1-2013

Global Governance in the Information Age: The Terrorist Finance Tracking Program

Hannah Bloch-Wehba
Texas A&M University School of Law, hbw@law.tamu.edu

GLOBAL GOVERNANCE IN THE INFORMATION AGE: THE TERRORIST FINANCE TRACKING PROGRAM

HANNAH C. BLOCH-WEHBA*

Europe has long been deemed "more protective" of privacy than the United States. In the context of transatlantic cooperation in the war on terrorism, divergences in privacy law and policy have become ever more apparent. As has always been the case, the same technologies that pose new and vital privacy issues with regard to personal information and private data are those that are important sources for government actors, including law enforcement and intelligence agencies. Despite the increasing reliance by national agencies on information flowing from other nations, regulation of information transfer, processing, and sharing has been achieved largely outside of the international sphere.

This Note argues that the use of personal information in the national security setting offers a new and important look at the functions and limitations of global governance in the information age. Exploring the Terrorist Finance Tracking Program (TFTP), a joint initiative among European states and the United States, within the framework of Global Administrative Law (GAL), I argue that common accounts of differences between U.S. and European law on privacy issues do not explain the very real tensions at stake in the TFTP. I show that the TFTP is a real effort at constituting a soft-law mechanism to manage privacy and security in the information age, and argue that it fails to embody those values of transparency, participation, legality, and accountability to which we generally hold GAL mechanisms.

* J.D. Candidate, New York University School of Law, 2013. I would like to thank Professor Eyal Benvenisti, Madalyn Wasilczuk, Matt Hartz, Angelina Fisher, Lorenzo Casini, Ben Heath, and the attendees of the 2012 International Law and Human Rights Scholarship Conference for their helpful comments and guidance on early versions of this Note. All errors are my own.

INTRODUCTION

Shortly after September 11, 2001, the U.S. Department of the Treasury began using administrative subpoenas to compel the disclosure of millions of records from SWIFT, a Belgian banking consortium, in an initiative known as the Terrorist Finance Tracking Program (TFTP). After the existence of the program came to light in 2006,[1] the Council of Europe reached an interim deal with the United States to continue sharing the bank data; the European Parliament vetoed the deal, complaining that it violated European law. The TFTP, said Jeanine Hennis-Plasschaert, the rapporteur on the issue, "must be considered as a departure from European law and practice in how law enforcement agencies would acquire individuals' financial records for law enforcement activities, namely individual court-approved warrants or subpoenas to examine specific transactions instead of relying on broad administrative subpoenas for millions of records."[2] As a result of the European Parliament vote, U.S. access to European bank data "went dark" for several months, until a revised deal was reached in summer 2010.[3]

---

1. Eric Lichtblau and James Risen, *Bank Data Is Sifted by U.S. in Secret To Block Terror*, N.Y. TIMES, June 23, 2006, http://www.nytimes.com/2006/06/23/washington/23intel.html.

2. Draft Recommendation on the Proposal for a Council Decision on the Conclusion of the Agreement Between the European Union and the United States of America on the Processing and Transfer of Financial Messaging Data from the European Union to the United States for Purposes of the Terrorist Finance Tracking Program, EUR. PARL. DOC. A7-0013 (2010).

3. Agreement Between the United States of America and the European Union on the Processing and Transfer of Financial Messaging Data from the European Union to the United States for the Purposes of the Terrorist Finance Tracking Program, U.S.-E.U., June 28, 2010, *available at* http://www.treasury.gov/resource-center/terrorist-illicit-finance/Terrorist-Finance-Tracking/Documents/Final-TFTP-Agreement-Signed.pdf.

In drawing a distinction between U.S. and European policy on this issue, Hennis-Plasschaert was signaling to long-running disputes between the two powers revolving around data privacy. The enactment of the Data Protection Directive in 1995[4] would have prevented data transfers to the United States were it not for the Safe Harbor agreement that was eventually effectuated.[5] More recently, in the context of the war on terrorism, the European Union reached an agreement with the United States on the sharing of airline passenger data, or "Passenger Name Records," only to have that agreement annulled by the European Court of Justice (ECJ) in 2006. Although intra-European disputes over the Passenger Name Records agreement centered on the protection of personal data, the ECJ did not decide whether the protection of personal data that it offered was sufficient, rather holding that the agreement needed parliamentary approval.[6] Indeed, in the SWIFT case, new powers under the Lisbon Treaty to pass on issues of police and judiciary cooperation certainly empowered the European Parliament to take a principled stand against data sharing.[7]

In contrast, as technology has changed, it has become increasingly easy for American law enforcement authorities to obtain personal information for use in a criminal investigation without first seeking a warrant.[8] Although Congress and state

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

5. *See Welcome to the U.S.-EU Safe Harbor*, EXPORT.GOV, http://export.gov/safeharbor/eu/index.asp (last visited Feb. 11, 2013) (introducing the Safe Harbor framework).

6. Joined Cases C-317/04 & C-318/04, European Parliament v. Council of the European Union and Commission of the European Communities, 2006 E.C.R. I-4795 ¶¶ 67–70.

7. Pre-Lisbon, criminal matters were essentially beyond the ambit of European Union law. Case C-176/03, Commission of the European Communities v. Council of the European Union, 2005 E.C.R. I-7907 ¶ 47 ("[N]either criminal law nor the rules of criminal procedure fall within the Community's competence.").

8. *See* Smith v. Maryland, 442 U.S. 735 (1979) (finding no warrant necessary for pen register recording numbers dialed from home phone because this does not constitute a "search" within the meaning of the Fourth Amendment); United States v. Miller, 425 U.S. 435 (1976) (finding no Fourth Amendment interest in the relevant bank records); and United States v.

legislatures have acted to pass legislation that protects privacy in various sectors, no general principle that consumers "own" their information exists in U.S. law.[9] The legal scenario with regard to personal data protection is thus very different from that in Europe.

Because the SWIFT case stands at the intersection of two vital areas of European-American cooperation—data transfers and counterterrorism—it is a hard case to understand, yet a vital one. A realist analyzing the case might argue that it is a classic example of bickering over the appropriate balance between privacy and security, made all the more potent by the implications for trans-Atlantic cooperation in the pursuit of terrorists.[10] Viewed more generously, the TFTP must be understood in the context of its integral role in the European data-protection framework as an illustrative example of the tensions at play in European data privacy law. On this reading, the European awareness of "the impact of new technologies, the fact that we are now living in a 'globalised' world," is at the root of disputes over data protection.[11] At the same time, the United States has taken the perspective that while European integration has propelled data sharing among European states, it has also hampered similar cooperation between EU member states and the United States.[12] Solutions like the

---

Jones, 565 U.S. __ (2012) (implementing third party doctrine by exempting categories of "shared" information from the Fourth Amendment's warrant requirement).

9. The proliferation of data breach notification laws in state legislatures is one example of sectoral legislation that acts to protect privacy in some contexts. *See State Security Breach Notification Laws*, NATIONAL CONFERENCE OF STATE LEGISLATURES, http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx (last visited Feb. 11, 2013) (listing state security breach notification laws).

10. *See, e.g.*, STEWART A. BAKER, SKATING ON STILTS: WHY WE AREN'T STOPPING TOMORROW'S TERRORISM 150 (2010) ("[T]he European Union seemed almost enthusiastic about threatening private companies with sanctions as a way of attacking U.S. government practices.").

11. Viviane Reding, Vice-President, European Comm'n Responsible for Justice, Fundamental Rights and Citizenship, Remarks at the Meeting of the Article 29 Working Party "Review of the Data protection legal framework": Towards a True Single Market of Data Protection (July 14, 2010), http://europa.eu/rapid/pressReleasesAction.do? reference=SPEECH/10/386&format=HTML&aged=0&language=EN&guiLanguage=en.

12. *See, e.g.*, Scenesetter: FBI Director Mueller's Berlin Visit, Cable from American Embassy Berlin to FBI and DOJ (Aug. 11, 2006), http://wikileaks.

TFTP and the Passenger Name Records agreement are attempts to solve the classic problem that emerges from increased international interdependence in the law enforcement arena. Yet in very real ways, these agreements neither reflect the historical differences in European and American privacy law, nor do they foster new normative agreement on these issues.

In this Note, I argue that the Terrorist Finance Tracking Program is best understood not as a "compromise" between European and American privacy values, but rather as a contested instrument of global administrative law, the result of two systems competing to achieve the effect of extraterritorial regulation according to their own domestic norms. Part I of this Note analyzes the European data protection framework as an instrument of global administrative law and explores the Terrorist Finance Tracking Program as part of that framework. I argue that although the European data protection framework seeks to impose European privacy norms on the international transfer of data, classical understandings of European and American privacy law do not explain how and why the two powers came to the TFTP agreement. Rather, I argue, the divergences between European and U.S. privacy law result from different statutory approaches that allow European legislators and regulators to respond much more quickly to technological change. In light of that fact, I argue in Part II that the TFTP can be best understood through the lens of global administrative law as implementing procedural and substantive rules to protect consumer privacy as understood in both Europe and the United States; however, the program suffers from deeply flawed approaches to transparency and accountability. Part III turns to an inquiry about the nature and privacy implications of large-scale automated data collection in the national security setting of both privacy regimes. I explore the growing utility of large-scale databases and discuss the difficulties and risks of regulating the bulk transfer of data at the global level.

---

org/cable/2006/08/06BERLIN2303.html ("While Germany is enhancing data exchange with its EU partners, the Germans have been reluctant to consider ways to enhance similar data-sharing with the U.S.").

I. INDIVIDUAL PRIVACY IN THE OLD WORLD AND THE NEW WORLD

A. *The European Data Protection Framework as Global Administrative Law*

Globalization and burgeoning interdependence among global powers has led to the rise of forms of international governance beyond classic treaties and formal agreements. New institutions of global governance take many forms and serve many functions, but do not always embody the kinds of checks and balances served by either formal diplomatic process or by democratic rule. As a result, questions about democratic legitimacy—about accountability, transparency, participation, and redress—are rife with regard to this new type of institution.[13] Global administrative law (GAL) responds to this phenomenon by recasting global governance as extant in an intermediary "global administrative space," in which domestic regulatory actors interact with international action in ways that are essentially mutually constituting.[14] In their seminal article, *The Emergence of Global Administrative Law*, Kingsbury, Krisch, and Stewart offered a taxonomy of global governance institutions, subjects, and sources of GAL—and suggested that global administrative bodies must "meet adequate standards of transparency, participation, reasoned decision, and legality, and . . . provid[e] effective review of the rules and decisions they make."[15]

GAL provides a useful lens through which to examine the European data protection framework as a whole and the Terrorist Finance Tracking Program as a problematic case of governance within that system. By unpacking the institutions operating within a state and closely examining the relationships with other institutions in other states and at the international level, GAL promises to "highlight[ ] the extent to which mechanisms of procedural participation and review, taken for granted in domestic administrative action, are lacking on the global level."[16]

---

13. Andrew Moravcsik, *Is There a 'Democratic Deficit' in World Politics? A Framework for Analysis*, 39 GOV'T & OPPOSITION 336 (2004).

14. Benedict Kingsbury, Nico Krisch & Richard B. Stewart, *The Emergence of Global Administrative Law*, 68 LAW & CONTEMP. PROBS. 15, 26 (2005).

15. *Id.* at 17.

16. *Id.* at 27.

