortly after the site had been put up, Lindqvist heard that some of her colleagues were unhappy about it and she promptly removed it from the Internet.[117]

Although the website had been taken down almost immediately after her church colleagues had complained, the Swedish data protection authority brought charges against Mrs. Lindqvist under Paragraph 49(1)(b) through (d) of the Personuppgiftslagen[118], Sweden's national legislation implementing the Directive.[119] In fact, according to at least one media account, the church lady asked to be prosecuted by the Swedish authorities because she viewed the whole

111. *Id.* at 692.
112. *Id.*
113. *Id.*
114. *Id.*
115. *Id.*; Tench, *supra* note 106.
116. *Lindqvist*, 1 C.M.L.R. at 692 (adding that Mrs. Lindqvist did not notify the state supervisory authority responsible for protecting electronically transmitted data).
117. *Id.* at 692–93.
118. *Id.* at 693; *see* 1 § Personnupgiftslagen (SFS 1998:204) (providing that the purpose of the Personuppgiftslagen (Personal Data Act of 1998) is to "protect people against the violation of their personal integrity by processing of personal data").
119. *See Lindqvist*, 1 C.M.L.R. at 693 (stating that the public prosecutor charged Mrs. Lindqvist with a breach of the Personnupgiftslagen based on three different grounds).

situation as "Big Brother gone mad" and she "wanted to be a test case."[120]

Generally, the prosecution claimed that Linquist had (a) "processed personal data by automatic means without giving prior written notification" to the Data Protection Authority; (b) processed sensitive personal data (the information regarding her colleague's foot injury) without the consent of the data subject; and (c) "transferred processed personal data to a third country without authorisation."[121] In the Swedish District Court, Linquist accepted the facts but denied that she was guilty of any offense.[122] The court, however, found the church lady guilty and fined her SEK 4,000, currently the equivalent of roughly $540, and ordered her to pay an additional SEK 300 to a public fund for victims of crime.[123] Lindquist appealed the conviction to the appellate court in Jönköping, Sweden[124], and that court, being uncertain about the interpretation of European Community law applicable in this area (i.e., the Directive), stayed the appeal and referred seven questions on the Directive to the ECJ for interpretation.[125] Some of the seven questions were answered by the ECJ in its decision and some not.[126]

---

120. Peter Hitchens, *The Superstar Footballer, a Swedish Lady's Injured Foot . . . and a Sinister Threat to Our Freedom*, MAIL ON SUNDAY (U.K.), Jan. 11, 2004, at 54 (revealing that, according to her lawyer, Mrs. Lindqvist was "deeply upset," viewed the situation as "an infringement of her rights," did not expect to lose, and felt "like the victim of a medieval witchhunt rather than a member of an advanced European society").

121. *See Lindqvist*, 1 C.M.L.R. at 693

122. *See id.*

123. *See id.* (explaining that the District Court established the amount of the fine by multiplying a sum representing Mrs. Lindqvist's financial position (SEK 100), by a factor representing the severity of the offense (40)).

124. *See id.* at 682.

125. *Id.* at 693–94. The seven questions referred by the Swedish court to the ECJ were: (1) Whether the act of referring, on an internet home page, to various persons and identifying them by name or by other means, for example, by giving their phone numbers, working conditions or hobbies, constitutes the "processing of personal data wholly or partly by automatic means" within the meaning of Article 3(1) of the Directive; (2) If not, "can the act of setting up on an internet homepage separate pages for about 15 people with links between the pages which make it possible to search by first name" constitute the "processing otherwise than by automatic means of personal data which form part of a filing system within the meaning of Art. 3(1)" of the Directive; (3) If Mrs. Lindqvist's dealings were within the scope the Directive, whether they are covered by one of the exceptions in Article 3(2) of the Directive—i.e., activities that specifically fall outside the scope

For the purposes of this discussion on tradeoffs, only the Court's analyses on the third, fifth and sixth questions are relevant.[127] Questions one, two, four and seven, are relatively straightforward applications of definitional terms in the Directive or related to the harmonization of laws among Member States and are not directly relevant to this discussion on tradeoffs.[128]

On the third question, the Court held that none of the exceptions under Article 3(2) of the Directive apply to exempt the church lady's conduct.[129] As noted above, these exceptions basically fall into two categories: (1) processing activities that fall outside the scope of Community law (and Article 3(2) sets forth several categories of activities that are outside the scope of Community law) and (2)

---

of Community law and processing operations concerning public security, defense, State security, economic well-being of the State and activities of the State in areas of criminal law, and/or data processing done by natural persons in the course of a purely personal or household activity; (4) Whether an indication that a person has injured her foot and is working half-time on medical grounds constitutes data concerning health (one of several types of so-called "sensitive data") within the meaning of Article 8(1) of the Directive; (5) whether data has been "transfer[red] to a third country" within the meaning of Art 25 of the Directive by the act of loading personal data onto an internet site hosted in the same state but accessible to anyone who connects to the internet; (6) whether, as applied to these facts, the restrictions contained in the Directive regarding the processing of personal data conflict with the general principles of freedom of expression or other freedoms and rights, which are applicable within the European Union.; and (7) whether Member States may provide for greater protection of personal data or provide a broader scope of application under the national implementing the Directive than that called-for by the Directive itself. *Id.* at 693–94.

126. *See id.* at 695 (noting that the answer to question one eliminated the need to answer question two).

127. *Id.* at 695–704.

128. On question one, the ECJ found that Lindqvist's conduct with the information on her church colleagues did in fact constitute "processing of personal information" since the information and the conduct fell squarely within the definitions under Article 2 of the Directive. *Id.* at 695. No answer to question two was required since question one had been answered in the affirmative. *Id.* On question four, the ECJ had no trouble finding that Lindqvist's reference to her colleague's injured foot constituted sensitive personal (medical) data under Article 8 of the Directive. *Id.* at 698. Finally, on question seven, the Court held that the Directive does not merely provide for a minimal level of harmonization of the laws of Member States (i.e., a floor), but rather, "harmonization which is generally complete." *Id.* at 704. However, Member States are free to extend the scope of their own implementing legislation to areas not within the scope of the Directive, "provided that no other provision of Community law precludes it." *Id.* at 705.

129. *Id.* at 698.

processing of personal data "by a natural person in the course of a purely personal or household activity."[130] Taking the second category of exceptions first, the ECJ determined that Lindqvist's conduct did not fit within that category since her making available personal data regarding fellow church members and workers to the public on the Internet was not a purely personal or household activity such as keeping an address book or perhaps making a list of friends and family for invitations to an event.[131] Lindqvist's activities concerned a community-based organization and the information was designed to reach some portion of the members of that community.[132] For the Court, it did not seem that there was much that was "purely personal" or household-like about the church lady's activity.[133]

On the first category of exceptions, the ECJ found that the church lady's conduct did not fall outside the scope of Community law and therefore was not excluded from the scope of the Directive.[134] The church lady's argument that her conduct was in fact outside the scope of Community law was, however, a pretty straight forward one: since the European Union may legislate only strictly in accordance with the powers conferred upon it by the Member States through treaties[135], and because the Directive was based on Article 95 EC[136] the purpose of which is the approximation of laws within the Member States toward the establishment and functioning of the internal market[137], then Lindqvist's wholly charitable and non-economic conduct (which wouldn't seem to have much to do with the internal market and which is an exercise of her freedom of

130. Council Directive 95/46, *supra* note 4, art. 3(2), 1995 O.J. (L 281) at 281/39.

131. *Lindqvist*, 1 C.M.L.R. at 696. The Directive's preamble mentions "correspondence" as an activity that is "exclusively personal or domestic." Council Directive 95/46, *supra* note 4, pmbl. ¶ 12, 1995 O.J. (L 281) at 281/32.

132. *Lindqvist*, 1 C.M.L.R. at 692–93.

133. *Id.* at 698.

134. *Id.* at 696–98.

