2004

Transgovernmental Networks vs. Democracy: The Case of the European Information Privacy Network

Francesca Bignami
George Washington University Law School, fbignami@law.gwu.edu

TRANSGOVERNMENTAL NETWORKS VS. DEMOCRACY: THE CASE OF THE EUROPEAN INFORMATION PRIVACY NETWORK

Francesca Bignami[*]

INTRODUCTION

In 2004, Northwest Airlines came under fire for breaking European information privacy laws.[1] The Dutch government agency responsible for privacy opened an investigation against Northwest. What was the

* Associate Professor, Duke University School of Law. Special thanks to Xavier Lewis for his research assistance. I would also like to thank George C. Christie, Donald L. Horowitz, Robert O. Keohane, Christopher H. Schroeder, and Giulio Vesperini for their comments. Jacob Visscher and Lino Liao of the Council of the European Union provided valuable assistance with my access to documents requests. I am grateful for research support from the German Marshall Fund Research Fellowship Program.

1. *See* Letter from Ulco van de Pol, Vice-President, College Bescherming Persoonsgegevens (Dutch data protection authority), to Northwest Airlines (Apr. 6, 2004), *at* http://www.cbpweb.nl/downloads_uit/z2004- 0310.pdf?refer=true&theme=purple.

charge? The airline company had turned over passenger data to NASA in breach of European privacy rights, to assist NASA with developing an anti-terrorism database. The Dutch agency closed the investigation without taking administrative action or turning the matter over to criminal prosecutors because Northwest had since changed its information privacy policy. But the Dutch agency expressed "serious doubts" as to whether Northwest had complied with European law.[2]

European and American citizens are caught between two very different, often clashing, legal cultures of privacy. In the European Union, privacy is essential to protecting citizens from oppression by the government and market actors and preserving their dignity in the face of opposing social and political forces. In the United States, privacy is secondary. In part, the explanation for the low value Americans attach to the legal concept of privacy is functional: protection against overweening state and market power is guaranteed by other means, including the radical fragmentation of state power in the American federalist and presidential system of government, and antitrust laws.[3] But the difference is also one of basic values. Outside the core physical space of the home, Americans do not care particularly about privacy.[4]

As a consequence, firms like Northwest that operate in an integrated transatlantic market must routinely come to terms with vastly different constitutions, laws, and regulatory systems. This Article takes a close look at the European side of the Atlantic, that is, the European regulation of corporations and other entities when they transfer the personal information of their clients and employees outside the European Union. Under the EU Data Protection Directive (Directive), firms that collect personal information from European citizens must guarantee their privacy even once such personal information is sent outside the European

2. *Id.*

3. The French case illustrates some of these functional considerations. The French legislation on information privacy was enacted in 1978 in response to what is known as the "Safari" episode. *See* Guy Braibant, Données personnelles et société de l'information : Transposition en droit français de la directive no. 95/46, 31 (1998) (on file with author). The daily newspaper "Le Monde" revealed the French government's "Safari" plan to introduce a single personal identification number for all entries in government databases, thus permitting the "connection" of all such information on individual French citizens. In response, a government commission was established to examine the problem and a comprehensive information privacy law was passed. *Id.* Before the internet age, such an information scheme would not have been possible in the United States because, in the American constitutional system, government is not an economic actor in areas such as healthcare, and many government functions are carried out by state, not federal, government. *See also* DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES 169–70 (1989).

4. *See* JEFFREY ROSEN, THE NAKED CROWD: RECLAIMING SECURITY AND FREEDOM IN AN ANXIOUS AGE (2004).

Union.[5] National privacy authorities are responsible for enforcing these duties against firms operating in their territories, subject to an elaborate system of Europe-wide checks involving other national regulators and the European Commission (Commission).[6] When foreign regulatory systems fail to afford the same privacy safeguards as exist in the European Union, the Commission has the power to negotiate with such countries to obtain improvements in their laws and regulations and hence allow the free, international flow of personal information.[7] For firms that do business globally, it is critical to understand the administration of European privacy law.[8]

This examination of the European regulation of international data transfers is important for another reason. The European institutional framework for international data transfers is an example of what Anne-Marie Slaughter calls "transgovernmental networks."[9] Such networks of national government officials are one of the principal forms of European governance. Ever since the European Community was founded in the 1957, Member States have been reluctant to transfer government powers to central European institutions, preferring to leave implementation and enforcement of European norms to their national administrations. Yet governments have always understood that rough equivalence in implementing rules and enforcement decisions is necessary for cooperation to succeed. Networks of national civil servants that develop common administrative standards are the solution to this dilemma of national government power and European integration. According to Slaughter, the international realm is coming to resemble Europe. More and more, international cooperation in areas such as the environment and financial markets is occurring through networks of government regulators who

5. Council and Eur. Parl. Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31 [hereinafter Data Protection Directive or Directive].