Europe's system of regulating data protection has been described as a "transgovernmental network."[17] Statutory protection of privacy in the European Union embraces a "comprehensive" approach, the groundwork for which was laid in the Council of Europe Convention but the bulk of which stems from later regulation.[18] In 1995, the Data Protection Directive came into effect with the goal of harmonizing European law while permitting differences among member states.[19] Data protection legislation at the supranational level inevitably sets up linkages to national law in that national governments have their own data protection authorities (in addition to the European Commission's Art. 29 Working Party and the European Data Protection Supervisor) and their own data protection legislation.[20]

The significance of the "network" denomination is contested, but insofar as the name serves to distinguish a relatively informal type of interaction among regulators from state-led diplomatic initiatives, it has stuck.[21] Networks are an "adaptable and decentralized" governance alternative to a classic

17. Francesca Bignami, *Transgovernmental Networks vs. Democracy: The Case of the European Information Privacy Network*, 26 MICH. J. INT'L L. 807, 822 (2005).

18. *See* David Banisar & Simon Davies, *Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments*, 13 J. MARSHALL J. COMPUTER & INFO. L. 1, 11, 13–14 (1999) (comparing comprehensive and sectoral models of privacy legislation).

19. *See* Data Protection Directive, *supra* note 4, pmbl. ("Whereas, in order to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of individuals with regard to the processing of such data must be equivalent in all Member States . . . .").

20. *See Id.* art. 28 (requiring each member state to designate a supervisory authority). In the German case, for example, the *Grundgesetz* includes privacy protections in Articles 2, 10, and 13 (Grundgesetz für die Bundesrepublik Deutschland [Grundgesetz] [GG] [Basic Law], May 23, 1949, BGBI. I (Ger.)), the Federal Data Protection Law (*Bundesdatenschutzgesetz*) sets out the rights of data subjects and the responsibilities of controllers and processors, and the individual states each possess data protection authorities to enforce and implement state data protection laws.

21. Anne-Marie Slaughter is largely credited with developing the concept of a transgovernmental network. ANNE-MARIE SLAUGHTER, A NEW WORLD ORDER (2004). For a different view, see generally José E. Alvarez, *Do Liberal States Behave Better? A Critique of Slaughter's Liberal Theory*, 12 EUR. J. INT'L L. 183, 211 (2001) (suggesting that the reliance on transgovernmental networks is overblown).

model of formal intergovernmental treaties or agreements.[22] Although networks can operate within a treaty-based framework, they can also exist apart from one;[23] networks can have the benefit of establishing law (soft and hard) without the risk of judicial review by an established tribunal. Of course, this can also pose dangers to democracy at the domestic and international levels.[24]

While the fact that the European data protection system exists within a statutory and treaty-based framework weighs in favor of its democratic legitimacy, it faces its own legitimacy problems at the member state and Union levels.[25] The Data Protection Directive "establish[es] an elaborate sequence of national and supranational administrative decisions," such that "national and European administrations share responsibility for a single determination of rights and duties under European law."[26] While the Directive was conceived of as a rem-

22. Kal Raustiala, *The Architecture of International Cooperation: Transgovernmental Networks and the Future of International Law*, 43 VA. J. INT'L L. 1, 4 (2002).

23. *See* Kingsbury et al., *supra* note 14, at 21 ("This horizontal form of administration can, but need not, take place in a treaty framework.").

24. *See generally* Robert Keohane, Stephen Macedo, and Andrew Moravcsik, *Democracy-Enhancing Multilateralism*, 63 INT'L ORGS. 1 (2009) (arguing that networks governed by formal treaties can actually enhance, not diminish, domestic democracy).

25. In the closely related issue of data retention, the German Constitutional Court held that Directive 2006/24/EC, of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC, 2006 O.J. (L 105) 54 [hereinafter European Data Retention Directive], was unconstitutional as applied to telecommunication traffic data. Bundesverfassunsgericht [BVERFG] [Federal Constitutional Court], Mar. 2, 2010, 1 Enscheidungen des Bundesverfassungsgericht [BVERFGE] 256/08 (1), 2010 ("Eine sechsmonatige, vorsorglich anlasslose Speicherung von Telekommunikationsverkehrsdaten durch private Diensteanbieter, wie sie die Richtlinie 2006/24/EG des Europäischen Parlaments . . . vorsieht, ist mit Art. 10 GG nicht schlechthin unvereinbar."). In May 2012, the European Commission responded to Germany's failure to transpose the Data Retention Directive into national law by bringing suit at the European Court of Justice and proposing that a daily penalty of over €315,000 be imposed. Press Release, European Comm'n, Data Retention: Commission Takes Germany to Court Requesting That Fines Be Imposed (May 31, 2012), http://europa.eu/rapid/press-release_IP-12-530_en.htm?locale=en.

26. Bignami, *supra* note 17, at 821.

edy to fragmentation among member states' differing privacy regimes, it has not gone far enough; the Commission therefore recently proposed to replace the Directive with a new Regulation of the European Parliament,[27] which would be directly enforceable and which is meant to raise the costs of non-compliance by the private sector and by member states.[28]

At the core of the European data protection framework's power as an instrument of global administration, however, is not its character as an informal network but rather its authority to make extraterritorial rules. As Kingsbury et al. identify, "distributed administration" is a core type of global administration, and it occurs when domestic agencies "take decisions on issues of foreign or global concern. An example is in the exercise of extraterritorial regulatory jurisdiction, in which one state seeks to regulate activity primarily occurring elsewhere."[29] While the European data protection regime should not be understood as a purely "domestic" regime, its power to regulate data transfers outside its own borders is a core attribute of distributed domestic administration.

Thus Article 25 of the Data Protection Directive, which forbids the transfer of data to "third countries" without adequate safeguarding mechanisms, purports to protect citizens' data regardless of where it is housed.[30] Arguably, Article 25 is not an extension of regulatory authority beyond European borders because it affects only European actors who want to

27. *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* [hereinafter *General Data Protection Regulation*], at 2, COM (2012) 11 final (Jan. 25, 2012), *available at* http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf ("The current framework remains sound as far as its objectives and principles are concerned, but it has not prevented fragmentation in the way personal data protection is implemented across the Union, legal uncertainty and a widespread public perception that there are significant risks associated notably with online activity.").

28. *See id.* at 2 (calling for a framework backed by "strong enforcement"); *see also Impact Assessment Accompanying the General Data Protection Regulation*, at 19, SEC (2012) 72 final (Jan. 25, 2012), *available at* http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf (finding that unenforceability was a problem that had plagued the Data Protection Directive and made it difficult to secure compliance).

29. Kingsbury et al., *supra* note 14, at 21.

30. Data Protection Directive, *supra* note 4, art. 25.

transfer data abroad.[31] Under Article 25, no transfer of data outside the European Union can be accomplished without either a decision by the Commission that the receiving nation's data protection regime is "adequate,"[32] or that an ad hoc "safe harbor" arrangement exists.[33] However, the practice of finding whether foreign data protection regimes effectively comply with European law has forced third countries to adopt new measures in order to comply.[34] In measuring the "adequacy" of a foreign data protection regime, the Commission shall take into account "the rule of law, judicial redress and independent supervision."[35] In practice, this requirement is not at all easy to meet; only five "third countries" have been recognized as having adequate protections.[36] Actors in other countries must adequately contract for data protection, a process that is seen as

31. *Id.*

32. *Id.*

33. *See id* (anticipating in subsection 5 that "the Commission shall enter into negotiations with a view to remedying the situation"); *see also* Model Contracts for the Transfer of Personal Data to Third Countries, EUROPEAN COMM'N, http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm (last visited Mar. 11, 2013) (allowing the Commission to determine that certain contractual clauses constitute "adequate safeguards", even for data transfers to those countries that otherwise would have insufficient safeguards), *and* Press Release, European Comm'n, Data Protection: Commission Adopts Decisions Recognizing Adequacy of Regimes in US, Switzerland and Hungary (July 27, 2000), *available at* http://europa.eu/rapid/press-release_IP-00-865_en.htm?locale=en ("Data transfers to US organisations that choose to remain outside the 'safe harbor' will normally still be possible, but will either need to benefit from one of the allowed exceptions (for example where the individuals concerned have given their agreement), or will require alternative safeguards such as a contract.").

34. *See, e.g.*, Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1, 55 (2000) ("The EU Directive has drawn attention to data privacy issues in the United States. It has pressed U.S. governmental authorities to address the adequacy of current U.S. data privacy regulation . . . . It has pressed U.S. businesses to enhance self-regulatory efforts to forestall EU restrictions on data transfers to the United States, divert demands for stricter U.S. regulation, and counter negative publicity . . . .").

35. *General Data Protection Regulation, supra* note 27, at 11.

36. Those countries are Switzerland, Canada, Argentina, and the U.K. territories of the Isle of Man and Guernsey. Press Release, European Comm'n, Standard Contractual Clauses for the Transfer of Personal Data to Third Countries - Frequently Asked Questions (Jan. 7, 2005), *available at* europa.eu/rapid/pressReleasesAction.do?reference=MEMO/05/3&format=HTML&aged=0&language=EN.

messy and ad hoc.[37] Indeed, the designation of "third countries" in the Data Protection Directive is somewhat archaic, given the extensive responsibilities that private actors have for safeguarding consumer data; it is not clear what, exactly, the responsibility of the recipient country should be.[38] In any case, it has been argued that the adequacy determination is not a "credible" determination of how data is actually processed, but rather a judgment of the degree to which the data protection scheme mirrors that of the European Union.[39]

Given the absence of formally binding international instruments in this area, the presence of soft law and overlapping norms that shape the development of law is of particular interest. Information privacy regulation in both the European Union and United States stems from a set of "fair information practice" principles, or FIPPs.[40] In the United States, these principles originated in a 1973 Department of Housing, Education and Welfare (HEW) report that recommended the establishment of a "Code of Fair Information Practices" that protected individuals' rights to consent to use of their data, to access and amend that data, and to know about the existence of the records.[41] Similarly, the 1980 OECD guidelines on privacy urge member states to adopt legislation, promote self-regula-

37. *See, e.g.*, Client Alert, Morrison & Foerster LLP, EU Data Protection Requirements: An Overview for Employers (Mar. 9, 2004), *available at* http://www.mofo.com/pubs/xpqPublicationDetail.aspx?xpST=PubDetail&pub=7569 ("The rules are extensive and still evolving. They also differ significantly from Member State to Member State.").

38. *See* ROBINSON ET AL., RAND CORPORATION, REVIEW OF THE EUROPEAN DATA PROTECTION DIRECTIVE 33 (2009), *available at* http://www.rand.org/pubs/technical_reports/2009/RAND_TR710.pdf ("[Interviewees] believed that distinguishing between countries inside and outside the EU was unnecessary and counter-productive in the modern world. For multi-national organisations operating across boundaries but applying the same high standards of data protection across all geographical divisions, this mechanism made no sense and was seen as contrary to harmonisation and global trade.").

39. *Id.* at 33–34.

40. *See* FEDERAL TRADE COMMISSION, PRIVACY ONLINE: A REPORT TO CONGRESS 7 (1998), *available at* http://www.ftc.gov/reports/privacy3/priv-23a.pdf (citing core principles of notice, consent, access, security, and redress as common to American, European, and Canadian law).

41. U.S. DEP'T OF HEALTH, EDUC. & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS: REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS 29–30, 41–42, 50 (1973).

tion, provide for enforcement of laws and oversight, and (perhaps most importantly) provide for due process of data subjects to access and control their own data.[42] The OECD guidelines are notable in that, while non-binding, they broadly enshrine principles of data protection that have been adopted (or given lip service) across the board by member states as well as corporations.[43] The FIPPs in the OECD guidelines also undergird the Council of Europe Convention, the only binding international instrument on data protection, which provides for broad protections for citizens to access their own data—as well as broad exceptions in the realms of "[s]tate security, public safety, the monetary interests of the State or the suppression of criminal offences."[44]

In its privacy rankings of European nations, Privacy International (PI) employs a number of metrics, including democratic safeguards, enforcement, constitutional and statutory protections, visual surveillance, communications interception and retention, and oversight of the agencies tasked with conducting surveillance.[45] While much is made in the data protection literature of the issue of oversight, the relative merits of sectoral as opposed to comprehensive regulation, and the

42. OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (1980), *available at* http://www.oecd.org/internet/interneteconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. In 2011, the OECD adopted a recommendation on Internet policymaking that recognized its own earlier privacy guidelines and called for enhanced "multi-stakeholder co-operation in policy development processes" in order to keep the Internet open and free. Because much of the debate over data protection centers on online activity, these multi-stakeholder processes have become the linchpin of the data protection debate in the United States. *See, e.g.*, John Verdi, *The Privacy Multistakeholder Process Turns to Substance*, NAT'L TELECOMMS & INFO. ADMIN. (Aug. 28, 2012), http://www.ntia.doc.gov/blog/2012/ privacy-multistakeholder-process-turns-substance.