135. Recall that European legislation must be based on a foundational treaty provision. *See supra* note 30 and accompanying text.

136. *See supra* note 48 and accompanying text.

137. *See* Council Directive 95/46, *supra* note 4, pmbl. ¶ 8, 1995 O.J. (L 281) at 281/32 (arguing that the Community must coordinate the laws of the Member States to ensure that the flow of personal data is regulated in a consistent manner for the internal market).

expression) cannot fall within the scope of Community law.[138] In fact, the Swedish government also seemed to agree (or at least not disagree) with Lindqvist on this point when it submitted to the ECJ that it cannot rule out the possibility that the exception under Article 3(2) of the Directive might apply to situations "in which a natural person publishes personal data on an Internet page solely in the exercise of his freedom of expression and without any connection with a professional or commercial activity."[139] Interestingly, the ECJ's Advocate General[140] appointed to the case opined that, since Lindqvist's activities were wholly non-economic and had no direct connection with the functioning of the internal market, the data processing was "outside the scope of Community law within the meaning of Art. 3(2)..." and thus should not be subject to the Directive.[141]

The ECJ rejected Lindqvist's straightforward argument and held that the exception did not apply; the church lady's conduct did not qualify as an "activity which falls outside the scope of Community law."[142] The Court explained (as it had done in *Rundfunk*) that just because the Directive uses Article 95 EC as its foundational basis, that, by itself, does not presuppose that every situation where the Directive applies is actually linked with free movement[143] within the Union and to the establishment of the internal market.[144] The Court further explained that to find otherwise would make the field of application of the Directive uncertain and would thus be contrary to one of the essential objectives of the Directive: to approximate the laws of the Member States in order to eliminate obstacles to the functioning of the internal market which arise from disparate

138. *Lindqvist*, 1 C.M.L.R. at 695–97.
139. *Id.*
140. The ECJ is composed of twenty-seven judges and eight advocate generals who are responsible for assisting the court and presenting, "with complete impartiality and independence," an opinion to the court in the cases assigned to them. See The Court of Justice of the European Communities, http://curia.europa.eu/en/instit/presentationfr/index_cje.htm (last visited Mar. 12, 2007).
141. *Lindqvist*, 1 C.M.L.R. at 686.
142. *Id.* at 697–98.
143. *See supra* note 38 and accompanying text.
144. *Lindqvist*, 1 C.M.L.R. at 697–98.

national legislative regimes.[145] The Court also examined the specific activities mentioned in Article 3(2) that are considered outside the scope of Community law, i.e., activities provided for by Titles V and VI of the Treaty on the European Union,[146] "processing operations concerning public security, defense, State security and activities in areas of criminal law."[147] In saying that these examples are intended to define the scope of the Article 3(2) exception, the Court stated these are activities of the State and unrelated to the fields of activity of individuals and thus, Lindqvist's non-commercial, charitable activities could not be classified in the same category.[148] Therefore, even though the church lady's conduct had no relation to commercial or professional activity, was carried out for charitable purposes, was an exercise of her right of free expression, and, in any event, would not seem to have any effect on the functioning of the internal market, the conduct was still within the scope of Community law and thus subject to the Directive.[149]

Probably, the most peculiar aspect of the ECJ's decision in *Lindqvist* concerns its analysis of the fifth question: whether the church lady's publication of the personal data on an Internet page constitutes a transfer of personal data to third countries lacking "adequate protection" as prohibited under Article 25 of the Directive.[150]

---

145. *Id.* at 697.

146. *See* Consolidated Version of the Treaty on European Union art. 11-42, *reprinted in* Consolidated Versions of the Treaty on European Union and of the Treaty Establishing the European Community, 2002 O.J. (C 325) 1, 13-28 (E.U.) [E.U. Treaty].

147. *Lindqvist*, 1 C.M.L.R. at 697–98.

148. *Id.*

149. *Id.*

150. *Id.* at 698–701; *see also* Council Directive 95/46, *supra* note 4, art. 25, 1995 O.J. (L 281) at 281/45. Immediately after its passage, Article 25 was the subject of considerable controversy because the United States had been designated by the European Commission as a country lacking "adequate protection" for personal data. Such a designation created the potential for very difficult legal consequences for the corporations collecting personal data on European citizens and transferring the data into the United States. In 2000, the European Commission agreed to exempt from enforcement of the Directive those U.S. companies that complied with data protection standards negotiated by the U.S. Department of Commerce and other agencies. *See* Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45,666 (July 24, 2000); Commission Decision 2000/520, art. 1, 2000 O.J. (L 215) 7 (EC). The so-called

Specifically, this question presupposes that the Internet page is hosted by an Internet service provider ("ISP") located in an E.U. Member State and that the information is accessible by anyone who connects to the Internet including persons in non-E.U. Member States.[151]

The Court determined that no transfer to a third country had taken place under the described circumstances.[152] The Court reasoned that it must account for both the practical and technical nature of Internet operation and the purposes of Chapter IV of the Directive[153] (the chapter containing Article 25).[154] On the nature of the Internet, the Court acknowledged that information on the Internet "... can be consulted by an indefinite number of people living in many places at almost any time."[155] The Court further acknowledged that the procedures for posting information on the Internet that were available to people like Lindqvist at the time she had created her site

---

"Safe Harbor Agreement" actually consists principally of the communications from the U.S. Department of Commerce to the European Commission of July 21, 2000 and from the European Commission back to the U.S. Department of Commerce on July 28, 2000.

151. *Lindqvist*, 1 C.M.L.R. at 698. The Swedish appellate court had also asked if the result would change if no one from a third country had, in fact, accessed the information or the server where the Internet page was stored was physically located in a third-country. *Id.* at 694. Since the Court had determined that no transfer of data to a third country had taken place, it declined to provide any answers to these other factual variations. *Id.* at 699–701. Several interested parties filed submissions on this question. The Swedish Government and the E.U. Commission considered that merely making such information accessible via the Internet constitutes a transfer to third counties under Article 25 regardless of whether the page is in fact accessed by anyone in a third country and regardless of whether or not the server on which the information is stored is physically located in a third country. *Id.* at 699. The Netherlands Government took the view that, since "transfer" is undefined by the Directive, it must mean only intentional transferring and that because no distinction can be made between means of third party access, loading personal data on to an Internet page cannot constitute transferring the data to a third country under Article 25. *Id.* Finally, the United Kingdom submitted that Article 25 concerns *transfer* of data to third countries and not accessibility to the data. "[T]ransfer," according to the UK, connotes "the transmission of personal data from one place and person to another place and person." *Id.* (emphasis added).

152. *Id.* at 701.

153. Council Directive 95/46, *supra* note 4, art. 25, 1995 O.J. (L 281) at 281/45–46.

154. *Lindqvist*, 1 C.M.L.R. at 699.