6. *See infra* text accompanying notes 67–78. The European Commission (Commission) is the EU's executive branch. It is staffed by civil servants and headed by a President and College of Commissioners appointed by the Member States with the consent of the European Parliament. PAUL CRAIG & GRÁINNE DE BÚRCA, EU LAW 54–59 (3d ed. 2003).

7. Directive, *supra* note 5, at art. 25.

8. There are four important types of legal acts in the EU: treaties, European laws (which include what are known as Directives and Regulations), European implementing regulations (which include what are known as implementing Directives and implementing Regulations), and European decisions. *See* Treaty Establishing a Constitution for Europe, arts. I-33, I-34, I-37, 1994 O.J. (C 310) 1 [hereinafter Constitutional Treaty] (not yet ratified). The most important treaties are: the Treaty Establishing the European Economic Community, Mar. 25, 1957, 298 U.N.T.S. 11, (the European Economic Community was renamed the "European Community" in 1992); the Treaty on European Union, Feb. 7, 1992, 1992 O.J. (C 191) 1, 31 I.L.M. 253 [hereinafter the Maastricht Treaty]; and the Constitutional Treaty, *supra*, which would replace the other two but has not yet been ratified.

9. ANNE-MARIE SLAUGHTER, A NEW WORLD ORDER 40, 43 (2004).

exchange information, develop common regulatory standards, and assist one another in enforcing such standards.[10] By studying the case of the European privacy network, therefore, we gain perspective on a phenomenon of growing importance not only in the European Union but throughout the world.

The perspective offered by this Article is twofold. The emergence of transgovernmental networks gives rise to two questions, one causal and the other normative. First, how do we explain transnational cooperation through networks? Why do governments and regulators choose to establish networks rather than retain virtually limitless discretion over policymaking, conditioned only by international legal obligations? Based on my examination of the records of the intergovernmental negotiations on the Data Protection Directive, I conclude that one precondition for fettering national discretion through networks is common preferences among governments on the substance of the policy to be administered. Compared to other areas of European law, the Data Protection Directive gives surprisingly few powers to the European network of privacy regulators; the bargaining history shows that this decision was driven by extreme disagreement on the importance of privacy. While networks can generate harmonization of national policies, consensus among the participating regulators on the "problem" to be addressed by such policies is necessary for networks to spring to life. To explain that consensus we must look elsewhere, to the market, technology, the international aid that the North can promise the South, epistemic communities, and other causes of convergence.

Second, how do transgovernmental networks fare when put to the normative test of respecting individual rights and guaranteeing the democratic accountability of bureaucrats to elected officials and the public? Modern understandings of legitimate public administration are inescapably tied to national experiences with democracy, yet that normative conceptual framework is confronted today with a novel form of radically disaggregated administration. Is the empirical reality of transgovernmental networks compatible with basic principles of liberal democracy? Based on Italy's experience with the European privacy network, I argue that networks as codified in European law do not undermine significantly individual rights. Roughly speaking, Italian and European law guarantee participation, judicial review, the rule of law, and transparency. The administrative practice of the European privacy network, however, alters substantially the rights calculus. The regulation of international data transfers is characterized by informality and failure to act, forms of government action against which individuals generally

10. *Id.* at 44–45.

cannot vindicate their rights in court. At least in the privacy case, therefore, rights suffer.

More troubling is the fate of democratic accountability. The sharing of powers among national and supranational regulators in networks makes it difficult for national publics and parliaments to hold such regulators accountable. Popular mobilization within one nation can control transgovernmental networks only if that nation is powerful enough to reject routinely the decisions that result from the network. In the European Union, no Member State has such power and, in the international realm, only the United States and certain European nations can claim that prerogative. Citizens, therefore, must be capable of mobilizing across national borders in the many different political communities in which transnational regulators operate. Yet, as documented in the scholarship on the democratic deficit in the European Union, overcoming national identities and setting the stage for vibrant democratic politics in transnational polities is no simple matter. If, as in the European privacy case, transgovernmental networks generate substantial inaction or informal action, the democratic deficit is particularly serious. In national systems, political accountability generally compensates for the inability of courts to police inaction and informal action; in the absence of transnational democratic mobilization, such accountability is weak in the European arena.