43. *See, e.g.*, INTERNET ADVERTISING BUREAU, SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING (2009), *available at* http://www.iab.net/media/file/ven-principles-07-01-09.pdf (recognizing "consumer control," "education," and "transparency" as core principles of regulation of online privacy).

44. Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data art. 9, Jan. 28, 1981, C.E.T.S. 108, *available at* conventions.coe.int/Treaty/en/Treaties/Html/108.htm.

45. Privacy International, European Privacy and Human Rights 42–44, *available at* https://www.privacyinternational.org/sites/privacyinternational.org/files/file-downloads/ephr.pdf.

presence or absence of a "right to privacy" in constitutions, PI's criteria point to an important observation: data protection issues do not exist in a vacuum, but are essentially related to other features of the state and constitution that permit surveillance, in varying degrees, by state and private entities.[46]

B. *Privacy Law in Europe and America*

While binding international regulation on data transfers and data protection is vague, incomplete, and generally lacking, European regulation is profuse. Article 8 of the European Convention on Human Rights enshrines the right to privacy, subject to limitation "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."[47] Litigation of the bounds of Article 8 has clarified somewhat the scope of the right. In general, the Court has engaged in a multi-step test in these inquiries: It first finds whether there was an infringement on Article 8, in which case it asks whether the surveillance was "authorized by law" and whether it was necessary to defend democracy.[48]

Thus, in *Klass*, the European Court of Human Rights (ECtHR) held that a German law permitting surveillance of post and telecommunications did not violate Article 8 because the subject of surveillance was notified as soon as was possible and because the safeguards in place would prevent the authorities from abusing their power.[49] In *Malone v. UK*, in contrast, the Court expanded on the notion of what it means for surveil-

46. Thus, in the European context, data protection law cannot be understood without reference to norms governing privacy more generally, including Article 8 of the European Convention on Human Rights, known as the ECHR, and individual national constitutions.

47. European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14 art. 8, Nov. 4, 1950, E.T.S. no. 5 [hereinafter ECHR]. The International Covenant on Civil and Political Rights, Dec. 16, 1966, 6 I.L.M. 368 [hereinafter ICCPR], also enshrines a right to privacy in Article 17, which is a derogable commitment.

48. Klass v. Germany, App. No. 5029/71 Eur. Ct. H.R. (Sept. 6, 1978), ¶¶ 43–44, http://hudoc.echr.coe.int/sites /eng/pages/search.aspx?i=001-57510; Malone v. United Kingdom, App. No. 8691/79 Eur. Ct. H.R. (Aug. 2, 1984), ¶ 62, http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57533.

49. Klass, App. No. 5029/71, ¶¶ 58–59.

lance to be "authorized," writing, "the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference" with Article 8 rights.[50] In *Malone*, the U.K. government suspected Malone of dealing in stolen goods, so (after obtaining a warrant) it placed a tap and a pen register[51] on his telephone. Finding that the relevant law on the issuance of warrants was rife with "attendant obscurity and uncertainty," the Court held that the surveillance was not "in accordance with the law."[52] Finally, in the paired cases of *Huvig v. France* and *Kruslin v. France*, with facts similar to *Malone*, the Court held that France's law on wiretapping did not adequately provide "clear, detailed rules," with the effect that the law had inadequate safeguards against abuse.[53] In so holding, the Court made clear that France had to set the safeguards out in law, rather than relying on its judicial culture to prevent abuse.

Building on the ECtHR's privacy jurisprudence are the several European Directives that directly address citizens' rights to privacy in the data protection and electronic contexts. Article 7 of the Data Protection Directive, which enshrines the notion that under many circumstances a data subject must consent to the collection, processing, and use of his or her data, and will later have access to that data, is among the most important substantive guarantees.[54] In 2002, another

50. Malone, App. No. 8691/79, ¶ 67.

51. A pen register records the numbers dialed from a phone, but not the conversations.

52. Malone, App. No. 8691/79, ¶¶ 79–80.

53. Huvig v. France, App. No. 11105/84 Eur. Ct. H.R. (Apr. 24, 1990), ¶¶ 32, 34, http://hudoc.echr.coe.int/sites/eng/ pages/search.aspx?i=001-57627.

54. Data Protection Directive, *supra* note 4, art. 7. User consent is at the core of the FIPPs, as well as the FTC "notice-and-choice" model that gave rise to the proliferation of privacy policies. *See* FEDERAL TRADE COMMISSION, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 2 (2012) ("The 'notice-and-choice model,' which encouraged companies to develop privacy policies describing their information collection and use practices, led to long, incomprehensible privacy policies that consumers typically do not read, let alone understand."). Choice is at the core of the "do not track" debate as well, which has given rise to a debate about whether consumer choice is accurately reflected in browser default settings communicating a preference not to be tracked.

Directive directly addressed regulation for electronic communications providers, exempting the regulations for state security that would be carried out by member states.[55] More recently, the European Union passed the Data Retention Directive, setting out rules for service providers to maintain data for a given period of time, noting, "retention of data has proved to be such a necessary and effective investigative tool for law enforcement in several Member States, and in particular concerning serious matters such as organized crime and terrorism," that a comprehensive data retention law was deemed immediately necessary.[56]

Most recently, proposed revisions to the European Union framework include for the first time a Directive specifically geared toward the use of personal data by government actors in the context of law enforcement. Before the passage of the Treaty of Lisbon, police and judiciary cooperation in criminal law enforcement was a "third pillar" matter, to be regulated by member states.[57] Now that the former third pillar falls under the rubric of the European Union, however, the Commission has proposed a new Directive to define "rules relating to processing of personal data for the purposes of prevention, investigation, detection or prosecution of criminal offences or

---

See id. at 35 ("Two trade organizations argued that the framework should identify those practices for which choice is appropriate rather than making choice the general rule . . . . The majority of commenters, however, did not challenge the proposed framework's approach of setting consumer choice as the default."); *see also* Letter from Randall Rothenberg, President and CEO, Internet Advertising Bureau, to the Federal Trade Commission (May 31, 2012), *available at* https://www.iab.net/public_policy/InternetExplorer ("We do not believe that default settings that automatically make choices for consumers increase transparency or consumer choice.").

55. Directive 2002/58, of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 2002 O.J. (L 201) 37, 38 ("E-Privacy Directive").

56. Directive 2006/24, of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC, 2006 O.J. (L 105) 54, 55 [hereinafter Data Retention Directive].

57. Pre-Lisbon, criminal matters were essentially beyond the ambit of European Union law. *See, e.g.*, Case C-176/03, Comm'n v. Council, 2005 E.C.R. I-7907. ("[N]either criminal law nor the rules of criminal procedure fall within the Community's competence").

the execution of criminal offences."[58] The new Directive would permit the transfer of data to third countries if "necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties," assuming compliance with safeguards set up in the Directive.[59]

It is worth noting that the requirements for safeguards in the new proposed Directive are far less stringent than the ones in the original Data Protection Directive, probably because the Directive deals explicitly with the exceptional circumstances surrounding law enforcement. In the Directive, for example, a data subject may "object at any time on compelling legitimate grounds . . . to the processing of data relating to him, save where otherwise provided by national legislation."[60] In the Regulation, in contrast, the controller may override an objection if it "demonstrates compelling legitimate grounds for the processing which override the interests or fundamental rights and freedoms of the data subject."[61] National legislation is thus no longer required for data controllers to rebut objections to processing. In addition, the relationship of the proposed new Directive to terrorism investigations is unclear, as European counterterrorism strategy overlaps with, but is in some ways distinct from, criminal law enforcement.[62]

American law on privacy differs sharply from European law in several respects. The United States Constitution does not enshrine a "right to privacy," although several provisions have been read to supply that right.[63] The Fourth Amend-

---

58. *Proposal for a Directive of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of Such Data,* at 6, COM (2012) 10 final (Jan. 25, 2012), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:EN:PDF.

59. *Id.* at 41.

60. Data Protection Directive, *supra* note 4, art. 14.

61. *General Data Protection Regulation, supra* note 27, art. 19.

62. *See* Kim Lane Scheppele, *Other People's PATRIOT Acts: Europe's Response to September 11*, 50 LOY. L. REV. 89, 94 (2004) ("With respect to terrorism offenses, one might say that September 11 created pressure for harmonization of domestic criminal law across the EU faster than previously thought possible.").

63. *See, e.g.*, Griswold v. Connecticut, 381 U.S. 479, 482, 484–85 (1965) (holding that the First, Third, Fourth, Fifth, and Ninth Amendments all implicate a "right to privacy").

ment's warrant requirement and protections against unreasonable search and seizure are the most classic source of citizens' privacy rights vis-à-vis the government.[64] In addition, the First Amendment has been read to guarantee free and anonymous speech,[65] and the Fourteenth Amendment's substantive due process guarantee has been considered a source of privacy rights in the family, the body, and intimate relations.[66] State constitutional provisions largely mirror those of the federal constitution, but ten states have enshrined explicit rights to privacy in their constitutions.[67]

Federal legislation protects privacy in an array of areas, including financial,[68] communications,[69] public records,[70] and health, educational, and consumer records.[71] In recent years, many states have also enacted data breach notification statutes to compel companies to disclose breaches related to personal

64. U.S. CONST. amend. IV; *see also Griswold*, 381 U.S. at 485 (quoting Mapp v. Ohio, 367 U.S. 643, 656 (1961)) (stating that the Fourth Amendment creates a right to privacy "no less important than any other right carefully and particularly reserved to the people").

65. McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 357 (1995) ("Under our Constitution, anonymous pamphleteering is not a pernicious, fraudulent practice, but an honorable tradition of advocacy and of dissent.").

66. *See, e.g., Griswold*, 381 U.S. at 486 (characterizing the right to marriage as a "right of privacy older than the Bill of Rights"); *see also* 381 U.S. at 500 (Harlan, J., concurring) (arguing that the ban on contraception use within marriage infringed the Due Process Clause); *see also Lawrence v. Texas*, 539 U.S. 558 (2003) (invalidating a prohibition on sodomy as inconsistent with the Due Process Clause).

67. Those states are Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina, and Washington. *See* PRIVACY PROTECTIONS IN STATE CONSTITUTIONS, NAT'L COUNCIL OF STATE LEGISLATURES, http://www.ncsl.org/issues-research/telecom/privacy-protections-in-state-constitutions.aspx (last visited Nov. 17, 2012).

68. *E.g.*, Fair Credit Reporting Act, 15 U.S.C. § 1681 (2011); Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401–3422 (2011).

69. *E.g.*, Foreign Intelligence Surveillance Act of 1978, 15 U.S.C. §§ 1801–1812 (2006); Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–2522, 2701–2709 (2006).

70. *E.g.*, Privacy Act of 1974, 5 U.S.C. § 552a (2012); Drivers' Privacy Protection Act of 1994, 18 U.S.C. §§ 2721–2725 (2012).