155. *Id.*

involved transmitting the data to the ISP who manages the computer infrastructure needed to store the data and connect the server hosting the site to the Internet.[156] This allows the data to be transmitted to anyone who connects to the Internet and seeks access to it.[157] From this brief explanation the Court concluded that under these circumstances, where personal data appear on a computer in a third country, coming from a person who has loaded them in the European Union onto an Internet site, no direct transfer of data has occurred between the two people but, instead, the transfer has taken place through the infrastructure and the ISPs.[158] The Court then took pains to stress that the conduct under scrutiny was not that of the ISPs, but that of Lindqvist, the person who created the webpage and transferred the data to an ISP for hosting.[159]

The Court went on to say that Chapter IV of the Directive regarding transfers to third countries contains no reference to the Internet[160] and, given how the Internet operates and the absence of any criteria governing the Internet and third country transfers, in the Directive, "one cannot presume that the Community legislature intended the expression transfer [of data] to a third country to cover the loading... of data onto an Internet page, even if those data are thereby made accessible to persons in third countries."[161] Further, the Court stated that if Article 25 were interpreted to mean that there is a transfer of personal data to third countries every time personal data were loaded onto an Internet page, the special regime created by Article 25 to deal with third county transfers would become "a regime of general application" dealing with the Internet.[162] Thus, if even a single country were found to lack adequate protection and where persons within that country had the technical means to access the Internet, Member States would be "obliged to prevent any personal data from being loaded onto the internet" so that it could not

156. *Id.*
157. *Id.* at 700.
158. *Id.*
159. *Id.*
160. *Id.*
161. *Id.* at 700–01.
162. *Id.* at 701. *See generally* Council Directive 95/46, *supra* note 4, art. 25, 1995 O.J. (L 281) at 281/45–46.

be accessed.[163] Therefore, notwithstanding that the personal data of E.U. citizens can end up in a third country lacking adequate protection, the ECJ declined to find that posting the data on the Internet constitutes a transfer to a third country.[164]

The sixth question put to the ECJ was whether the restrictions in the Directive present a conflict with the general principles of freedom of expression applicable in the European Union.[165] The Court said that the provisions in the Directive do not inherently bring about restrictions that conflict with the general principles of freedom of expression and it is for the national authorities to balance the competing interests between data privacy and freedom of expression.[166] The Court reasoned that, on its face, the Directive recognizes that its provisions are meant to harmonize national laws on data protection for both securing the free flow of data within the European Union and protecting the rights of individuals in their personal data and that there may likely be a tension between these twin objectives.[167] In spite of recognizing the tradeoff that must be made, the Court did not give priority to one of these fundamental rights over the other in Lindqvist's case and left it for national authorities to strike the balance.[168]

C. THE PNR CASE

The most recent ECJ case to interpret the Directive is what has come to be known as the *PNR* case.[169] PNR stands for "passenger name record" and consists of information collected for the automated reservation and departure control systems of commercial airlines and which relates to individual passengers.[170] In the context of this ECJ case, the PNR data specifically related to 34 data fields on passengers including, among other items, names, addresses, telephone numbers, e-mail addresses, payment and credit card

163. *Lindqvist*, 1 C.M.L.R.at 701.
164. *Id.* at 700–01.
165. *Id.* at 701.
166. *Id.* at 703–04.
167. *Id.* at 702.
168. *Id.* at 703–04.
169. The *PNR* case actually consists of two cases that were heard together by the ECJ but retained separate case numbers. *See PNR*, 3 C.M.L.R. at 256, 309.
170. *PNR*, 3 C.M.L.R. at 319–20.

information, travel itinerary, "no show" history, one way ticket status, baggage and seat information, travel agency used, date of flight reservation and ticket issuance and travel status of passenger.[171] These data, in addition to other categories of data, are routinely collected by air carriers in the course of supplying air travel services to consumers.[172] The information can also be a valuable tool for governments as they seek to combat terrorism and other international crime by more closely monitoring who is entering and leaving the country and by tracking particular individuals.[173] Because of the usefulness of this data, the U.S. government began demanding the turn-over of the PNR data collected by air carriers.[174] It was in this context that the *PNR* case arose.

The *PNR* case consisted of two separate actions brought by the Parliament against each of the Council and the Commission for annulment of decisions reached by each of these E.U. bodies.[175] To understand the decisions reached by the Commission and the Council, some brief background is necessary.

Just after the September 11, 2001 terrorist attacks in the United States, the United States passed legislation requiring all air carriers operating flights to or from the United States or through U.S. territory to provide U.S. Customs and Border Protection ("CBP") with electronic access to all of the PNR data contained in their

---

171. *See* Commission Decision 2004/535, Attachment A, 2004 O.J. (L 235) at 22 (setting out the U.S. implementation of the Directive's Article 25 "adequate level of protection" requirements with respect to third state transfers); Undertakings of the Department of Homeland Security Bureau of Customs and Border Protection Regarding the Handling of Passenger Name Record Data, 69 Fed. Reg. 41,543, 41,547 (July 9, 2004).

172. *See, e.g.*, American Airlines, Privacy Policy, http://www.aa.com/aa/i18nForward.do?p=/footer/privacyPolicy.jsp, United Airlines, Privacy Policy, http://www.united.com/page/article/0,6722,1002,00.html?jumpLink=%2Fprivacy.

173. *See* Jeffrey W. Seifert, Congressional Research Service, DATA MINING AND HOMELAND SECURITY: AN OVERVIEW 5 (2007), *available at* http://www.fas.org/sgp/crs/homesec/RL31798.pdf.

174. *Id.* at 8–9.

175. Joined Cases C-317 & 318/04, Eur. Parliament v. Council of the Eur. Union (*PNR*), 2006 E.C.R. I-4721, 3 C.M.L.R. 9, 319–21 (2006). The Parliament's case against the Council was designated C-317/04 and its case against the Commission was designated C-318/04.

reservation and departure control systems.[176] In June 2002, the Commission, while recognizing the importance of the security interests at stake, informed the U.S. government that the U.S. legislation requiring access to PNR data could come into conflict with European law on the protection of personal data.[177] Although the U.S. authorities postponed the entry into force of the legislation until March 2003, from that point forward the CBP refused to waive the right to impose stiff penalties (or revoke landing privileges) against air carriers not in compliance with the legislation.[178] The European airlines were thus caught between a rock and a hard place: they could either provide the PNR data to the CBP and, at the same time, subject themselves to possible liability in the European Union for violations of data protection laws, or they could comply with the E.U. data protection laws and suffer penalties, risk having landing privileges revoked and experience major disruptions to their transatlantic service.[179] In March 2003, several large airlines in the European Union began providing the CBP with access to their PNR data.[180] Simultaneously, the Commission began negotiating with the U.S. authorities towards an eventual agreement that would alleviate the burden on the airlines by allowing the PNR data to be transferred and still respect E.U. data protection laws.[181] As a result of these negotiations, an agreement between the European Union and the United States on the sharing of the PNR data (the "Agreement") was reached.[182] While the Council approved of the conclusion of the Agreement, the Parliament was not pleased with the actions of either the Commission or the Council.[183]

---

176. *See* 49 U.S.C. § 44909(c)(3) (2006); 19 C.F.R. 122.49b(b) (Apr. 1, 2006).

177. *PNR*, 3 C.M.L.R. at 319–20.

178. *Id.* Under 19 C.F.R. 122.14(d), CBP can revoke landing rights and under 49 U.S.C. § 46301 CBP can impose a fine of $25,000 for each day that the failure to provide the PNR data continues. *See* 19 C.F.R. 122.49b(d) (Apr. 1, 2006); 49 U.S.C. § 46301(a) (2006).

179. *PNR*, 3 C.M.L.R. at 319–20.

180. *Id.*

181. *Id.* at 320.

182. *See U.S. Urges Global Commitment to Travel, Cargo, Standards and Technology*, ST. DEP'T PRESS RELEASES & DOCUMENTS, June 24, 2004, *available at* 2004 WLNR 2606867; Sara Kehaulani Goo, *E.U. Agrees to Give U.S. Airline Passenger Data*, TECHNEWS.COM, May 15, 2004, *available at* 2004 WLNR 16682947.