The European Parliament's vigorous efforts to stop the recent EU–U.S. agreement on European airline passenger data suggests that the democratic future of European networks is not so bleak. When scholars speak of a democratic deficit in the European Union, they use the term to refer to two different phenomena. The first is the absence of the formal institutions of liberal democracy in European governance, a failure that can be traced to the system's origins as an international organization. The second is the lack of a European identity that transcends national identities and that leads citizens to band together with citizens elsewhere in Europe to promote common causes, participate in European politics, and develop allegiances to their European governors. The airline passenger data episode suggests that both sources of the democratic deficit might be overcome in the not too distant future.

Since 1992, in response to the first democracy critique, the European Parliament has acquired significant powers. Among those powers is the right to deliberate and vote on non-binding resolutions regarding the administrative decisions of European networks.[11] Furthermore,

11. FRANCESCA E. BIGNAMI, THE ADMINISTRATIVE STATE IN A SEPARATION OF POWERS CONSTITUTION: LESSONS FOR EUROPEAN COMMUNITY RULEMAKING FROM THE UNITED STATES

fundamental rights are becoming an increasingly important element of the European legal order, as evidenced by the Charter of Fundamental Rights of 2000 and the Constitutional Treaty of 2004. Recently, the European Parliament asserted its new prerogative over administrative decisions and it did so to protect the European fundamental right to privacy: Parliament voted against a EU–U.S. agreement allowing transfers of passenger data to the United States for counter-terrorism purposes. Thus the concern that European decisions are made by technocrats, without the involvement of a directly elected legislative assembly, appears somewhat attenuated. Likewise, the mobilization of parliamentarians around a common, highly symbolic, European right to privacy suggests that gradually, through similar episodes, European Members of Parliament and their constituents might develop a shared identity. Yet even though this chapter in transatlantic relations is cause for optimism about European networks, it is also a reminder of the unfortunate tension between democracy and international cooperation. Europe's new constitutional order might alleviate concerns of a democratic deficit in European transgovernmental networks, but it also might get in the way of international cooperation through other transgovernmental networks.

The Article proceeds as follows. Part One gives general background on European information privacy law and the different procedures and institutions that have been devised, in the fifty years since the European Community was first established, to implement and enforce European law. The focus then shifts to European networks, the similarities with transgovernmental networks, the specifics of the European information privacy network and their implementation into Italian law. Because the Data Protection Directive, like most European law, rests on implementation into national law and allows for significant discretion in how the Directive's terms are implemented, it is virtually impossible to understand European regulation of information privacy without considering national law. For reasons that I explain later, I have chosen the Italian case to bring this important national perspective to the analysis.

Part Two reviews the experience to date with the regulation by network of international data transfers. The next Part takes up the question of why governments establish networks and argues that the European privacy network was delegated very few powers because of radical disagreement among the Member States over the right to privacy. In Part Four, the European privacy network is evaluated from the perspective of individual rights and democratic accountability. In light of the diversity

(Jean Monnet Working Paper No. 5/99, 1999), *at* www.jeanmonnetprogram.org/papers/99/990502.html.

of liberal democratic traditions and the law of administration in those of traditions, Italian administrative law again serves as the point of reference. This assessment is divided into two sections: the European law of the privacy network, as it appears in the Data Protection Directive; and the administrative practice of the privacy network, which departs significantly from the formal law. Finally, the Article reviews the recent transatlantic dispute over information privacy and the European Parliament's important role in that dispute.

I. THE REGULATION OF INFORMATION PRIVACY

A. *European Information Privacy Policy*

What are the concerns and objectives that motivate the European regulators who interact in the privacy network? Laws regulating the collection and use of personal information date back to the early 1970s, when computer technology was first widely used by government agencies and large private organizations such as banks to gather, elaborate, and utilize personal data.[12] These early national laws, European and American, were followed by two international instruments: the OECD Guidelines of 1980[13] and the Council of Europe Convention of 1981.[14] In 1990, negotiations on a European law began, and in 1995, many years and diplomatic fights later, the Data Protection Directive was adopted.[15]

Even though the social and technological setting of information privacy laws has changed radically since the 1970s, many of the same concerns drive both the earlier and later generations of legislation. The most basic one, and an area in which little difference separates countries, is the danger of inaccurate personal information and the serious adverse