71. *E.g.*, Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104–191 (1996); Family Educational Rights and Privacy Act of 1974, 20 U.S.C. §§ 1221, 1232g (2011); Cable Communications Policy Act of 1984, 47 U.S.C. § 551 (2012); Video Privacy Protection Act of 1988, 18 U.S.C. §§ 2710–2711 (2012).

data.[72] The statutory differences between European and American law are perhaps the most discussed aspect of the divergence between the two systems.[73] The "sectoral" approach, it is said, means that "protections frequently lag behind" those in Europe,[74] and was one of the reasons for developing the Safe Harbor Agreement that permitted data transfers after the passage of the Data Protection Directive in 1995.[75]

U.S. jurisprudence on privacy is wide-ranging and complex, and relates largely to intrusions by the government. In 1967, the seminal case of *Katz v. United States* held that a warrant was required to wiretap a public phone, reversing decades of decisions finding that whether an intrusion was a "search" protected by the Fourth Amendment depended on whether it intruded on a constitutionally protected area.[76] *Katz*, in contrast, held that privacy was the "right to be let alone"—regardless of where one found oneself.[77] Justice Harlan's concurrence in *Katz* established the two-part test for defining the scope of Fourth Amendment searches—"first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[78]

Since *Katz*, however, a large loophole has been carved out for searches of information shared with third parties. In 1976, the Supreme Court held in *United States v. Miller* that citizens

---

72. *State Security Breach Notification Laws*, National Conference of State Legislatures, http://www.ncsl.org/issues-research/telecommunications-information-technology/security-breach-notification-laws.aspx (last visited Feb. 15, 2013).

73. *See, e.g.*, Shaffer, *supra* note 34, at 26 ("While U.S. data privacy protection may be adequate under EU standards in some sectors, it was thought inadequate in most."); *see also* PRIVACY INTERNATIONAL, EUROPEAN PRIVACY AND HUMAN RIGHTS 42 (2010), *available at* https://www.privacyinternational.org/sites/privacyinternational.org/files/file-downloads/ephr.pdf (writing that sectoral legislation is "additional" to comprehensive legislation).

74. Banisar and Davies, *supra* note 18, at 14.

75. *See* Shaffer, *supra* note 34, at 59 ("In an effort to demonstrate to the European Union that privacy protection can be assured through business self-regulation and, in the process, shield U.S. businesses engaged in self-regulation from data transfer restrictions, Commerce issued a draft of 'Safe Harbor Principles' in November 1998 . . . .").

76. Katz v. United States, 389 U.S. 347, 351 (1967) ("[T]he Fourth Amendment protects people, not places.").

77. *Id.* at 350.

78. *Id.* at 361 (Harlan, J., concurring).

had no expectation of privacy in the data they share with their banks.[79] Likewise, the Court extended the carve out in 1979 to include transactional records kept by phone companies.[80] This lacuna has come to be known as the "third-party doctrine," which essentially defines information shared with a third party as beyond the scope of the Fourth Amendment.[81] This degree of government access to personal information is far beyond the scope of anything imagined under European jurisprudence on Article 8.

Technological innovation further complicates the picture of third-party doctrine by rapidly eroding the distinction between content and non-content information. As transactions increasingly take place on the Internet, internet service providers host a huge amount of personal information, both transactional and content related. The Electronic Communications Protection Act distinguishes between records that include "content" from those that do not, requiring that government authorities obtain a warrant before getting content information. What records are "content" and what are not is unclear. In *United States v. Warshak*, the Sixth Circuit held that citizens retain a reasonable expectation of privacy in the contents of their email.[82] However, Orin Kerr points out that it is sometimes very difficult to distinguish content from "envelope" information—not only conceptually, but also logistically.[83]

---

79. 425 U.S. 435, 442–44 (1976).

80. Smith v. Maryland, 442 U.S. 735, 740–42, 745–47 (1979).

81. *See* Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 596–601 (2011) (summarizing the development of a third party doctrine in U.S. jurisprudence), *and* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 566–70 (2009) (summarizing the development of the third-party doctrine); *see also* United States v. Jones, 565 U.S. __ (2012) (Sotomayor, J., concurring) ("[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties." (citing Smith v. Maryland, 442 U.S. 735, 742 (1976) and United States v. Miller, 425 U.S. 435, 443 (1976))).

82. United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) (holding that a subscriber of a commercial Internet service provider enjoyed a reasonable expectation of privacy in his emails, but leaving open the question whether contractual terms may sometimes suffice to eliminate that expectation).

83. *See* Orin S. Kerr, *Internet Surveillance Law After the USA PATRIOT Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 613–15 (2003) (explaining that in some cases content and envelope may be bundled and transmitted in a single, indivisible "packet" of information). Additionally, the inclusion of

C. *Understanding the Divergence*

An all-encompassing definition of privacy is hard to find; Daniel Solove suggests that even within the United States' legal tradition, the notion of "privacy" is incoherent, arguing, "[i]t is no accident that various problems are referred to as privacy violations; they bear substantial similarities to each other. But we also must recognize where they diverge."[84] Scholars and policymakers often deem the European approach, which treats privacy as a "fundamental right," to be at odds with the American approach, which frequently balances between competing interests. At least two accounts of this divergence emerge in the literature. Either the two traditions have evolved very different conceptions of privacy, which their respective laws reflect, or one approach simply protects privacy "more" than the other.

In James Whitman's account of the divergence, European law protects a dignitarian conception of privacy, while American law is focused more on protecting privacy as it pertains to liberty. "When continental lawyers speak of 'privacy' as a set of rights over the control of one's image, name, and reputation, and over the public disclosure of information about oneself, they are speaking to these selfsame continental sensibilities."[85] In contrast, Francesca Bignami argues that divergences in

---

"content" information in the "envelope" would conceivably render that information no longer subject to the Fourth Amendment under third-party doctrine, even though the user did not know or intend the content of his email to be shared. And certain types of activity do not lend themselves to the "content/envelope distinction." *See, e.g.*, Matthew D. Lawless, *The Third Party Doctrine Redux: Internet Search Records and the Case for a "Crazy Quilt" of Fourth Amendment Protection*, 11 UCLA J. L. & TECH., 2007, no. 2, 2007, at 1, 18 ("Internet search records bear no characteristics that would make them wholly analogous to either content or envelope information ex ante."); *see generally* Ian James Samuel, *Warrantless Location Tracking*, 83 N.Y.U. L. REV. 1324, 1332 (2008) (arguing that location tracking information does not readily fit within the content/envelope distinction).

84. Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 486 (2006).

85. James Q.Whitman, *The Two Western Cultures of Piracy: Dignity Versus Liberty*, 113 YALE L.J. 1153, 1167 (2004); *see also* EDWARD J. EBERLE, DIGNITY AND LIBERTY: CONSTITUTIONAL VISIONS IN GERMANY AND THE UNITED STATES 62 (2002) (explaining the German conception of constitutional "personality rights" as an outgrowth of human dignity and "Kant's theory of moral autonomy").

counterterrorism policy disclose merely that "liberty is protected more in Europe than in the United States."[86] Bignami attributes divergence in regulation of the public sector to gaps in enforcement and executive power, and to Europe's "particularly vivid understanding of the possible abuses of state power."[87]

Understanding the extent of the normative divergence between Europe and the United States is crucial to assessing the success of the Terrorist Finance Tracking Program as an instrument of global administrative law. Given the two statutory schemes' common sources in FIPPs, the differences do not seem to be deeply ideological, but rather more profoundly rooted in choices about implementation. Where the United States has embraced industry self-regulation, and legislation only in the event of serious breaches, the European Union has engineered a more holistic approach that seeks to anticipate privacy-invading technological developments before they happen.

II. THE TERRORIST FINANCE TRACKING PROGRAM

A. *Characterizing the TFTP*

In 2006, Eric Lichtblau and James Risen—the same journalists who broke the story of the National Security Agency's warrantless wiretapping operations—informed readers of the *New York Times* that the Central Intelligence Agency and Treasury Department had accessed "tens of thousands" of financial records from the Society for Worldwide Interbank Financial Transactions (SWIFT) using administrative subpoenas.[88] The novel part of the arrangement was in its scope: Rather than using warrants or subpoenas to access individual transactions, or transactions related to a particular suspect, the Terrorist Finance Tracking Program sifted through millions of records contained in a database.[89] Indeed, in testimony before a House subcommittee after the New York Times article had run, Treasury Undersecretary Stuart Levey maintained that because of the restrictions on use of the database, the Treasury

86. Francesca Bignami, *European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining*, 48 B.C. L. REV. 609, 612 (2007).

87. *Id.* at 688.

88. Lichtblau & Risen, *supra* note 1.

89. *Id.*

Department had accessed "only a minute fraction of the data that SWIFT has provided."[90]

Although most of the reports on the TFTP did not make clear the exact contours of the database to which the United States gained access, a few aspects are evident. First, the SWIFT database encompassed the data of many European and American citizens.[91] Second, the United States did not gain access to *all* of SWIFT's data—although it is not clear to what extent the cooperative would have access to routine American financial transactions in the first place, the subset of data which the government could access certainly did not include information on American ATM transactions, etc.[92] Third, in order to process the vast quantities of information to which the Department had suddenly gained access, it needed to use sophisticated technological tools.[93]

In response to the disclosures, the data protection authorities of the European Union and of the member states initiated investigations and protests. The Article 29 Data Protection Working Party, an independent European Commission advisory body, issued an opinion stating that the mere "processing and mirroring" of data in SWIFT's United States servers violated the Data Protection Directive, not to mention the transfer of that data to the Treasury.[94] "The lack of trans-

90. Testimony of Stuart Levey, Under Secretary for Terrorism and Financial Intelligence, U.S. Department of the Treasury, Before the House Financial Services Subcommittee on Oversight and Investigations, 109th Cong. (2006), *available at* http://archives.financialservices.house.gov/media/pdf/071106sl.pdf.

91. Lichtblau & Risen, *supra* note 1 ("One person involved in the Swift program estimated that analysts had reviewed international transfers involving 'many thousands' of people or groups in the United States.").

92. *See* Testimony of Stuart Levey, *supra* note 90, at 30 (claiming that no ATM transactions were included in the data set transmitted by SWIFT).

93. *See, e.g.*, Ekrem Duman & Ayse Buyukkaya, *Money Laundering Detection Using Data Mining, in* MINING MASSIVE DATA SETS FOR SECURITY 287 (F. Fogelman-Solié et al. eds., 2008) (identifying problems with using "rule-based" detection techniques to implement anti-money laundering systems and suggesting a two-phase anti-money laundering system that uses data mining instead).

94. ARTICLE 29 DATA PROTECTION WORKING PARTY, OPINION 10/2006 ON THE PROCESSING OF PERSONAL DATA BY THE SOCIETY FOR WORLDWIDE INTERBANK FINANCIAL TELECOMMUNICATION (SWIFT) 21 (2006), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp128_en.pdf.

parency and adequate and effective control mechanisms that surrounds the whole process . . . represents a serious breach" of the Data Protection Directive, the Working Party concluded.[95] The Belgian Data Protection Authority issued a preliminary opinion on the issue concluding that SWIFT's failure to notify its customers and its decision to transfer data to the United States violated the Data Protection Directive, although it acknowledged that SWIFT was in a conflict of laws situation with regard to the dueling objectives of European data privacy law and the American subpoenas.[96]

In response, the European Union and the United States negotiated a stopgap solution by which SWIFT would join the Safe Harbor agreement, making the certifications necessary for it to be able to transfer personal data to the United States.[97] In addition, the Treasury made unilateral representations to the Commission describing the "rigorous controls and safeguards" in the program.[98] Negotiations continued for a more comprehensive solution. In November 2009 the European Commission and the United States reached a draft short-term agreement on bank data transfers,[99] which the European Parliament voted down in February 2010.[100]

---

95. *Id.* at 26.