183. *See* Tobias Buck, *Legal Challenge Over Air Passenger Data*, FIN. TIMES

To summarize a complex and lengthy story, through the course of the negotiations with the U.S. authorities and the resulting U.S. agreement to undertakings regarding the handling of the PNR data, the Commission[184] eventually issued its decision on the adequacy of protection that would be afforded to the PNR data by U.S. authorities.[185]

Various exchanges took place between the Commission and the Parliament and the Council and the Parliament regarding the Commission's decision on adequacy and the Council's proposal for action in concluding the agreement with the United States.[186] Notwithstanding the Parliament's concern over the adequacy of protection of the PNR data in the United States and that neither the Commission nor the Council had the legal authority to act as they proposed to act, on May 14, 2004, the Commission approved its final Decision on Adequacy.[187] Then, on May 17, 2004, the Council approved the conclusion of the international agreement with the United States.[188] On July 27, 2004, the Parliament initiated proceedings in the ECJ against both the Commission and the Council to annul Commission's decision on adequacy and Council decision to approve the conclusion of an agreement with the United States.[189]

The Parliament made several arguments in support of annulment of each decision, some of which were based on privacy concerns.[190]

(London), July 31, 2004, at World News 7; *U.S./E.U./Air Transport: Parliament Refers Data Transfer Issue to the Court of Justice*, EUR. REP., June 26, 2004, *available at* 2004 WLNR 7310733; Daniel Dombey & Ralph Minder, *U.S.-E.U. Deal on Flight Data Leads to Dispute*, EIU VIEWSWIRE (E.U.), June 17, 2004, at 20.

184. *See PNR*, 3 C.M.L.R. at 320–21.

185. *See supra* note 68–70 and accompanying text. Under Article 25 of the Directive, the Commission has the responsibility of determining the "adequacy" of protection afforded personal data of E.U. citizens in non-E.U. countries. If the third country in question "adequately" protects personal data (perhaps even if only specific kinds of data), then a transfer of such data to the third country can take place; if there is no such adequate protection, then transfer of the data is prohibited.

186. *PNR*, 3 C.M.L.R. at 320–21.

187. *Id.* at 321.

188. *Id.*

189. *Id.*

190. On the Commission's decision on adequacy, the Parliament claimed that the Commission: (1) engaged in ultra vires action; (2) breached fundamental principles of the Directive; (3) breached fundamental rights; and, (4) breached the principle of proportionality. *PNR*, 3 C.M.L.R. at 321. On the Council's decision,

The Court, however, declined to entertain most of the Parliament's arguments and, instead, annulled both decisions on very narrow grounds.[191]

First, on the Commission's decision, the Court zeroed-in on the Parliament's argument that the Commission breached the Directive.[192] The Court determined that the Commission's actions could not have been validly adopted on the basis of the Directive since Article 3(2) of the Directive excludes from its scope the processing of personal data in the course of activities which fall outside Community law.[193] The processing of personal data in this case, according to the Court, constituted processing operations concerning public security and the activities of the State in the areas of criminal law which are expressly excluded from the scope of the Directive.[194] Thus, according to the Court, the Commission could not act on the basis of the Directive using its Article 25 powers to assess the adequacy of the level of protection afforded by the U.S. authorities for the PNR data since the Directive itself excludes such data processing activities from its scope.[195] Since the Court was able to annul the Commission's adequacy decision on this basis, it made no further determinations on the remaining arguments made by the Parliament.[196]

In its reasoning the Court drew a distinction between the data processing done by the airlines in the course of selling airline tickets and the data processing activities "regarded as necessary for safeguarding public security . . . ."[197] Further, the Court explained

---

the Parliament argued that the Council: (1) incorrectly used Article 95 of the Treaty of the European Communities ("EC") as the legal basis for the decision; (2) breached Article 300(3) of the EC; (3) breached Article 8 of the European Convention on Human Rights; (4) breached the principle of proportionality; (5) breached the requirement to "state reasons" (ostensibly to support its decision); and, (6) breached the principle of cooperation in good faith (ostensibly cooperation with the Parliament). *PNR*, 3 C.M.L.R. at 323.

191. *See PNR*, 3 C.M.L.R. at 322–23

192. *Id.* at 321–23.

193. *Id.* As mentioned in *Lindqvist*, Article 3(2) specifically excludes processing activities involving national security and criminal law. *See supra* notes 146–148 and accompanying text.

194. *PNR*, 3 C.M.L.R. at 322–23.

195. *Id.*

196. *Id.* at 323.

197. *Id.* at 322.

that, although it held in *Lindqvist* that the processing activities excepted from the scope of the Directive described in Article 3(2) are activities of the State and unrelated to the field of activities of individuals, this does not mean that the processing at issue in this case is not covered by Article 3(2).[198] "The transfer falls within a framework established by the public authorities that relates to public security."[199] So, even though in *Lindqvist* the ECJ carefully defined the processing activities referred to in the Article 3(2) exceptions as activities of the State (or of state authorities) and not related to the field of activities individuals, in *PNR,* the Court essentially placed the processing activities of private commercial actors (air carriers) and their transfer of data to a non E.U. country in the same category as State activity.[200]

Concerning the Council's decision approving the conclusion of the Agreement, the ECJ used a similar basis for its annulment.[201] This portion of the decision is even more devoid of discussion on privacy issues and therefore does not add much to the discussion here. Suffice it to say that the ECJ determined that Article 95 EC was the incorrect basis for the Council's decision to approve the conclusion of the Agreement with the U.S. authorities.[202] Basically, Article 95 EC represents one aspect of the first pillar powers of E.U. institutions.[203] Since, as was determined under the Court's analysis of the Commission's decision, the processing activities were done for purposes of law enforcement and public security (second and third pillar matters), the Council should have relied on a third pillar basis for its decision.[204] In a rather terse statement the Court stated, "[t]he Agreement relates to the same transfer of data as the decision on

198. *Id.* at 323; *see also Lindqvist*, 1 C.M.L.R. at 697–98.
199. *PNR*, 3 C.M.L.R. at 323.
200. *Id.* at 322–23.
201. *Id.* at 323–24.
202. *Id.*
203. Article 95(1) EC states "[t]he Council shall, . . . adopt the measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market." *See* E.C. Treaty, *supra* note 48, art. 95(1), 2002 O.J. (C 325) at 69.
204. *PNR*, 3 C.M.L.R. at 324 ("Article 95 EC, read in conjunction with Article 25 of the Directive, cannot justify Community competence to conclude the Agreement.").

adequacy and therefore to data processing operations which, as has been stated above, are excluded from the scope of the Directive.[205] Consequently, [the Council's] Decision... cannot have been validly adopted on the basis of Article 95 EC."[206]

Cognizant of the drastic impact on air carriers and transatlantic travel that its decision could have if it were to be immediately effective, the ECJ left the Commission's decision on adequacy (and also the Agreement) in effect until September 30, 2006.[207] The ECJ was apparently buying some time for the Commission and the Council to renegotiate the Agreement with the United States using a proper legal basis and also meeting the Parliament's approval.[208] In October 2006, the European Union and the United States in fact reached a second, but temporary, agreement on the sharing of PNR data.[209] In most substantive respects the agreement is the same as the one annulled by the ECJ and it will remain in place until July 2007.[210] This time, the European Union used an ostensibly proper basis for the agreement[211] and the European Union and the United States are in the process of negotiating a permanent agreement for the sharing of PNR data. However, this second temporary agreement does not seem to do much beyond preserving the status quo, and that,

---

205. *Id.*

206. *Id.*

207. *Id.*

208. *See* Nicola Clark & Matthew L. Wald, *Hurdle for U.S. In Getting Data on Passengers*, N.Y. TIMES, May 31, 2006 at A1 (quoting a U.S. diplomat's contention that "Washington would seek a diplomatic arrangement with the E.U. that respected the ruling without disrupting air travel").

209. *See* Sarah Laitner, *Brussels Agrees Pact Handing Details on Airline Passengers to U.S. Agencies*, FIN. TIMES (London), Oct. 7, 2006, at Europe 7; *Europeans Agree on Sharing Airline Passenger Data*, ST. DEP'T PRESS RELEASES AND DOCUMENTS, Oct. 6, 2006, *available at* 2006 WLNR 17427225.

210. The agreement is basically the same substantively because it binds the United States to the Undertakings—regarding handling of the personal data—that were part of the Agreement that the ECJ nullified. *See* Agreement Between the European Union and the United States of America on the Processing and Transfer of Passenger Name Record (PNR) Data by Air Carriers to the United States Department of Homeland Security, 2006 O.J. (L 298) 29, 29–30.