12. These early laws include the Hessian Data Protection Act of 1970, the Swedish Data Act of 1973, the U.S Privacy Act of 1974, the German Federal Data Protection Act of 1977, and French Law No. 78-17 of 6 January 1978 on computers, data files, and liberties. *See* COLIN J. BENNETT & CHARLES D. RAAB, THE GOVERNANCE OF PRIVACY: POLICY INSTRUMENTS IN GLOBAL PERSPECTIVE 102 (2003); ELECTRONIC PRIVACY INFO. CTR., PRIVACY & HUMAN RIGHTS: AN INTERNATIONAL SURVEY OF PRIVACY LAWS AND DEVELOPMENTS 238–44, 245–56, 474–79 (2003). For excellent comparative discussions of the early history of information privacy, see COLIN J. BENNETT, REGULATING PRIVACY (1992) and FLAHERTY, *supra* note 3.

13. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, OECD Doc. C 58 (Oct. 1, 1980).

14. Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, Eur. T.S. No. 108.

15. Spiros Simitis, *From the Market to the Polis: The EU Directive on the Protection of Personal Data*, 80 IOWA L. REV. 445, 446 (1995)[hereinafter Simitis, *From the Market to the Polis*].

consequences that may follow.[16] Wrong information in a database can lead to arrest, the denial of a loan application, and other injustices. Such errors can occur in a number of ways. The information may be recorded incorrectly in the electronic system to begin with. Personal information can become obsolete—an individual may have paid back her debts or been cleared of a criminal charge—and yet, once large organizations enter information into a database, they have few incentives to review and update such information.

When personal information is used for purposes other than those for which it was collected originally or is combined with other data, collected by another institution for another reason, the risk of inaccuracy increases exponentially. What is known as "data mining" magnifies the danger of inaccuracy because data is coded differently depending on the database and the purposes for which it is collected. In consolidating personal information, immense care must be taken to ensure that like is combined with like. A notorious example of this form of information abuse occurred in Sweden: a town attempted to root out welfare fraud in public housing grants by matching recipients' names with their income figures as reported in other databases.[17] About one thousand individuals came under suspicion of breaking the law. Yet, as it turned out, only one of them was actually guilty. The discrepancy in income figures had nothing to do with welfare fraud but rather was the product of the different formulae used to calculate incomes in each of the databases.

A second hazard that information privacy laws address, in both Europe and the United States, is the risk that personal information will fall into hands other than those for whom it was intended. This is the danger that an individual's personal information—national identification number, credit card number, or bank account number—will be used by someone other than that individual to claim her government benefits, charge her credit card, or empty her bank account. Fraud is not the only risk of unsecured data. Stalkers and killers as well as thieves may obtain the information. For instance, the U.S. Driver's Privacy Protection Act of 1994[18] was enacted in response to the murder of actress Rebecca Shaffer by an obsessed fan who had obtained her address from the California Department of Motor Vehicles.[19]

16. *See generally* LEE A. BYGRAVE, DATA PROTECTION LAW: APPROACHING ITS RATIONALE, LOGIC, AND LIMITS 145–50 (2002).

17. *See id.*, at 106; Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. PA. L. REV. 707, 718 (1987).

18. Driver's Privacy Protection Act of 1994, 18 U.S.C. §§ 2721–2725 (2005).

19. *See* Edward J. Eberle, *The Right to Information Self-Determination*, 2001 UTAH L. REV. 965, 977 n.72 (2001).

The spectre of Big Brother is the last concern common to information privacy regulation on both sides of the Atlantic. At the origins of the first information privacy laws was the fear that governments would use personal information to oppress their citizens and establish authoritarian regimes. The belief was that the many government agencies that collect information—welfare agencies, health authorities, the police—might combine their databases to monitor and control each and every citizen with whom they came into contact. As Alan Westin said in *Privacy and Freedom*, the book that served as one of the catalysts for information privacy laws in both the United States and Europe:

> In the area I have called data surveillance, the rapid pace of computer development and usage throughout American society means that vast amounts of information about individuals and private groups in the nation are being placed in computer-usable form. More and more information is being gathered and used by corporations, associations, universities, public schools, and governmental agencies. And as "life-long dossiers" and interchange of information grow steadily, the possibilities increase that agencies employing computers can accomplish heretofore impossible surveillance of individuals, businesses, and groups by putting together all the now-scattered pieces of data.[20]

The current attempts of the U.S. government to identify terrorists by creating computer systems that would combine the information gathered by private businesses, local government, and federal agencies serve as a reminder that Westin's warning, almost forty years later, must still be taken seriously.[21]

A purely functional and universalist analysis of information privacy cannot reveal fully the motivations and objectives of European privacy policy. European and American concepts of privacy differ in important respects, a fact that has far-reaching consequences for their information privacy regulation. To explore these differences I will focus for the time being on German law. As I develop in greater detail later on, not only do Europeans and Americans differ on privacy but so too do European democracies. It is appropriate to single out Germany because it has one of the longest experiences with information privacy regulation and served as an important source of inspiration for the Data Protection Directive.