96. Commission de la Protection de la Vie Privée [Belgian Data Protection Authority], *Avis relatif à la transmission de données à caractère personnel par la SCRL SWIFT suite aux sommations de l'UST* [*Opinion on the Transfer of Personal Data by the CSLR SWIFT by Virtue of UST (OFAC) Subpoenas*], SA2 / A / 2006 / 035, at 21 (Sept. 27, 2006), *available at* http://www.statewatch.org/news/2006/sep/swift-belgium-opinion-fr.pdf (last visited Mar. 11, 2013).

97. *See SWIFT Safe Harbor Policy*, SWIFT, http://www.swift.com/about_swift/legal/compliance/data_protection_policies/swift_safe_harbor_policy.page (last updated July 17, 2012) (describing the Safe Harbor program); *see also Organization Information*, http://safeharbor.export.gov/companyinfo.aspx?id=15776 (showing that SWIFT was certified in July 2007) (last visited Mar. 4, 2013).

98. Letter from United States Department of the Treasury regarding SWIFT/Terrorist Finance Tracking Program (EU) No. 09/2007 of 20 July 2007, 2007 O.J. (C 166) 7, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:166:0017:0017:EN:PDF.

99. Agreement, *supra* note 3.

100. Press Release, European Parliament, SWIFT: European Parliament Votes Down Agreement with the US (Feb. 11, 2010), *available at* http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+IM-PRESS+20100209IPR68674+0+DOC+XML+V0//EN.

In July 2010, the European Parliament passed a new bank transfers deal, which took effect the following month.[101] The new agreement purportedly addressed the Parliament's concerns with the earlier version, which did not adequately address the substantive issues associated with data protection and did not provide an adequate "redress mechanism."[102] In response to these concerns, the TFTP agreement as implemented installs Europol, the European law enforcement agency, as an intermediary body to "verify" United States requests to European Union-based holders of bank data, and imposes a number of conditions on the United States Treasury when making its requests, including specifying necessity, clear identification of the data, and narrow tailoring of the requests.[103] The next section of this Note addresses whether the new TFTP agreement embodies rules that can be considered as adequate as a mechanism of global administrative law.

B. *The TFTP as a Mechanism of Global Administrative Law*

Nominally, at least, the European backlash against TFTP was prompted by the lack of procedural protections in the program. In the aftermath of the press's disclosures, European data privacy activists decried the lack of oversight,[104] notice,[105] opportunity to challenge the collection,[106] and the very nature of the subpoenas.[107] Strictly speaking, the TFTP might be viewed as a more classic example of international lawmaking—a bilateral agreement between two nations geared toward solving a specific problem.[108] Yet the program's role as a method of extending intergovernmental standards on safeguarding privacy to a national regime makes it more complex. The

101. Agreement, *supra* note 3.

102. Press Release, *supra* note 100.

103. Agreement, *supra* note 3, art. 4.

104. ARTICLE 29 DATA PROTECTION WORKING PARTY, *supra* note 94, at 19–20 (discussing the implications of failure to notify European data protection authorities).

105. *Id.* (failure to notify data subjects).

106. *Id.* at 11 ("SWIFT decided to comply with the US subpoenas.").

107. *Id.* at 8 ("The scope of the UST subpoenas in this case is materially, territorially and in time very wide . . . .").

108. Kingsbury et al., *supra* note 14, at 25 ("[I]n some areas of regulatory administration, such as international security, the classical view that global governance is directed at the behavior of governments toward other governments, rather than toward private actors, still has great force.").

TFTP exists at the overlap of several distinct subject areas within the global administrative space and embodies some of the distinct characteristics of mechanisms operating within that space. Particularly, as Kingsbury et al. point out, the TFTP is an example of a scenario in which "the decisions of domestic administrators are increasingly constrained by substantive and procedural norms established at the global level; the formal need for domestic implementation thus no longer provides for meaningful independence of the domestic from the international realm."[109]

The roots of the TFTP exemplify the classic traits evident in global administrative law mechanisms more generally. The TFTP is oriented toward restraining not only government actors, but also private actors who, by their very nature, engage in data collection and analysis.[110] Its implementation of Europol as the reviewing body superimposes another level of review onto the respective administrative review mechanisms extant in European and American law. At the same time, however, the TFTP remains riddled with gaps that make its value as a GAL mechanism highly questionable. Specifically, as addressed below, while the Agreement is meant to realize common procedural and substantive norms of privacy protection, it fails to do so. More seriously, by failing to implement meaningful redress or provide for "reasoned decisionmaking" on the part of Europol, the TFTP agreement achieves neither meaningful legality, reasoned decisionmaking, nor effective review.[111]

In assessing the TFTP's success, or lack thereof, as an instrument of Global Administrative Law, traditional conceptions of the distinction between substance and procedure do not always play out as expected with regard to legal protections for privacy. As a GAL mechanism, the TFTP is best understood as offering both substantive and procedural privacy protections. As I demonstrate, these protections overlap significantly, both in the guarantees offered by the TFTP itself as well as in the European privacy laws with which it must comply. Articles

109. *Id.* at 26.

110. *See* Commission de la Protection de la Vie Privée, *supra* note 96, at 20–21 (chastising SWIFT for complying with U.S. subpoenas and for maintaining servers in the United States more generally).

111. Kingsbury et al., *supra* note 14, at 28.

6, 7, 25, and 26 of the Data Protection Directive, which articulate, respectively, the conditions for the principles of data quality and proportionality, legitimacy of processing, principles for data transfers to a third country, and conditions for derogations from those principles, create a hodgepodge of substantive and procedural protections for personal data.[112] In contrast, Articles 10, 11, 18, 19, and 20 offer concrete procedural requirements with which data controllers must comply.[113]

Article 6 of the Directive requires that personal data be accurate, processed "fairly and lawfully" and for "specified, explicit and legitimate purposes," and that it not be retained for longer than necessary.[114] It also imposes a requirement that processing be proportional to the initial purpose for which data was collected.[115] Article 7 articulates the conditions under which data processing is "legitimate": unambiguous consent of the subject, or that it is necessary for fulfillment of a contract, compliance with a legal obligation, protection of the "vital interests" of the subject, "performance of a task carried out in the public interest," or the legitimate interests of the data controller.[116]

These conditions substantially mix the procedural and substantive interests at stake. Indeed, perhaps the biggest distinction between the Fair Information Practices that undergird U.S. and EU privacy law and the provisions of European law itself is the specification of procedures to protect privacy. The requirement that data be processed "lawfully" and for "specified, explicit and legitimate purposes" implies that national law provides the procedures by which a company can comply. And, indeed, member states' data protection laws require that data processors inform consumers of the use and purpose of their data processing.[117] But the proportionality requirement

112. Data Protection Directive, *supra* note 4, arts. 6, 7, 25, 26.

113. *Id.* arts. 10, 11 (setting out the scope of information to be given to the data subject); arts. 18–21 (setting out the obligation to notify the Member State's supervisory authority, the scope of notification requirement, and the obligation of supervisory authority to conduct checks and to publicize operations).

114. *Id.* art. 6(1).

115. *Id.* art. 6(1)(c) ("adequate, relevant and not excessive").

116. *Id.* art. 7.

117. *See, e.g.*, Bundesdatenschutzgesetz [BDSG] [Federal Data Protection Act], Sept. 1, 2009, BGBL. 2009 I at 2814, § 4(2) (Ge.); Loi relative à la pro-

in Article 6 is not always met with substantive definitions in national law. In the Belgian privacy law, in fact, the Directive's requirements are simply reiterated, not elaborated upon, whereas in the German privacy law they are not even repeated.[118] Thus, while some of the Directives' requirements clearly embody procedural requirements to satisfy substantive norms of notice and limitation on data use, others raise more questions than they answer.

In the TFTP case, the German chancellor interpreted German data protection law to be amenable to data sharing of the kind Treasury sought.[119] German members of European Parliament (MEPs), however, led the charge against the TFTP in the European Parliament, angering Angela Merkel and jeopardizing the transatlantic relationship.[120] In fact, one of the MEPs' reactions to the ultimate TFTP deal was to call for an international binding agreement on the content of the definition of privacy—a notion that, given the amount of strife both transatlantically and within Europe on this issue, seems laughable.

Europol's Joint Supervisory Body (JSB) reviewed Europol activities in November 2010 for compliance with these procedures. While many of their findings remain classified,[121] the conclusion is stunning. The JSB found that Treasury's requests were "almost identical in nature," so "abstract" and "broad" as to render it "impossible" to assess whether they were in compliance with the terms of the agreement. Moreover, JSB noted, "[i]nformation provided orally—to certain Europol staff by

---

tection des données à caractère personnel [Privacy Protection in Relation to the Processing of Personal Data] of Dec. 8, 1992, Moniteur Belge [M.B.] [Official Gazette of Belgium], Feb. 3, 1999, 3049, art. 9.

118. *Id.* art. 4, § 1.

119. *See* Cable from American Embassy Berlin to Depts. Of Treasury, Homeland Security, Justice et al., Chancellor Merkel Angered by Lack of German MEP Support for TFTP (Feb. 12, 2010), *available at* http://wikileaks.org/cable/2010/02/10BERLIN180.html (indicating that Merkel had "personally lobbied" German MEPs to support the agreement and that they voted against it anyway).

120. *Id.*

121. EUROPOL JOINT SUPERVISORY BODY, REPORT NO. JSB/INS. 11-07, REPORT ON THE INSPECTION OF EUROPOL'S IMPLEMENTATION OF THE TFTP AGREEMENT 5 (2011), *available at* http://europoljsb.consilium.europa.eu/media/111009/terrorist%20finance%20tracking%20program%20(tftp)%20inspection%20report%20-%20public%20version.pdf.

the US Treasury Department, with the stipulation that no written notes are made—has had an impact upon each of Europol's decisions; however, the JSB does not know the content of that information."

As a matter of global administrative law, JSB's findings indicate a severe accountability deficit. Accountability mechanisms are meant to share four features:

> (1) a specified accountor, who is subject to being called to provide account including, as appropriate, explanation and justification for some specified aspect or range of his conduct; (2) a specified account holder or accountee; (3) authority on the part of the accountee to demand that the accountor render account for his performance; and (4) the ability and authority of the account holder to impose sanctions or secure other remedies for performance that he judges to be deficient or, in some cases, to confer rewards for superior performance.[122]

In this case, while the first three features are present, the "account holder"—JSB—has no practical ability to impose sanctions on the Treasury for failing to comply. Moreover, JSB's report suggests not only that the Treasury may not be complying with the terms of the agreement, but also that *the very nature of the manner in which the requests are made renders it impossible for the supervising body to do its job.* From the perspective of global administration, the failure of procedures at this level is even more troubling than the potential disregard for substantive norms, as it implies that transparency and free access to information are also being disregarded. Because Europol (and, by extension, the JSB) is the primary source of accountability for EU citizens whose data are being requested, the suggestion that the very architecture of the agreement makes accountability and oversight impossible leaves open the question of whether the program can be accountable at all to a European citizen.

Equally troubling is the lack of a concrete redress mechanism, a problem at the heart of the European Parliament's initial rejection of the program. The agreement sets out rights of

122. Richard Stewart, Accountability, Participation, and the Problem of Disregard in Global Regulatory Governance 15 (Jan. 2008) (draft) (on file with author).

access and rectification for European citizens to verify that their information has been collected in compliance with the terms of the agreement.[123] In turn, the Treasury Department has published its "redress procedures," which essentially require that those whose requests are denied sue the Department under the Administrative Procedures Act and/or the Freedom of Information Act (FOIA).[124] If this requirement was merely onerous for European citizens, it would probably still be a permissible way of achieving judicial oversight of the program. But the nature of the Acts that the Redress Procedures cite is such that almost every request will be turned down under FOIA's national security exemption.[125]

Moreover, it is practically inexplicable that the agreement completely removes any redress mechanism within Europe itself. Not only does this place an extremely high burden on European citizens to familiarize themselves with American administrative law and to bear the high costs of litigating these (ultimately fruitless) suits, it also insulates the private actors whom it seeks to regulate from liability in their home jurisdictions by placing them completely outside of the scope of the Directive and providing an American remedy in its stead. Failing to provide a European remedy, in other words, intentionally overlooks the significance of European law on data protection in terms of negotiating the TFTP at the outset.