211. The Council Decision to approve the new temporary agreement with the United States specifically references Title V (foreign and security policy—second pillar) of the Treaty on the European Union as the foundational basis for the decision. *See* Council Decision 2006/729, pmbl., 2006 O.J. (L 298) 27, 27 (E.U.); E.C. Treaty, *supra* note 48, arts. 24, 38, O.J. (C 325) at 18, 26.

for only a short while. Since the conclusion of the new agreement, several ministers of the E.U. Parliament have continued to voice their dissatisfaction over the way the personal data of European air travelers will be handled by the United States and they insist that any future permanent agreement must meet European privacy standards.[212] Therefore, it seems unlikely that this new temporary agreement or any subsequent permanent one will be able to escape a legal challenge on privacy grounds. And, this time, the ECJ will not be able to use narrow technical means to avoid the larger questions of privacy.

IV. UNREALIZED TRADEOFFS

A. DATA PRIVACY VERSUS FREE FLOW OF DATA IN COMMERCE

The ECJ's holding in *Rundfunk* seems to do a pretty good job at realizing the data privacy versus the free flow of data tradeoffs as set out in the Directive. The ECJ examined the Austrian statute requiring public disclosure of the personal financial data of public employees to determine if the disclosure was warranted in light of an important public purpose.[213] This seems to be a reasonable and practical application of the Directive's general principles. Indeed, Articles 7 and 13 of the Directive provide exceptions for Member States to allow the processing of personal data when the processing is necessary for public interest purposes including economic interests,

---

212. *See E.U. Concern at Data Transfers*, BBC NEWS, Jan. 31, 2007, http://news.bbc.co.uk/2/hi/europe/6315893.stm (discussing the continued concerns of European officials, including one who noted that "[t]he right to privacy for me is non-negotiable"); *see also* Laitner, *supra* note 209 (quoting one Parliamentarian saying, "[i]t seems that the European Union has totally caved in to U.S. blackmail," and another calling the new temporary PNR agreement the "least worst option," saying that "[i]t seems clear . . . that the current American administration is determined to extract ever more personal data and share with the wider intelligence community."); Molly Moore, *Deal Reached on Fliers' Data: E.U. Will Share Info With U.S. – Some European Officials Skeptical*, SEATTLE TIMES, October 7, 2006, A4 (quoting a German Minister of the European Parliament who noted that "[t]he E.U. has once again caved in to the U.S. pressure at the expense of E.U. citizens' civil liberties").

213. *See* Joined Cases C-465/00, C-138 & 139/01, Rechnungshof v. Rundfunk, 2003 E.C.R. I-4989, 3 C.M.L.R. 10 (2003); *supra* Part III.A (discussing *Rundfunk*).

and as such, these provisions clearly express the tradeoff between data privacy and the free flow of data in commerce.[214] Further, the ECJ's equating of the balancing of the interests that must take place under the Directive to the balancing done pursuant to Article 8 of the ECHR (interference with private life versus a justification of the interference), also embodies the tradeoffs.[215] The ECJ's guidance to the Austrian court to conduct this balancing test looks to be what the framers of the Directive had in mind: the fundamental right of privacy should be weighed against important public interests that justify interference with that fundamental right.[216]

Perhaps the only thing amiss in *Rundfunk* as far as the tradeoffs are concerned is the fact that the ECJ said that it is for the national courts to decide whether the interference with the data privacy of the effected Austrian citizens was justified by the important public economic purpose.[217] By giving the question back to the Austrian national courts to decide, it is possible that the precise tradeoffs in the Directive will be given effect to differing degrees in different E.U. Member States. Therefore, it is possible that the same tradeoff will not be made throughout the European Union. This problem, however, is more about E.U. institutional structure and less about the particular privacy versus data flow tradeoffs even though the problem affects how the tradeoffs are realized. Be that as it may, *Rundfunk* shows a pretty straightforward, if not inoffensive, application of the Directive and the tradeoffs between data privacy and data flow in commerce were largely realized.[218] To the extent that *Rundfunk* left the impression that the Directive's tradeoffs could be realized, that impression can no longer be maintained after *Lindqvist* and *PNR*.[219]

---

214. Council Directive, *supra* note 4, arts. 7(e),13(1) 1995 O.J. (L 281) at 40, 42.

215. *Rundfunk,* 3 C.M.L.R. at 298–300; *See* discussion, *supra* notes 102–104 and accompanying text (discussing the court's balancing approach).

216. *Rundfunk,* 3 C.M.L.R. at 298–300.

217. *See id.* at 300.

218. *Id.* at 298–300 (holding that the collection of information on public and human resource expenditures unquestionably serves a vital public interest).

219. Case C-101/01, Lindqvist, 2003 E.C.R. I-12971, 1 C.M.L.R. 20 (2004); Joined Cases C-317 & 318/04, Eur. Parliament v. Council of the Eur. Union (*PNR*), 2006 E.C.R. I-4721, 3 C.M.L.R. 9 (2006); *see supra* Part III.A–B.

Lindqvist demonstrates in several ways that the Directive's spelled-out tradeoffs in data privacy and free flow of data cannot be effectuated in the real world. First, *Lindqvist* exposes this ineffectiveness in the Court's determination of the Directive's scope. On the surface, there does not seem to be anything that is *per se* unreasonable about the Court's holding that the conduct at issue was within the scope of Community law (and thus that the Directive applied).[220] Not requiring a showing of an actual link between every situation covered by the Directive and "free movement" within the Union (i.e. a link with the functioning of the internal market) would seem to make sense because there are undoubtedly situations that, while not directly involving commercial or market-oriented conduct, might affect the functioning of the internal market.[221] The *Lindqvist* Court, however, did not discuss any such indirect effect on the functioning of the internal market that the church lady's conduct might have had and merely reasoned that to require such a link would result in uncertainty in the field of application of the Directive.[222] The Court essentially said that even though Lindqvist's conduct was non-commercial and not for profit (suggesting, at best, a tenuous tie to the functioning of the internal market), that did not matter.[223] It was enough for the Court that no actual link between the free movement and the situation covered by the Directive need be shown and that her conduct did not neatly fit into the first category of exceptions, State activities, or the second category, "purely personal" or "household" activities.[224]

At first blush, it would appear that the ECJ is applying a similar reasoning to that found in the Commerce Clause[225] line of United States Supreme Court cases. Under those U.S. cases, Congress' Commerce Clause power is able to reach conduct that is non-economic or wholly intrastate so long as the conduct has a

220. *Lindqvist*, 1 C.M.L.R. at 697–98.

221. *See id.* at 697 (holding that a link requirement would make the laws more uncertain and create more disparate national legislation).

222. *Id.* at 697–98.

223. *Id.*

224. *Id.* at 698 (holding that the exceptions apply "only to the activities which are expressly listed there or which can be classified in the same category").

225. U.S. CONST. art. 1, § 8, cl. 3 (giving the U.S. Congress "the power . . . to regulate commerce with foreign nations, and among the several states, and with the Indian tribes").

"substantial economic effect on interstate commerce." [226] If the ECJ were just giving a broad construction to the parameters of Community law so that E.U. laws passed on the basis of facilitating the functioning of the internal market can govern conduct that is non-commercial but that still might affect the Community, it would seem to be a reasonable attempt at effectuating the tradeoffs. The Directive (and thus the tradeoffs) would be triggered if an effect on the functioning of the internal market could be shown. But this is not what the ECJ was doing. The U.S. Commerce Clause line of cases articulated the substantial effect standard and then applied that standard to the facts of a given case.[227] The Court in *Lindqvist* does not supply a rule to determine when conduct would be too far removed from the functioning of the internal market to be considered outside the scope of Community law.[228] Therefore, the ECJ seems to be giving the Directive a construction that is limited only by two narrow categories of exceptions.[229] Such a broad construction leaves individuals like Lindqvist who engage in non-commercial activity that is in essence speech, exposed to liability under the Directive. The framers of the Directive certainly could not have been interested in regulating conduct like the church lady's. And, if they were interested in regulating this type of activity, the tradeoff as it is shown by *Lindqvist* is not one that is desirable. A rule that makes the tradeoff as it did in *Lindqvist* restricts the individual's right to communicate about others even when such communication has nothing to do with commercial activity and is essentially an exercise of free expression.