---

20. ALAN F. WESTIN, PRIVACY AND FREEDOM 366 (1967).

21. *See* TECHNOLOGY AND PRIVACY ADVISORY COMMITTEE, U.S. DEP'T OF DEFENSE, SAFEGUARDING PRIVACY IN THE FIGHT AGAINST TERRORISM viii (2004) (describing different government data mining programs).

Information privacy is rooted in the Basic Law (*Grundgesetz*).[22] In 1983, the Constitutional Court recognized the right to "informational self-determination" (*informationelles Selbstbestimmungsrecht*) based upon the rights to human dignity and the free development of personality set down in Articles One and Two of the Basic Law. Informational self-determination can be translated as the right of control over one's personal information. In Germany, therefore, information privacy is linked to a rich constitutional doctrine on a protected private sphere within which the individual can develop and flourish.[23] The general law of human dignity and free development of personality seeks to protect individual autonomy from a variety of abusive state and private practices, ranging from discrimination based on race and sex, to attempts to influence consumer preferences. To that end, German information privacy law gives individuals the tools to control their personal information in a wide array of circumstances.[24]

The legal concept of privacy that informs American information privacy law is narrower. The constitutional and common law of privacy focuses mainly on the physical places and personal facts which, if invaded or disclosed, would offend common expectations of privacy.[25] While information privacy statutes are more comprehensive in their treatment of the problem, legislators are inevitably influenced by the background principles of the Constitution and the common law.

Additionally, as with many other German constitutional rights, the Constitutional Court has held that the rights to dignity and personality upon which information privacy is based constitute both positive and negative rights.[26] That is, the state is under a duty to protect and further the individual exercise of information privacy rights. The right to privacy is not simply a shield against intrusive state action, but a claim on the

22. *See* Paul Schwartz, *The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination*, 37 AM. J. COMP. L. 675, 676, 686–90, 701 (1989) (discussing German Constitutional Court case that established the right to informational self-determination).

23. *See* Axel Halfmeier, *Country Report for Germany, Case No. 5*, *in* THE COMMON CORE OF EUROPEAN PRIVATE LAW, PERSONALITY RIGHTS IN EUROPEAN TORT LAW, 5 (Gert Bruggemeier & Aurelia Colombi Ciacchi eds., forthcoming) (on file with author); *see also* EDWARD J. EBERLE, DIGNITY AND LIBERTY: CONSTITUTIONAL VISIONS IN GERMANY AND THE UNITED STATES 256–66 (2002) (comparing German and American law of personality rights).

24. *See* Eberle, *supra* note 19, at 92 (discussing ramifications of the German constitutional law on the statute); FLAHERTY, *supra* note 3, at 30–39 (discussing the different goals underpinning the German law).

25. *See* WESTIN, *supra* note 20, at 350; David A. Anderson, *The Failure of American Privacy Law in* PROTECTING PRIVACY 139, 139–67 (Basil S. Markesinis ed., 1999).

26. *See* DONALD P. KOMMERS, THE CONSTITUTIONAL JURISPRUDENCE OF THE FEDERAL REPUBLIC OF GERMANY 312 (2d ed. 1997) (discussing obligation of the state to establish conditions for the realization of the right to dignity).

state for affirmative, legislative action.[27] The American tradition is different in that rights are generally conceived as affording protection against government action. The Supreme Court does not interpret the Constitution to impose affirmative duties on government to pass legislation safeguarding individual rights like privacy.[28]

Finally, in German law, all threats to dignity, personality, and informational self-determination are treated on roughly equal terms regardless of whether the offender is a public or private actor. No categorical distinction is drawn between the control and manipulation of persons which may occur in the public sector and that which may occur in the market and society. Dignity and personality rights can be invoked not only against state action but also against private information collection and surveillance.[29] Likewise, the Federal Data Protection Law applies across-the-board to both the private and public sectors.[30] That is not to say that the dangers posed by public and private uses of personal information are believed to be identical. German law recognizes that public entities are better positioned than private entities to collect, use, and misuse personal information; the law imposes more onerous duties on the public sector.[31]