These characteristics of the TFTP—lack of redress, lack of accountability, and lack of oversight—should put to rest any illusions that European opposition to the program was based on principled objections to privacy-invasive activity. It is indeed difficult to see why, if European procedural protections are so strong, at least slightly more responsive mechanisms were not built into the program. I turn now to a final odd requirement within the TFTP agreement, Article 5's "safeguard" that "the TFTP does not and shall not involve data mining or any other

123. Agreement, *supra* note 3, art. 15.

124. DEP'T OF TREASURY, TERRORIST FINANCE TRACKING PROGRAM: REDRESS PROCEDURES FOR SEEKING ACCESS, RECTIFICATION, ERASURE, OR BLOCKING (2010), *available at* http://www.treasury.gov/resource-center/terrorist-illicit-finance/Terrorist-Finance-Tracking/Documents/Revised%20Redress%20Procedures%20for%20Web%20Posting%20(8-8-11).pdf.

125. 5 U.S.C. § 552(b)(1) (2000). Envtl. Prot. Agency v. Mink, 410 U.S. 73 (1973) (stating that the national security exemption prevents plaintiffs from obtaining any properly classified records).

type of algorithmic or automated profiling or computer filtering."[126] As I discuss in the next Part, it is precisely the existence of algorithmic filtering capabilities that makes bulk data transfers like those in the TFTP useful. This prohibition thus raises unanswerable questions about the content of the TFTP in a technological sense. More importantly, as I conclude, it presages important developments in the use of bulk data transfers that may not yet be ripe for international regulation.

III. IMPLICATIONS OF THE TERRORIST FINANCE TRACKING PROGRAM FOR "DATAVEILLANCE"

Although the TFTP is in large part conceived as an agreement to facilitate cooperation in the law enforcement and counterterrorism realm, it has much to say as well about the nature of evolving technology. Restrictions on bulk transfers, data processing, aggregation, and analysis techniques speak both to traditional concerns about limiting government's ability to surveil citizens and to novel concerns about the evolving capabilities of technology in conducting surveillance. And the TFTP is best understood in light of the fact that while formal and informal agreements on mutual legal assistance and cooperation among intelligence agencies are rich and plentiful, neither normative nor procedural limitations on the uses of technology are forthcoming. Independently operating agreements like the TFTP, thus, are prime examples of how global administration is stepping in to fill the gaps in a less-than-comprehensive manner.

The landscape of international technology governance is surprisingly bleak. Technological innovation is governed in large part by recourse to the international intellectual property regime, exemplified by the World Intellectual Property Organization and the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement).[127] The Internet Corporation for Assigned Names and Numbers (ICANN) controls the allocation of domain names, internet protocol (IP) addresses, and port and parameter numbers,[128]

126. Agreement, *supra* note 3, art. 5.

127. Katherine Strandburg, *Evolving Innovation Paradigms and the Global Intellectual Property Regime*, 41 CONN. L. REV. 861, 862–66 (2009).

128. *About Us*, ICANN, http://www.icann.org/en/about/welcome (last visited Nov. 15, 2012).

which is something like entrusting a nonprofit corporation to allocate street addresses, zip codes, and telephone numbers for the entire globe. With regard to internet governance in particular, some have raised the issue that developing nations have only an "advisory" role in influencing policy; despite seeing the internet as a global "public good," the U.S. government (through ICANN) has a monopoly on regulating it.[129] Others have noted that since TRIPS was concluded in 1994, and ICANN was chartered in 1998, technology has changed drastically—not just in terms of its capabilities, but also by shifting from a market-based model toward one of "user innovation and . . . open and collaborative innovative activity."[130]

This shift is telling not only with regard to internet governance (where much user innovation takes place) but also as shifts in communication and information technology more generally have far outpaced the expectations of the global technology governance regime writ large. As Strandburg puts it, a result of evolutions in communication technology is that "the open and collaborative innovation paradigm is able not only to find, make use of, and respond to heterogeneous and localized preferences and experience but also to operate via a global networked organizational structure which is not defined by geographical or political boundaries."[131] Yet just as the United States informally exercises control over the development of the Internet through ICANN, the European Union is drastically shaping the norms surrounding data privacy well beyond Europe's borders. As Gregory Shaffer points out, through the Article 25 constraints on data transfers, "European regulation casts a net wider than Europe. In a globalizing economy, European law also constrains U.S. domestic privacy policies and practices."[132] In the case of the TFTP, European data privacy legislation exhibited a clear preference against large-scale data-mining.

129. Surya Mani Tripathi et al., *Internet Governance: A Developing Nation's Call for Administrative Legal Reform*, 37 INT'L J. LEGAL INFO. 368, 382 (2009).
130. Strandburg, *supra* note 127, 871.
131. *Id.* at 884.
132. Shaffer, *supra* note 34, at 4.

The TFTP is a compelling example of a new form of surveillance, the contours of which are still being defined.[133] Three characteristics set "dataveillance" apart from its predecessor intelligence gathering and analysis techniques. First, dataveillance is general, not individuated; surveillance takes place inside a large dataset, not by looking for information on individual suspects. Second, dataveillance relies heavily on information collected or aggregated by private actors, reducing the costs imposed on the government to compile that information itself. Finally, dataveillance is conducted by using forms of analysis developed in large part by private actors.[134]

SWIFT is essentially a network or platform for financial institutions to communicate with each other securely. Its "core" service is the FIN messaging platform, which facilitates communication of financial transactions between banks and other institutions.[135] SWIFT provides an "end-to-end view on payment transactions and enquiries which eliminates the 'black hole' issue" for banks and their customers.[136] The network also permits the transfer of batched transaction information through its filesharing service, FileAct.[137] SWIFT publishes information on its traffic monthly, making clear that it provides support to thousands of financial institutions in more than 200 countries, and transmitting millions of FIN and FileAct messages daily.[138] It is easy to see the value of these messages in terms of financial intelligence: The same "end to end view" that benefits banking customers whose transactions get lost in the ether is the one that makes clear to the Treasury Department the pathways of terrorist finance.

The Terrorist Finance Tracking Program is just one of many financial surveillance tools in the Treasury Department's

133. Martin Kuhn dubs this form of surveillance "dataveillance," a moniker I adopt as well. MARTIN KUHN, FEDERAL DATAVEILLANCE: IMPLICATIONS FOR CONSTITUTIONAL PRIVACY PROTECTIONS (2007).

134. *Id.* at 4.

135. *FIN: Overview*, SWIFT, http://www.swift.com/products/fin (last visited Feb. 19, 2013).

136. *Reaching Your Counterparties*, SWIFT, http://www.swift.com/solutions/banks/reaching_your_counterparties.page (last visited Feb. 9, 2013).

137. *File Act: Overview*, SWIFT, http://www.swift.com/products/fileact (last visited Feb. 19, 2013).

138. *See* SWIFT IN FIGURES, JANUARY 2011, http://www.swift.com/about_swift/company_information/swift_in_figures (last visited Mar. 8, 2013).

arsenal. Indeed, in the oversight hearing that took place after the program's disclosure, several members of Congress raised the issue that much of terrorist finance took place through the *hawala* system rather than through Western-style banking.[139] Shane Harris reports that a separate team within Treasury, called Operation Green Quest, was responsible for surveillance of *hawala* transactions, going so far as to build dummy websites in order to trap users who might be donating to terrorist causes.[140]

But the TFTP differs tremendously from earlier programs, not only in the scope of the data it includes, but also in the methods by which that data is parsed and followed up to develop investigations. As the following analysis should show, both public and private actors maintain a veritable arsenal of tools by which to analyze vast quantities of data, but the methods by which that analysis is accomplished are subject to very different rules in the United States than in Europe. I turn now to technological developments that are changing the landscape of data usage and analysis.

A. *The Power of Data*

The study of the potential of very large data sets to disclose predictive patterns is at the heart of what is known as computational social science, an emerging field that supplies new technologies for exploring vast quantities of data. Private industry has developed numerous algorithms to find patterns and relationships among thousands or even millions of transactions. For example, Google data on the volume of queries associated with particular industries is correlated with economic activity in those industries, to the extent that the trends "predict the present."[141] Private industry accumulates and implements user data in a number of ways. Targeted advertising is perhaps the best-known example for consumers. In the United States, online tracking—the collection and usage of

139. *The Terror Finance Tracking Program: Hearing Before the Subcomm. on Oversight and Investigations of the H. Comm. on Financial Services*, 109th Cong. 28 (2006) (statement of Rep. Paul, Member, H. Comm. on Financial Services).

140. SHANE HARRIS, THE WATCHERS: THE RISE OF AMERICA'S SURVEILLANCE STATE 206–07 (2010).

141. Hyunyoung Choi & Hal Varian, *Predicting the Present with Google Trends*, 88 ECON. REC. (SPECIAL ISSUE) 2, 2 (2012).

large quantities of information about one's web browsing history—is governed only by industry self-regulation, not by statute.[142] This has resulted in an "opt-out" structure for consumer consent to data gathering,[143] and consequently the proliferation of open-source software and other alternatives to limit consumers' exposure.[144] In contrast, the European E-Privacy Directive requires consumers to consent *ex ante* to usage of their data for "value added services."[145] An economic analysis of behavioral advertising regimes discloses that the reasons for adopting an opt-in as opposed to opt-out rule is not economic as much as it is related to the "value" of personal privacy and the somewhat intangible "costs" incurred when third parties breach that right.[146]

---

142. Byron Acohido, *More Web Surfers Tell Trackers To Keep Out*, USA TODAY, Dec. 30, 2011, at B1 ("The FTC called for a Do Not Track mechanism that would enable Internet users to request not to be tracked . . . . But tracking and online advertising companies lobbied intensively to maintain industry self-policing as the status quo."); *see also* AM. ASS'N OF ADVER. AGENCIES ET AL., SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING 1, 15–16 (2009), *available at* http://www.iab.net/media/file/ven-principles-07-01-09.pdf (exemplifying a self-regulatory approach to online tracking).

143. *See* Andrea N. Person, *Behavioral Advertisement Regulation: How the Negative Perception of Deep Packet Inspection Technology May Be Limiting the Online Experience*, 62 FED. COMM. L.J. 435, 448–49 (2010) (noting that, though not required by law to do so, some companies have responded to congressional and media pressure by moving to more transparent, opt-in consent structures).

144. *See, e.g.*, GHOSTERY, https://www.ghostery.com (last visited Feb. 19, 2013); AD-BLOCK PLUS, https://addons.mozilla.org/en-US/firefox/addon/adblock-plus/ (last visited Feb. 19, 2013); TRACKERBLOCK, https://addons.mozilla.org/en-US/firefox/addon/trackerblock/ (last visited Feb. 19, 2013); *Prepared Statement of the Federal Trade Commission on Do Not Track: Before the Subcomm. on Commerce, Trade, and Consumer Protection*, 111th Cong. 16 (2010) (statement of David Vladeck, Dir. of the Bureau of Consumer Protection of the Fed. Trade Comm'n), http://www.ftc.gov/os/testimony/101202donottrack.pdf ("[T]he Commission supports a more uniform and comprehensive consumer choice mechanism for online behavioral advertising, sometimes referred to as 'Do Not Track.'").

145. Directive 2009/136, of the European Parliament and of the Council of 25 Nov. 2009 Amending Directive 2002/22/EC on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services, art. 6(3), 2009 O.J. (L 337) 11, 30–31 (EC).