---

226. Beginning with *Wickard v. Filburn*, the United States Supreme Court has repeatedly held that entirely intrastate and often non-commercial conduct can be reached by Congress under its Commerce Clause power if the conduct in question "exerts a substantial economic effect on interstate commerce." *See* Wickard v. Filburn, 317 U.S. 111, 125 (1942) (holding that Congress could proscribe a farmer's production of wheat for personal consumption because the activity substantially affected interstate commerce); United States v. Lopez, 514 U.S. 549, 559 (1995) ("Congress' commerce authority includes the power to regulate those activities having a substantial relation to interstate commerce, i.e., those activities that substantially affect interstate commerce." (citations omitted)); Gonzalez v. Raich, 545 U.S. 1, 15–18 (2005) ("Congress has the power to regulate activities that substantially affect interstate commerce.").

227. *See Gonzalez*, 545 U.S. at 15–26 (collecting cases).

228. *Lindqvist*, 1 C.M.L.R. at 697–98.

229. *Id.*

While it is true that the church lady's conduct was, strictly speaking, neither state conduct nor purely personal, it is conduct that would not seem to be what the Directive is aimed at controlling.[230] Whether it is the poorly conceived wording of the Article 3(2) exceptions or the inflexibility of the ECJ in interpreting it, the result is the same: non-commercial, non-profit conduct like Lindqvist's, that is not different in any important respect from a person using or relaying information about friends and perhaps passing on a phone number to someone else or posting the information on a bulletin board in the lobby of a church, gets pulled into the same category as a huge data aggregator that collects consumer information for consumer profiling and marketing purposes.[231] The practical consequences of this are enormous. It means that just about any processing of personal data, unless it can safely be categorized as done in the course of a purely personal or household activity or categorized as an activity of the State, is subject to the provisions of the Directive. In fact, not long after the ECJ rendered its decision in *Lindqvist*, the Norwegian data protection authorities announced that they would be seeking to prosecute web site operators that post photos of people without their consent.[232] The Directive is thus neither effectively making the tradeoffs that it purports on its face nor are these tradeoffs made where they should be made since the church lady's conduct is not likely to be the kind of conduct that raises concerns about data privacy.

In a second and quite different way, *Lindqvist* demonstrates that the data privacy tradeoffs in the Directive cannot be realized. The

---

230. While the Directive's preamble contains a number of points indicating tradeoffs between data privacy and data flow, it makes special mention of economic activities such as the increase in "the exchange of personal data between undertakings," the fact that differing levels of privacy protection in Member States can be "an obstacle to the pursuit of a number of economic activities at the Community level and distort competition," and the idea that equivalent data protection is "vital to the internal market." Council Directive 95/46, *supra* note 4, pmbl. ¶¶ 5,7–8, 1995 O.J. (L 281) at 31–32. This strongly suggests that even though Lindqvist's activities were caught in the wide web of the Directive, this may be due more to the failure of the framers to exclude processing activities of this type, i.e., miscalculating the tradeoffs, or because the ECJ was too inflexible when interpreting Article 3(2).

231. *See* Council Directive 95/46, *supra* note 4, art. 3(2), 1995 O.J. (L 281) at 39.

232. *See* Klosek, *supra* note 106.

Court's holding that posting personal data on the Internet where the ISP is located within the European Union and where the data is accessible by persons located in third countries does not constitute the transfer of data to a third country[233] is another application of the Directive that leads to results opposite the aims of the Directive. Yet, the ECJ did not seem to have much choice to interpret it differently. The ECJ relied on a distinction between the accessibility of data by persons in a third country and the actual transfer of the data by the data controller to those persons.[234] This reasoning seems contrived when it is obvious that the person posting the personal data on the Internet means for it to be available to other persons who use the Internet.

The Court also relied on the apparent situation that, if Article 25's prohibition on transfer of data to third countries lacking adequate protection were intended to include posting such data on the Internet, Article 25 would necessarily become a regime generally applicable to Internet transfers instead of being specifically concerned with transfers of data to third countries.[235] While the Court's statement about a regime applicable to processing on the Internet may be true, it is also a recognition that the theoretical underpinnings of the Directive do not match up to the practical realities of sharing and transferring of information over the Internet. It should make little difference whether the data controller actually placed the personal data in the hands of a person in a third country or transferred the data by other means such as the Internet. For purposes of the data privacy tradeoffs in the Directive, once personal data is posted on the Internet, it is *in* that third country and accessible. If the third country in question lacks adequate protection for the data, the personal data of E.U. citizens is no longer protected once in that country, regardless of how it got there. Under the Court's stilted interpretation of Article 25's application to the Internet, entirely different results would obtain if the church lady had sent the personal data by postal

233. *Lindqvist*, 1 C.M.L.R. at 701.

234. *Id.* at 700–01 (stressing that it is not considering the processing activities of the hosting providers who may, in fact, be physically transferring data to someone accessing the Internet).

235. *Id.* at 701.

service, to say, data brokers Choicepoint or Acxiom in the United States instead of using the Internet.[236]

The Court's holding on the Article 25 transfer question therefore recognizes the dilemma that to hold that posting the information on the Internet constitutes a transfer would generally either require eliminating the use of the Internet or make the enforcement of the Directive's data protection regime virtually impossible since it would require vigorous policing of the Internet. The Court's holding creates a loophole by which the privacy rights of E.U. citizens under the Directive are not protected when it was clearly the intent to protect these rights in the circumstance where data might be transferred to a third country. The ECJ was caught in the difficult position of trying to maintain the Directive's effect while not allowing this flaw to swallow the entire regime. Essentially, the inability to reconcile the Article 25 transfer prohibition with the practical and ubiquitous nature of the Internet shows that the Directive's purported tradeoffs can not in fact be made when it comes to use of the Internet.

As a practical matter, the fact that posting information on the Internet does not constitute a transfer of data to a third country has, however, been largely well-received by the business community.[237] While this aspect of the case does not mean that by posting personal data on the Internet, businesses are able to avoid their obligations under the Directive, it does mean that when an E.U. business provides personal data to its partners or affiliates in third countries (the United States, perhaps) via posting it on the Internet, they do not commit a separate violation of the Directive by transferring the information in this manner.

The down-side of this is the negative consequence for the E.U. citizen whose data ends up in the United States and would no longer seem to be subject to the stringent controls in Europe. Thus, while an E.U. citizen may have provided the necessary unambiguous consent to the controller in Europe and can basically revoke that consent and has rights of action against the controller for violations of data

236. *See id.* at 699–700 ("Where a third country does not ensure an adequate level of protection the *transfer* of personal data *to* that country must be prohibited." (emphasis added)).

237. *See* Fiebig, *Sweden Regulations*, *supra* note 106 ("In general this [decision] is good news for business.").

protection laws, these protections evaporate once the data finds its way into a third country lacking adequate protection and the data is processed by an affiliate in the third country.

The *Lindqvist* case also highlights a third way in which the Directive's tradeoffs are not being realized. In its holding that the Directive does not conflict with general principles of freedom of expression, the ECJ essentially recognized this tension and said that it is for the national courts to balance the fundamental interests of data privacy and freedom of expression.[238] While this may sound like the Court is giving effect to the tradeoffs by way of a balancing test, the fact that the Court did not supply such a test but merely kicked the question back to the national courts to decide shows that the tradeoff is not actually given any effect. Individual Member States will have to give effect to the tradeoff between data privacy and freedom of expression and do so without explicit guidance from the Directive or ECJ as to where the data privacy line begins and the freedom of expression line ends. The tradeoffs here are thus not made by the Directive but ad hoc by the Member States which may lead to disparate balancing among the Member States.