Unlike German law, U.S. law strictly separates invasions of privacy committed by the state from those perpetrated by corporations and other private sector entities. As with all rights, the Constitution only protects the right to privacy against state action. The common law of tort does not contain a strong right to privacy.[32] The statutory protections enacted by Congress display a similar bias. While Congress passed the Privacy Act in 1974 to discipline the collection and use of information in all federal agencies, it has adopted private sector legislation sporadically and on a piecemeal basis, in reaction to particular privacy abuses in sectors of the

27. *See* Schwartz, *supra* note 22, at 686.

28. Information privacy is protected under the Fourth Amendment provisions on unlawful searches and seizures and under the substantive due process guarantees of the Fifth and Fourteenth Amendments. *See* DANIEL J. SOLOVE & MARC ROTENBERG, INFORMATION PRIVACY LAW 182–202, 275–322 (2003).

29. *See, e.g.*, Amtsgericht Berlin-Mitte [Berlin Center District Court], Geschäftsnummer [Docket No.] 16 C 427/02 (Dec. 18, 2003) (F.R.G.) (judgment on file with author) (holding for plaintiff in suit by pedestrian against Berlin department store for removal of surveillance cameras based on Basic Law, Arts. 1 & 2, and Federal Data Protection Act 2001).

30. *See* ELECTRONIC PRIVACY INFO. CTR., *supra* note 12, at 246–48.

31. *See* Federal Ministry of the Interior, Federal Data Protection Act: An Implementation of Directive 95/46/EG (Feb. 18, 2002) (power point presentation on file with author). The new German legislation enacted in 2001 to implement the Data Protection Directive has equalized somewhat the treatment of the public and private sectors.

32. *See* Anderson, *supra* note 25.

economy such as healthcare, the financial industry, and telecommunications.[33]

The Data Protection Directive was heavily influenced by the German understanding of information privacy.[34] European laws, unlike domestic ones, are generally drafted to accommodate multiple, long-standing national policies in the area to be governed by the legislation. European laws often bring to mind a patchwork of different provisions and terms of art drawn from national laws and sewn together in Brussels rather than a coherent policy reflecting the will of a legislative majority. The Data Protection Directive is a clear example of this form of legislative drafting.[35] At the time that the first proposal was published, seven of the then twelve Member States had information privacy laws: Denmark, Germany, France, Ireland, Luxembourg, the Netherlands, and the United Kingdom.[36] The German and French models were highly influential because of their acknowledged role as trendsetters in the privacy field and because of the German and French origins of the officials charged with drafting the proposals.[37]

The Directive promotes each of the objectives discussed earlier—accuracy, defense against fraud, protection from government oppression, and informational self-determination—by imposing a number of general

33. *See* Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (codified in scattered sections of 12 and 15 U.S.C.) (imposing requirements on financial institutions when collecting personal data); Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 26 and 42 U.S.C.) (mandating protections for health privacy); Cable Communications Policy Act of 1984, 47 U.S.C. §§ 521–561, § 551 (protecting personal records kept by cable television companies). *See generally* SOLOVE & ROTENBERG, *supra* note 28, at 563–66 (describing and assessing piecemeal regulation of information privacy).

34. The purpose of this discussion is to give some background on European information privacy law, beyond the sometimes arid and abstract text of the Data Protection Directive. The claim, however, is not that German law was the only national experience to influence the Directive. The impact of most of the Member States that negotiated the Directive can be traced in one way or another. Further, as will be discussed in greater detail below, the Directive is not what in EU law is called a "complete harmonization directive." That is, it sets minimum, not maximum, standards for information privacy. *See* Spiros Simitis, *Data Protection in the European Union—The Quest for Common Rules*, *in* 8 COLLECTED COURSES OF THE ACADEMY OF EUROPEAN LAW 95, 111–115 (European Univ. Inst., Florence, Academy of European Law ed., 1997) [hereinafter Simitis, *Data Protection in the European Union*]; Simitis, *From the Market to the Polis*, *supra* note 15, at 445, 463–64. Therefore, Member States could retain most elements of their pre-existing information privacy systems at the implementation phase even though some of those national systems were not expressly incorporated in the Directive.

35. *See* Simitis, *From the Market to the Polis*, *supra* note 15, at 449–50.