146. Michael R. Hammock & Paul H. Rubin, *Applications Want To Be Free: Privacy Against Information*, 7 COMPETITION POL'Y INT'L 41, 46–47 (2011) (arguing that privacy advocates do not consider the "efficiency" of the default rule by not conducting a quantitative cost-benefit analysis).

The proliferation of information about users is a consequence of the proliferation of modern technology. Verizon Wireless has 94 million wireless subscribers;[147] AT&T has more than 100 million.[148] Data is routinely recorded on each subscriber, conveying information not just on usage of text messaging and data plans but also on location, movement, and patterns of communication.[149] Similarly, data on such disparate occurrences as credit card transactions, online searches, electricity usage, mammograms, and traffic jams is collected and stored by commercial providers.[150] This data provides a wealth of information on public health issues, social relations, and economic and geographic trends, which social scientists have embraced, finding new methods of mining and analyzing sources for new patterns of human behavior.

Not surprisingly, one of the first areas to use large amounts of privately available data was public health. In 2008, Google started its Predict and Prevent Initiative, a global health initiative designed to integrate information on livestock, human, wildlife, and agricultural disease issues, and to embrace digital detection technologies.[151] In 2009, a group of Google software engineers, statisticians, and social scientists published a paper on Google Flu Trends, a Google initiative that matched online search query patterns with the actual occurrence of influenza. The authors noted, "[b]ecause search

147. *Verizon Communications Fact Sheet*, VERIZON, http://216.70.96.173/themes/site_themes/agile_records/images/uploads/2Q12_VZ_Fact_Sheet.pdf.

148. *AT&T Reports Solid Earnings, Strong Cash Flow, Robust Mobile Broadband Sales and Improving Wireline Revenue Trends*, AT&T (Oct. 20, 2011), http://www.att.com/gen/press-room?pid=21794&cdvn=news&newsarticleid=33126&mapcode=financial.

149. *See, e.g.*, *AT&T Privacy Policy*, AT&T, http://www.att.com/gen/privacy-policy?pid=2506 (last visited Feb. 19, 2013) (indicating that the service collects and uses account information, usage information, and location information, and shares some of it, in some forms, with third parties).

150. *See generally* Jan Beyea, *The Smart Electricity Grid and Scientific Research*, 328 SCI. 979, 979–80 (2010) (discussing the increased access to customer data that is soon to be possible through the application of new technologies to electricity grids in the United States); *Google Privacy Policy*, GOOGLE, https://www.google.com/policies/privacy/ (last updated July 27, 2012) (discussing the collection and storage of credit card transactions, search queries, and more).

151. *Predict and Prevent*, GOOGLE.ORG (Oct. 14, 2008), http://www.google.org/Predict_Prevent_Brief.pdf .

queries can be processed quickly, the resulting ILI [influenza-like illness] estimates were consistently 1-2 weeks ahead of CDC ILI surveillance reports."[152] One of the authors of the paper, Larry Brilliant, later served as the chair of the National Biosurveillance Advisory Subcommittee, which endorsed (in vague terms) the use of "digital innovations" to speed detection and information, while acknowledging potential roadblocks in the form of rules about data sharing and intellectual property.[153] Google has since expanded its predictive search efforts in this area to dengue fever, using Dengue Trends to track outbreaks in the countries most affected by the illness.[154]

"Smart" technologies also offer potential troves of data that can solve many public health conundrums. "[T]he small, cheap electronic technologies embedded into medical devices, pharmaceuticals, and environmental sensors" can be used to track asthma and respiratory illness outbreaks in the Middle East and Asia, areas currently underserved by biosurveillance technologies.[155] Likewise, Jan Beyea argues that the many petabytes of data created by "smart meters," which transmit information on electricity usage to utility companies, have implications for epidemiological studies related to obesity, air pollution, and electromagnetic fields.[156] This latter example also has broad economic significance, as Beyea points out, in that electricity usage can be examined in connection with price, household income, and household size.

Similarly, Google has shown that for certain industries, such as automotive sales, online search query trends are positively associated with contemporaneous economic activity.[157] Likewise, Jure Leskovec analyzed a set of 90 million news and

152. Jeremy Ginsberg et al., *Detecting Influenza Epidemics Using Search Engine Query Data*, 457 NATURE 1012, 1013 (2009).

153. NAT'L BIOSURVEILLANCE ADVISORY SUBCOMM., IMPROVING THE NATION'S ABILITY TO DETECT AND RESPOND TO 21ST CENTURY URGENT HEALTH THREATS: FIRST REPORT OF THE NATIONAL BIOSURVEILLANCE ADVISORY SUBCOMMITTEE 9 (2009), *available at* http://www.cdc.gov/osels/pdf/NBAS%20Report%20-%20Oct%202009.pdf.

154. Google Dengue Trends, GOOGLE.ORG, http://www.google.org/denguetrends/.

155. David Van Sickle, *The Next Generation of Public Health Approaches to Asthma in Asia and the Middle East*, 22 ASIA-PACIFIC J. PUB. HEALTH 229S, 231S (2010).

156. Beyea, *supra* note 150, at 980.

157. Choi & Varian, *supra* note 141, at 7–8.

blog articles to show both how contemporaneous "memes"—"short, distinctive phrases that travel relatively intact through on-line text"—compete with each other and how the diffusion of information across the Internet is achieved.[158]

But the emergence of extremely large datasets has presented novel problems and questions for investigations of social relations and social networks. In one sense, this is almost redundant—each investigation of cell phone usage, Web sites visited, or search query patterns necessarily discloses something about users' interests and motivations. On the other hand, researchers have uncovered patterns that delve far more deeply into users' interests. Jure Leskovec's work quantifying how social networks affect purchasing decisions is one example.[159] Leskovec examines the influence of buyers upon each other and buyer-seller trust in the context of a large data set gleaned from Taobao, a Chinese e-commerce site, concluding that the greatest influence upon a user's decision to buy something is the user's previous communication through the site's social networking tool, and not the price or the seller rating.[160] In a separate study, Leskovec compares European cell phone data with two social networking sites that allow users to "check in" at specific locations, concluding that while most user travel can be explained by periodic tasks and static routines, long distance travel is correlated with visiting a far-away friend.[161]

The personal nature of many of these inquiries makes it easy to see how Europeans concerned about the implications of technology for civil liberties and human dignity might worry; however, these predictive qualities also make user data a potential trove of information for law enforcement officials

158. Jure Leskovec et al., *Meme-Tracking and the Dynamics of the News, in* PROCEEDINGS OF THE 15TH ACM SIGKDD INTERNATIONAL CONFERENCE ON KNOWLEDGE DISCOVERY AND DATA MINING 497, 497 (2009), *available at* http://dl.acm.org/citation.cfm?id=1557077&bnc=1.

159. Jure Leskovec et al., *The Role of Social Networks in Online Shopping: Information Passing, Price of Trust, and Consumer Choice, in* PROCEEDINGS OF THE 12TH ACM CONFERENCE ON ELECTRONIC COMMERCE 157, 157 (2011), *available at* http://dl.acm.org/citation.cfm?id=1993598&bnc=1.

160. *Id.* at 166.

161. Jure Leskovec et al., *Friendship and Mobility: User Movement in Location-Based Social Networks, in* PROCEEDINGS OF THE 17TH ACM SIGKDD INTERNATIONAL CONFERENCE ON KNOWLEDGE DISCOVERY AND DATA MINING 1082 (2011), *available at* http://dl.acm.org/citation.cfm?id=2020579&bnc=1.

who seek to predict and prevent crimes. One of the most lamented post-9/11 surveillance programs, Total Information Awareness (TIA), explicitly called for "very large scale databases covering comprehensive information about all potential terrorist threats."[162] TIA's innovation was to use both private enterprise information as well as government databases to create a more holistic picture of surveillance targets, and then use link analysis tools to come up with portraits of suspects.[163] After John Poindexter, the former head of the Information Awareness Office, resigned in 2003, the TIA was defunded and the NSA took over at least two of the TIA's projects.[164] One was the "Information Awareness Prototype System," which was described in the initial TIA call for proposals as "an end-to-end, closed-loop prototype system to aid in countering terrorism through prevention by integrating technology and components from existing DARPA programs."[165] The second program that NSA adopted was called "Genoa," later "Topsail," the goal of which was "to develop decision-support aids for teams of intelligence analysts and policy personnel to assist in anticipating and pre-empting terrorist threats to U.S. interests."[166] In this context, a "database" was "a new kind of extremely large, omni-media, virtually-centralized, and semantically-rich information repository that is not constrained by today's limited commercial database products . . . . Innovative technologies are sought for treating these databases as a virtual, centralized, grand database."[167]

"Data mining" is not the only technology at play here—other tools, including link analysis, pattern matching, and network surveillance, are gaining currency as well.[168] Moreover,

---

162. *EPIC Analysis of Total Information Awareness Contractor Documents,* ELEC. PRIVACY INFO. CTR. (Feb. 2003), http://epic.org/privacy/profiling/tia/doc_analysis.html.

163. Shane Harris, *Two Controversial Counter-Terror Programs Share Parallels,* GOV'T EXEC. (Jun. 16, 2006), http://www.govexec.com/dailyfed/0606/061606njl.htm.

164. Shane Harris, *TIA Lives On,* NAT'L J., Feb. 23, 2006, at 66, *available at* http://shaneharris.com/magazinestories/tia-lives-on/.

165. ELEC. PRIVACY INFO. CTR., *supra* note 162.

166. Harris, *supra* note 164, at 67.

167. ELEC. PRIVACY INFO. CTR., *supra* note 162.

168. *See* Open Letter from the Exec. Comm. on Ass'n for Computing Mach. Special Interest Grp. on Knowledge Discovery and Data Mining, "Data Mining" Is NOT Against Civil Liberties (June 30, 2003), http://www.sigkdd.

information about data mining, which is often disclosed under the Privacy Act, does not include other tools such as link analysis, which are sometimes equally or more important as data mining narrowly defined. Broadly, however, it is clear that the analysis of large data sets is now at the core of the American intelligence enterprise. The NSA reportedly employs a "high-volume, automated voice recognition and pattern matching system" to filter the content of international calls on which it eavesdrops.[169] With the cooperation of service providers, NSA also monitors Internet traffic, including web browsing, using optical splitters within telecom facilities that duplicate the data stream and send a copy to NSA.[170] In addition to its other real-time monitoring capabilities, NSA may also use third-party data mining software to establish the location and online identity of a suspect. NSA has developed some real-time monitoring capabilities with regard to detecting cyberattacks,[171] including the "Perfect Citizen" initiative to detect attacks on critical infrastructure networks such as the electricity grid.[172] Although Perfect Citizen focuses on operators of essential utilities, it leaves open the option of expansion to other parts of the private sector. In addition, utilities may allow NSA to monitor the technology on their networks, or may choose to deploy the technology themselves.

---

org/civil-liberties.pdf ("Data mining is but one of many technologies that may be used in these projects. Other technologies include database management, online analytical processing, speech recognition, image (face, iris, fingerprint, etc.) recognition, natural language understanding and translation, data warehousing, data integration, information retrieval, etc. Does it make sense to attempt to outlaw any or all of these?").

169. Jon Stokes, *The New Technology at the Root of the NSA Wiretap Scandal*, ARS TECHNICA (Dec. 20, 2005, 1:35 PM), http://arstechnica.com/old/content/2005/12/5808.ars.

170. Ellen Nakashima, *A Story of Surveillance*, WASHINGTON POST, Nov. 7, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/11/07/AR2007110700006.html.

171. Bruce Gabrielson, National Institute of Standards and Technology, Presentation at the 6th Annual IT Security Automation Conference and Expo: Progress in Near-Real Time Attack Detection at the Platform Level (Sept. 22, 2010), http://scap.nist.gov/events/2010/itsac/presentations/day2/Network_Automation-Progress_in_Near-Real_Time_Attack_Detection_at_the_Platform_Level.pdf.