B. DATA PRIVACY VERSUS SECURITY

The Directive's attempt to balance the need to process personal data for public security purposes against data privacy is also unworkable.[239] Although the Directive's exclusion of important state activities from its scope and its exceptions to state obligations when security is concerned demonstrates that the Directive is intended in part to balance public security against data privacy, the *PNR* case shows that this balancing is not practically possible.[240]

First, the ECJ's holding in *PNR* on the applicability and scope of the Directive shows that this particular tradeoff cannot be realized.[241] The ECJ essentially invalidated the Commission's decision on the

238. *Lindqvist*, 1 C.M.L.R. at 703–04.

239. *See* Council Directive 95/46, *supra* note 4, art. 3(2), 1995 O.J. (L 281) at 39 (exempting public security operations from the scope of the Directive).

240. *Id.* pmbl. ¶¶ 13, 16, 30, 43, arts. 3(2), 7(e), 8(4), 13, 1995 O.J. (L 281) at 32, 34, 39.

241. Joined Cases C-317 & 318/04, Eur. Parliament v. Council of the Eur. Union (*PNR*), 2006 E.C.R. I-4721, 3 C.M.L.R. 9, 324 (2006).

adequacy of protection of personal data in the United States because the transfer of PNR data by commercial airlines to U.S. authorities was accomplished pursuant to a security/criminal law framework established by public authorities.[242] Thus, the Article 3(2)'s exception for certain state activities was triggered and rendered the Directive inapplicable to the processing activities.[243] At first glance, it appears that exactly what was supposed to happen did happen: E.U. Member States are concerned about preserving their sovereignty in the area of state security and required that the Directive not apply to security related activities. The exception was thus triggered which brought the data processing activity outside the scope of Community law and of the Directive. On the other hand, a comprehensive data protection regime should not become inoperable when the question concerns data privacy versus data flow for security, and especially not when the comprehensive regime on its face purports to deal with the privacy versus security issue as the Directive does.

Further, the unrealized tradeoff between data privacy and security is evident in that the state security at issue could not have been the type of state security intended to trigger the exception. The state security exception under Article 3(2) should not have been triggered since the personal data at issue had been collected by commercial airlines in the European Union and transferred by them to the U.S. authorities. Although the Court took pains to distinguish the processing activities of the commercial airlines[244] from the processing that took place pursuant to the security/criminal law framework put into place by public authorities, the security/criminal law framework was not that of the European Union but, rather of the United States.[245] The demand by the United States for the PNR data from the air carriers was the genesis of all subsequent action on this issue by E.U. authorities. The Commission had even made the U.S. authorities aware of the potential conflict between the compliance with U.S. law and the compliance with E.U. data protection

242. *Id.* at 323.

243. *Id.*

244. That is, the processing of personal data required in the course of the sale and purchase of airline tickets.

245. *See PNR*, 3 C.M.L.R. at 322. (distinguishing "data processing necessary for a supply of services" from "data processing regarded as necessary for safeguarding public security and for law-enforcement purposes").

standards.[246] In fact, the ECJ even acknowledged that the requirements for the transfer of the PNR data are based on the U.S. statute and implementing regulations promulgated under it.[247] It was therefore not a *European* security/criminal law framework under which the decisions of the Commission and Council were made and thus they should not have been excluded from the Directive's scope.

The Commission's motivation in negotiating any agreement with the United States for the sharing of PNR data seems to have been primarily to preserve the privacy protections of E.U. citizens and avoid negative economic consequences to the commercial interests of E.U. air carriers and the traveling public. The aims of the Commission and the Council in proceeding as they did on the PNR issue appear to be more related to commerce than to security and criminal law. While the European Union recognized the U.S. need for the data, the European Union sought to make sure that any turn over of the data would also include protections of it.[248] Therefore, the Commission's decision on adequacy, which would have (1) provided additional protections to the data of E.U. citizens in the United States by getting the United States to agree to privacy protections it would not have otherwise provided, (2) avoided the negative economic consequences to E.U. air carriers and to the public and (3) provided enhanced security in connection with U.S. bound flights, was not allowed to take effect because the ECJ deemed the Directive inapplicable to the Commission's actions.[249] Thus, language of the Directive itself excluded this situation from its scope and no effective tradeoff between privacy and security resulted.

On a related point, *PNR* shows that the security tradeoff is not realized because the Commission was not allowed to do what it is supposed to do under Article 25 of the Directive: assess the adequacy of protection in third countries and negotiate with the third country to

246. *Id.* at 319–20 (following the explicit U.S.-E.U. dialogue on the implementation of the Directive).

247. *Id.* at 319–22 ("It is apparent from the sixth recital in the preamble to the [Commission's] decision [on adequacy] that the requirements for that transfer are based on a statute enacted by the United States . . . and on implementing regulations adopted by CBP under that statute.").

248. *Id.* at 319–20 (following negotiations concerning the adequacy of U.S. protections).

249. *Id.* at 323.

obtain an adequate level of data protection.[250] The Directive purports to address the security concern by relaxing the data protection obligations for states in matters of security and by excluding certain state activities from its scope.[251] It simultaneously purports to provide for increased protection of personal data in the transnational context by creating a scheme by which the Commission could assess the level of protection in a third country and negotiate with that country for increased protection if necessary.[252] The Commission did exactly what the Directive tells it to do, yet the ECJ nullified its actions. Therefore, there is no resultant increase in data protection for E.U. citizens and no enhanced security for the transatlantic flying public.

PNR shows that the privacy versus security tradeoff is not realized in another important way.[253] By nullifying the decisions of the Commission and the Council, the ECJ has essentially sacrificed the security of both the United States and the European Union. It is difficult to imagine that the PNR data would not be useful in combating terrorism and other international criminal enterprises, evils that both the European Union and the United States have a vested and professed interest in combating.[254] The PNR data provides a means by which to track suspects and identify potential perpetrators. The ECJ's decision rendering the U.S./E.U. agreement to share the PNR data ineffective, has essentially propelled the interest in data privacy to a far higher priority than interests in security. The language of the Directive shows the intent to balance these interests and the Commission and Council sought to give life to that balance by negotiating an agreement that would simultaneously protect privacy under E.U.-like privacy standards and allow security concerns to be addressed. But, the ECJ's decision invalidated the Commission and Council's attempt at effectuating the security tradeoff. Now, if the data is made unavailable to the United States, the United States will lack an important tool in combating crime and

250. *PNR*, 3 C.M.L.R. at 324.

251. *See* Council Directive 95/46, *supra* note 4, arts. 3(2), 13, 1995 O.J. (L 281) at 39, 42.

252. *See id.* art. 25, 1995 O.J. (L 281) at 45.

253. *PNR*, 3 C.M.L.R. at 324–25.

254. *See id.* at 319–20 (noting the Commission's "acknowledg[ment] of the security interests at stake" and the Council's assertion that "[t]he fight against terrorism . . . justifies the proposed measures").

terrorism which may lead to a less secure environment for both the United States and the European Union. While data privacy in the European Union has been preserved, it has been at the expense of security in the United States and in the European Union. And, it has not merely been a tipping of the scales slightly in one direction. As far as the PNR data is concerned, privacy has been completely maintained and security completely sacrificed.

The consequences that may follow from the ECJ's ruling in *PNR* show just how poorly the data privacy versus security tradeoff is made by the Directive. The lack of clarity that now attends to situations where private commercial actors collect data but where that data is then used for a law enforcement or quasi-law enforcement purpose presents particular difficulties. *PNR* creates a lack of protection of the European citizen since it is no longer clear that data collected for commercial purposes but which is later used by police are protected by the Directive. So, the Directive, with its seemingly clear spelling-out of obligations and exceptions for both public and private actors, now perhaps will not protect the privacy interests it was designed to protect once the data has moved beyond the initial controller who may have obtained the data subject's unambiguous consent.