36. Commission Communication on the Protection of Individuals in Relation to the Processing of Personal Data in the Community and Information Security, [hereinafter Communication on the Protection of Individuals].

37. *See* Interview with Spiros Simitis, Professor of Labour, Civil, and Computer Science and Law, Johann Wolfgang Goethe University, in Frankfurt-Main, Germany (July 1, 2003) (notes on file with author).

requirements on those who collect, use, and transfer personal information. Personal data must be processed fairly and lawfully; personal information can be collected only for specific and legitimate purposes; the amount of information collected may not be excessive in relation to those purposes; personal data must be accurate; and information can be kept no longer than necessary to fulfill the original purpose of collection.[38] The Directive then extensively elaborates on these basic principles. It specifies the information that must be provided to individuals when their data is collected,[39] the types of personal information that may and may not be collected,[40] the circumstances under which such information may be used,[41] and the rights of individuals in checking on their information.[42] These rights and duties apply to the private and public sectors alike, although extensive exceptions are carved out for government use of personal information in areas such as national security, domestic policing, foreign affairs, and defense.[43]

B. *Application and Enforcement of Information Privacy Law*

1. Modes of Implementing and Enforcing European Law

Equipped with a basic understanding of the rationale and contents of European information privacy law, we can now turn to enforcement of privacy rights. European policymakers have devised a dizzying array of institutional arrangements for implementing the common policies set out in laws like the Data Protection Directive. Scholars traditionally identify two modes of European administration: administration of select policy areas such as competition law by the Commission (direct administration) and administration of the rest by Member States with little or no interference from above (indirect administration).[44] The powers exercised by the Commission are unknown in other international regimes, given the reluctance in virtually every other part of the world to cede the sovereignty necessary to institute such a supranational body.[45] The powers

38. Directive, *supra* note 5, at art. 6.
39. *Id.* at arts. 11–12.
40. *Id.* at art. 8.
41. *Id.* at arts. 6–7.
42. *Id.* at arts. 12–14.
43. *Id.* at art. 13.
44. *See* Jürgen Schwarze, *The Convergence of the Administrative Laws of the EU Member States, in* THE EUROPEANISATION OF LAW: THE LEGAL EFFECTS OF EUROPEAN INTEGRATION 163, 165 & n.9 (Francis Snyder ed., 2000).
45. *See* Daniel Philpott, *Westphalia, Authority, and International Society*, 47 POL. STUD. 566, 585 (1999); William Wallace, *The Sharing of Sovereignty: The European Paradox*, 47 POL. STUD. 503 (1999). The Secretariat of the World Trade Organization, for instance, only provides technical and logistical support to member countries and the Dispute Settlement

exercised by the Member States, however, are typical of most international organizations—the World Trade Organization, the Council of Europe, and the Climate Change Convention, just to name a few.[46]

Over the past couple of years, attention has shifted to a new set of institutions, procedures, and legal requirements designed to curb national discretion in the second form of European administration (indirect administration).[47] European legislation often imposes requirements on national authorities, such as independence from the executive branch and the duty to consult interest groups.[48] Member States are subject to extensive reporting duties[49]so that the Commission can monitor their track records on rulemaking and enforcement and, in extreme cases of noncompliance, step in with proposals for new European legislation or with enforcement actions.[50] A series of European agencies have been estab-

Body, the WTO's judicial body. *See* Marrakesh Agreement Establishing the World Trade Organization, art. 6, Apr. 15, 1994, LEGAL INSTRUMENTS—RESULTS OF THE URUGUAY ROUND vol. I, 33 I.L.M. 1125 (1994); INFO. AND MEDIA RELATIONS DIV., WORLD TRADE ORG., UNDERSTANDING THE WTO 107 (3d ed. 2003), *available at* http://www.wto.org/english/thewto_e/whatis_e/tif_e/utw_chap7_e.pdf; *Cf.* ABRAM CHAYES & ANTONIA HANDLER CHAYES, THE NEW SOVEREIGNTY: COMPLIANCE WITH INTERNATIONAL REGULATORY AGREEMENTS 2–28 (1995) (discussing limitations of classic international regimes in ensuring compliance).

46. In all international regimes, States are under a duty to implement the obligations undertaken in the governing treaties. *See* IAN BROWNLIE, PRINCIPLES OF PUBLIC INTERNATIONAL LAW 12 (5th ed. 1998).