172. Siobhan Gorman, *U.S. Plans Cyber Shield for Utilities, Companies*, WALL ST. J., July 8, 2010, *available at* http://online.wsj.com/article/SB10001424052748704545004575352983850463108.html.

Finally, the TFTP case is a classic example of intelligence agencies' reliance upon databases recording communications and transactions, including phone, text messaging, email, and financial transaction records.[173] The real question is how NSA analyzes the data once it has obtained it. In 2004, the General Accounting Office issued a report on the prevalence of data mining in U.S. federal agencies. The report found that 52 agencies were using data mining techniques, many of which relied on data shared between agencies or between the private and public sectors. The NSA did not respond to the survey.[174] Speculation abounds that the NSA is using social network analysis tools to analyze connections between people, transactions, and communications.[175] The NSA potentially uses its own software to do so, but it may be as likely that the agency turns to commercial solutions, which are often cheaper and faster.[176]

B. *Global Regulation of Data Mining*

As is clear, bulk data is a valuable commodity for both private and public actors, and it invites privacy concerns about aggregation as well as about data subjects' consent, anonymity, and usage. And those concerns seem more concretely addressed in the European framework—which confers enforceable rights to access, amend, control, and delete one's data—

173. *See* Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA TODAY, May 11, 2006, *available at* http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm (investigating the extent of phone record databases maintained by NSA); *see also* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-04-548, DATA MINING: FEDERAL EFFORTS COVER A WIDE RANGE OF USES, 2 (2004), *available at* http://www.gao.gov/new.items/d04548.pdf (citing credit reports and credit card transactions as examples of data mining by federal agencies).

174. U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 173, at 7.

175. Alexander Dryer, *How the NSA Does "Social Network Analysis,"* SLATE (May 15, 2006), http://www.slate.com/id/2141801/; Kim Zetter, *NSA Whistleblower: Wiretaps Were Combined with Credit Card Records of U.S. Citizens*, WIRED (Jan. 23, 2009), http://www.wired.com/threatlevel/2009/01/nsa-whistlebl-1/.

176. See, for example, the Department of Homeland Security's decision to turn to commercially available software instead of their in-house ADVISE data-mining software because the commercial product was cheaper. Anne Broache, *Report: DHS Kills Data-Mining Project*, CNET (Sept. 6, 2007), http://news.cnet.com/8301-10784_3-9773243-7.html.

than in the United States framework, whose "notice and consent" and "harm-based" models are far more skeletal and reliant on industry self-regulation. In other words, the collection of this type of data, even before it is put to suspect use, is the subject of real concern in the European legal community.

Moreover, the European data protection framework—by virtue of its extraterritorial reach—has served to "ratchet up" privacy protections in other areas of the world.[177] By forcing companies to pay the heightened costs of protecting privacy in multiple legal regimes, the European norms governing data privacy have diffused, to some extent, to transnational businesses based in the United States. In some sense, this goes hand in hand with the purpose of the Directive—achieving uniformity and consistency among legal regimes in Member States. By virtue of Article 25's adequacy requirements, a degree of consistency among the European states and its external trading partners now seems not only desired but also attainable. Even if this adequacy determination takes place on a case-by-case basis—as was the case with the TFTP agreement—rather than as a general matter, it is clear that the European data privacy rules have the capacity to force less-protective nations to, in some sense, comply. Exporting privacy is a key purpose of the European data privacy regime.

In light of these concerns, balanced against the existing (and growing) analysis capabilities, the TFTP agreement's allowance of bulk data transfers juxtaposed with its prohibition on "computer filtering" is curious.[178] One interpretation is that Article 5 has been craftily worded so as to allow the desired analysis capabilities while seeming to prohibit all automated data analysis.[179] If this is the case, it might speak to the fact that while data mining has a bad reputation in civil liberties circles, the use of computerized techniques to filter massive amounts of data is now a fact of life.[180] In 2006, the Ger-

177. *See generally* Shaffer, *supra* note 34.

178. Agreement, *supra* note 3, arts. 2, 6.

179. This may be the case because searching a data set of millions of transactions is literally impossible without some form of "computer filtering." Because the term is undefined, however, it is unclear which forms of "computer filtering" are prohibited.

180. *See* Exec. Comm. on Ass'n for Computing Mach. Special Interest Grp. on Knowledge Discovery and Data Mining, *supra* note 168 ("[T]he current debate that portrays these Government projects as 'developing massive data

man Constitutional Court held that data mining was only permissible in the event of a "concrete danger."[181] Admitting that computerized searching is taking place in the context of intelligence-gathering, rather than a specific investigation, is tantamount to conceding that a "concrete danger" exists with regard to terrorism—although this threat is by definition general, not individuated. It is thus possible that although Article 5 seems to prohibit all automated analysis, computer-aided searching goes on uninhibited under a different name. The JSB's contention that the Treasury's requests continue to be incredibly vague seems to indicate that this is the case—certainly, Treasury does not have the manpower to filter through literally millions of results without computerized assistance.

Another possibility is that the Agreement in Article 5, in the context of the European data privacy regime more generally, is actually attempting to set some kind of standard on use of cross-border bulk data transfers.[182] Indeed, one argument in favor of the development of a European Terrorist Finance Tracking System is that it would avoid the evil of having to transfer the data to a third country.[183] However, since the main benefit of having bulk data—rather than data collected based on individualized suspicion—is that the sheer quantity of information makes it ripe for computer-aided analysis, it is unlikely that a European version of the TFTP would not use data mining or analysis techniques.[184]

Hesitancy about the usage of bulk data is rooted in substantive concerns about necessity, proportionality, and aggre-

---

mining systems' is misleading and injurious to the large scientific community working on the research and development of data mining technology.").

181. Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] Apr. 4, 2006, 1 BVerfGE ¶ 158 (Ger.) ("Diese Voraussetzungen sind bei der Rasterfahndung gewahrt, wenn der Gesetzgeber den Grundrechtseingriff an das Vorliegen einer konkreten Gefahr für die bedrohten Rechtsgüter knüpft.").

182. *See generally* Shaffer, *supra* note 34 (arguing that the European regime on privacy standards is leading to the creation of national standards).

183. *See, e.g.*, EUROPEAN COMMISSION, EUROPEAN TERRORIST FINANCING TRACKING PROGRAMME ROADMAP 2 (2010), *available at* http://ec.europa.eu/governance/impact/planned_ia/docs/2011_home_003_terrorist_financing_tracking_en.pdf (stating the goal of being able to filter the banking data within Europe so as to provide more "targeted data" to the Treasury).

184. *Id.*

gation.[185] Because of the sharply divergent statutory frameworks and privacy norms in the EU and United States, it would be difficult to obtain consensus on how to use large quantities of data in privacy-protective ways. The online behavioral advertising approach is illustrative; where objectors to behavioral advertising in the United States use ad-hoc methods to block ads, the European E-Privacy Directive is meant to provide a blanket limitation on use of consumer data for advertising purposes.[186] This example does not entail data transfer for additional purposes, which would further complicate the picture. Yet the policies are so different as to make it difficult to see what kind of normative agreement would facilitate responsible data transactions.

Perhaps what European-style regulation can best achieve is to implement a framework for data subjects to access, correct, and have control over their data, regardless of their nation of citizenship and the nation that is requesting or obtaining the data. But even in this relatively limited scenario, which the TFTP embodies, the difficulties of achieving global agreement on this issue have been legion, showcased (as discussed above) by the lack of redress and review mechanisms. Yet as the information society continues to grow and shift, already copious quantities of data will also continue to grow, and procedures for dealing with them are paramount.

---

185. *See, e.g.*, *General Data Protection Regulation*, *supra* note 27, at Article 5 (ensuring necessity and proportionality by requiring that data be "adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed"); *see also United States v. Jones*, No. 10–1259 (U.S. Jan. 23, 2012) (Sotomayor, J., concurring) ("[T]he Government's unrestrained power to assemble data that real private aspects of identity is susceptible to abuse . . . . GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may 'alter the relationship between citizen and society . . .'") (citing *United States v. Cuevas-Perez*, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)).

186. *See, e.g.*, *France Introduces Prior Opt-in Consent for Cookies*, PRIVACY AND INFORMATION SECURITY LAW BLOG (Aug. 26, 2011), http://www.huntonprivacyblog.com/2011/08/articles/france-introduces-prior-opt-in-consent-for-cookies/#more-1869 (reviewing French implementation of E-Privacy Directive by imposing opt-in consent requirements for cookies, which are necessary for targeted or behavioral advertising).

One solution may be to conceptualize data as a good that can be traded in and to erect an international framework around it (paralleling, in some way, the TRIPs Agreement, for example). This solution, at the very least, would acknowledge the crucial role that data transfer has played and will continue to play in building the international economy. On the other hand, it would also probably subjugate privacy concerns to economic ones. Moreover, since the issue here is not trade of data among corporations, but rather a one-way transfer from a corporation to government, conceptualizing data transfers as a form of international trade is probably not the correct framework.[187]

A more effective solution may be to empower more actors in this area to contract for adequate data protection and transfer. Contracts, as the European system anticipates, play a crucial role in incorporating data protections while facilitating usage.[188] The costs of complying with European regulations on one side of the Atlantic and American regulations on the other have also fostered a market for self-regulation and privacy labeling programs that can, along with contract terms, help guarantee that private enterprises take privacy more seriously.[189] Contracts can also govern relationships among a variety of types of actors, including public, private, and hybrid. Empowering European companies to contract with the American government, while maintaining the threat of enforcement of European law, might raise the standard of data protection overall by forcing key stakeholders in the United States to

187. *See* Data Protection Directive, *supra* note 4, pmbl. (noting that the "free movement of goods . . . require[s] . . . that personal data should be able to flow freely," and hence distinguishing between the movement of "goods" and "data"); *see* Shaffer, *supra* note 34, at 50 (discussing the potential role of the WTO in adjudicating data transfer disputes, and concluding that the EU has a legitimate public policy rationale to restrict data transfers to protect its citizens).

188. Model Contracts for the Transfer of Personal Data to Third Countries, EUROPEAN COMM'N, http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm (last visited Feb. 21, 2013).

189. *See, e.g.*, TrustE, http://www.truste.com/ (last visited Feb. 21, 2013) (providing online privacy solutions to businesses); *BBB Accredited Business Seal for the Web*, BETTER BUSINESS BUREAU, http://www.bbb.org/us/bbb-online-business/ (last visited Feb. 21, 2013) (offering certifications of compliance with privacy policies).

comply with European law. However, the balance of power will always be uneven when government requests information from private industry, especially in light of the counterterrorism rationale. In addition, the exchange of large sets of aggregate data would probably continue to anger European citizens and lawmakers.

CONCLUSION

This Note aims to showcase the limited capabilities of the Terrorist Finance Tracking Program as a means to regulate global data transfers. Although the normative divergences between European and U.S. privacy law are far fewer than the dominant literature suggests, the procedural differences are extensive. This makes it very difficult to come up with a regulatory regime whose procedural protections actually have teeth, despite the fact that the European data protection framework has generally achieved a "ratcheting up" of data protection standards.[190] The result is that while the European predilection for procedural protections won out in this case, the implementation has been highly flawed. Moreover, whether bulk data transfers, and the privacy implications for aggregated consumer data analyzed through emerging technology, are *sui generis* remains unsolved. Yet despite its flaws, the TFTP is one of the only attempts to develop an international regulatory framework for dealing with transfers of data—a commodity that is essential not just to commerce but also to government functions. Its gaps suggest both the difficulties of coming up with a more comprehensive framework, and the imminent need to do so.

190. *See* Shaffer, *supra* note 34, at 55–56 (describing the attention that European privacy protections have drawn to the practices of American businesses).