By way of extension, there is also uncertainty regarding private data transfers that somehow relate to law enforcement or public security. Examples might be transfers undertaken by private sector actors at the request or direction of public authorities engaged in law enforcement or security activities or purely private sector transfers undertaken to combat fraud, money laundering, counterfeiting or identity theft. When Visa or MasterCard collect data in connection with anti-fraud activities, are these data now done within the framework of law enforcement established by public authorities so that the Directive no longer applies? The dual facets of fraud prevention, both within the realm of the criminal law and in the interests of private businesses like credit card companies, make it difficult to determine if, after *PNR,* such data processing would be subject to the Directive. If the Directive does not apply to such situations because the activity is deemed a law enforcement/security related activity, then such private processors might be able to act with impunity against the interests of data subjects which does not

amount to a desirable privacy/data flow tradeoff when private commercial actors are involved.

It is also worth noting that even though the status quo of the PNR issue has been maintained by a subsequent new temporary agreement (with a proper legal basis), the issue of the privacy versus security tradeoff has not gone away and will likely surface as soon as a more permanent arrangement comes into being.

C. LESSONS FROM EUROPE

The picture that emerges from the ECJ cases on the Directive is that the European Union approached the personal data protection issue with two main assumptions in place: any legislation should be comprehensive and broadly cover all sorts of processing activities, and *privacy* in personal data is paramount to other concerns. The above analysis on the ECJ cases demonstrates that both of these assumptions do not necessarily provide a sound basis on which to develop a regime that will both protect personal data and, at the same time, not hinder its flow. It seems that the European Union did not give enough consideration to what particular problems people worry about when it comes to their personal data, nor did it fully consider the balancing of interests.

The European Union perhaps went too far in making its regime comprehensive. The lack of focus on particular data protection issues that citizens are really concerned about led to legislation that regulates not only conduct that citizens worry about but also innocuous conduct like the church lady's. For example, most citizens do not want large shadowy enterprises collecting data on them to create digital dossiers[255] that are used by private and public sector actors without the data subject's knowledge. However, most citizens would not want to be restricted from expressing themselves just because the expression involves information about others. The E.U. legislators would have been wise to approach the data protection issue with more focus on exactly what people care about when it comes to others processing their personal data, but instead, they took

255. The term "digital dossier" is used by Daniel Solove to describe comprehensive digital profiles created primarily by data aggregators like ChoicePoint and Acxiom. *See* DANIEL J. SOLOVE, THE DIGITAL PERSON 13–26 (Jack M. Balkin & Beth Simone Noveck eds., 2004).

a panoramic approach and wound-up restricting conduct that is in fact desirable in a democratic society.

Although much of the Directive's language seems pointed toward the dual goals of privacy and harmonizing the data protection laws within the European Union so as not to disrupt data flow, the cases make clear that the Directive was crafted with privacy as the overriding concern. Of course, this is only natural; if there were no regulation of data privacy, the undesirable uses of personal data would surely flourish and regulation would be needed to remedy the problem. Regulation aimed at remedying a privacy problem would naturally have 'creating more privacy' as its main objective. However, approaching the problem from this angle (that more privacy is the principle concern) ignores the importance of the competing goal of ensuring societal benefits that accrue from free flow of data. In other words, a comprehensive regime should start from the premise that what we want is to achieve the right balance and not from the premise that privacy is lacking so we need more of it. The flow of data in a democratic and free-market society is essential to its functioning. Europe's law seems to have been enacted from a "privacy is paramount" perspective with less emphasis on balancing privacy against accessibility of data.

Given these shortcomings of the Directive and mistaken premises on which it was based, U.S. law makers should carefully consider making any comprehensive U.S. data protection legislation apply only to commercial actors. Commercial actors could be held to higher standards in the handling of citizens' personal data while leaving individual citizens not engaged in commercial or professional activities free to use and disclose personal data on others. The higher standards for commercial actors could be similar to the broad standards that apply to everyone under the E.U. Directive and incorporate the eight general data protection principles enshrined in the Directive.[256] Any time that there is a commercial component to an individual citizen's personal data processing, they would then be subject to the higher standard just as any other commercial actor is. This would also create an incentive for citizens to share needed information with commercial enterprises, for

256. *See supra* note 56.

example, their employers, their banks and healthcare providers, knowing that the information would be protected. It would also encourage citizens to avoid sharing information with private individuals who, in the data subject's opinion, should not have possession of it. Finally, it would not hamper citizens' private and non-commercial ability to freely express themselves even where it involves information about others.

A second consideration that should be taken into account by U.S. law makers is the realities of international data transfers. Any comprehensive U.S. legislation would need to deal with the question on protections afforded to personal data once it leaves the borders of the United States. The global economy being what it is today means that cross-border data transfer must be facilitated.[257] That the Internet is one of the most important means of cross-border communication is obvious. Therefore, any data protection scheme should take account of the crucial role that the Internet plays in data flow and recognize that once personal data is placed on the Internet it is available and useable, for good or for worse, in places that have different protection (or none) than the place from which the data originated. Perhaps the answer is, instead of aiming enforcement at the transferor as the Directive does, to use an extraterritorial application of a U.S. data protection regime to tag offenders in foreign counties with liability under the U.S. law. For example, when a data aggregator sets up shop in India and is collecting data on American consumers that it gathers via the Internet and then violates a provision of the U.S. law, it could be hauled into a U.S. court if it has sufficient contacts with the United States which it would likely have if data on American consumers is important enough to its business to aggregate. Such a scheme would generally make U.S. data protection standards apply to data on U.S. citizens wherever it winds up.

A third point that should be considered by U.S. law makers is that there are certain societal needs that may outweigh the need for

257. In fact, differences in the level of protection provided for personal data in the United States and in the European Union almost led to a trade embargo which was avoided by the Safe Harbor Agreement. *See* Council Directive 95/46, *supra* note 4, pmbl. ¶¶ 56, 59, art. 25, 1995 O.J. (L 281) at 36–37, 45; Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. at 45,667; Commission Decision 2000/520, *supra* note 150, art. 1, 2000 O.J. (L 215) at 2.

privacy in personal information. Although commercial actor's collection of personal data for commercial purposes may not outweigh an individual's right to keep personal information safe, when the need for the data is related to public security, for example, most Americans might say that this should take precedence over privacy. The government should of course be subject to high standards of care for the personal information it obtains and perhaps be prohibited from handing it over to third parties (commercial actors or other governments). But, in an age where security is a real concern and much of what threatens security is done through information, law enforcement in the United States should not be hampered to the degree that they are under the E.U. Directive. Any approach to the drafting of comprehensive data protection legislation should therefore proceed on the basis of balancing the privacy interests against the security interests rather than beginning from the premise that privacy is the norm and data flow is the exception.

V. CONCLUSION

In debating the form that any proposed data protection regime might take in the United States, much can be learned from Europe's mistakes in this area. As laudable as the goals behind the European Data Privacy Directive may be, the ECJ cases show that in several important respects these goals are not practically capable of realization. The lines demarcating the tradeoffs between privacy and data flow as drawn by Europe show that privacy prevails over data flow in a non commercial expressive context. Data privacy is also given paramount importance to the practical exclusion of security interests that depend on the flow of data. The ECJ cases have also shown that the rights extended to E.U. citizens by the Directive fail to recognize the practical realities of how data is used in global commerce. Although the Directive portends to have these protections apply to the personal data wherever it may wind up, the nature of data transfer methods like the Internet defy the scheme by which the Directive attempts to secure this protection outside the European Union. If comprehensive data protection legislation is a future possibility in the United States, law makers would be well-advised to focus more specifically on the particular data privacy problems caused by personal data being too freely available and avoid

approaching the issue with the assumption that data privacy in general is inherently better than its ability to flow freely.