47. *See* THE EUROPEANISATION OF ADMINISTRATIVE LAW: TRANSFORMING NATIONAL DECISION-MAKING MECHANISMS (Karl-Heinz Ladeur ed., 2002).

48. For instance, the Framework Directive for telecommunications requires that national regulatory authorities be independent. *See* Council Directive 2002/21/EC on a Common Regulatory Framework for Electronic Communications Networks and Services, art. 3, 2002 O.J. (L 108) 33, 38 [hereinafter Framework Directive]. National administrations are required to consult the public when they undertake projects with possible environmental impacts. See Council Directive 85/337/EEC on the Assessment of the Effects of Certain Public and Private Projects on the Environment, 1985 O.J. (L 175) 40, when they regulate air and water quality, see Council Directive 96/61/EC Concerning Integrated Pollution Prevention and Control, 1996 O.J. (L 257) 26, and when they regulate the telecommunications industry, see Framework Directive, *supra*, at art. 6.

49. Member States are, almost without fail, required to notify the Commission of the measures taken to implement Directives. *See, e.g.*, Data Protection Directive, *supra* note 5, at art. 32.4. Examples of notification duties in the routine administration of European regulatory schemes include telecommunications, see Framework Directive, *supra* note 48, at art. 3, and public decency in television broadcasting, see Council Directive 97/36/EC Amending Council Directive 89/552/EEC on the Coordination of Certain Provisions Laid Down by Law, Regulation or Administrative Action in Member States Concerning the Pursuit of Television Broadcasting Activities, art. 23a, 1997 O.J. (L 202) 60.

50. For instance, in 1999, the Commission conducted an extensive review of the experience with European telecommunications regulation and proposed a series of new directives, which resulted in the passage of the Telecommunications Package in 2002. *See* Framework Directive, *supra* note 48; Council Directive 2002/20/EC on the Authorisation of Electronic Communications Networks and Services, 2002 O.J. (L 108) 21; Council Directive 2002/19/EC on Access to, and Interconnection of, Electronic Communications Networks and Associated

lished, not to replace domestic regulators, but to gather information for their use[51] or to serve as an alternative to national agencies for firms dissatisfied with their national systems.[52]

Lastly, in a number of areas including information privacy, European laws establish an elaborate sequence of national and supranational administrative decisions. In doing so, such laws routinize and legalize the networks of government officials that pervade European policymaking but that generally operate on an informal basis. In this procedure, which I shall refer to as "mixed administration"[53] or "mixed procedure," national authorities promulgate rules and bring enforcement actions but their decisions are checked and, in some instances, reversed by the Commission and other Member States acting through comitology committees.[54] Both national and European administrations share responsibility for a single determination of rights and duties under European law. The determination (to draw on categories familiar in systems of national administrative law) might be specific to an individual or firm, i.e., administrative adjudication, or generally applicable to a class of firms or individuals, i.e., administrative rulemaking.

This administrative architecture is highly unusual in national legal systems. It is unusual even when compared to a federal system like Germany in which legislative and administrative authority are usually divided between the federal government on the one hand and Länder

Facilities, 2002 O.J. (L 108) 7; Council Directive 2002/22/EC on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services, 2002 O.J. (L 108) 51. In the case of information privacy, the Commission conducted a review of national implementing laws and regulations in 2002 and 2003 and decided against amending the existing European regulatory framework. *See* First Report on the Implementation of the Data Protection Directive (95/46/EC), COM(03)265 final at 7. An illustration of prosecutorial action is the Commission's suit against France for failing to notify its implementing privacy legislation. Action Brought on 6 December 2000 by the Commission of the European Communities against the French Republic: Case C-449/00, 2001 O.J. (C 45) 11.

51. *See* Edoardo Chiti, *Administrative Proceedings Involving European Agencies*, 68 LAW & CONTEMP PROBS. (forthcoming Winter 2004) (discussing European Environmental Bureau).

52. *See id.* (discussing European Medicines Agency).

53. *See* Francesca Bignami, *Foreword* to 68 LAW & CONTEMP. PROBS. (forthcoming Winter 2004); Sabino Cassese, *European Administrative Proceedings*, 68 LAW & CONTEMP. PROBS. (forthcoming Winter 2004); Sabino Cassese, *Il diritto amministrativo europeo presenta caratteri originali?*, 53 RIVISTA TRIMESTRALE DI DIRITTO PUBBLICO 35, 44 (2003); EDOARDO CHITI & CLAUDIO FRANCHINI, L'INTEGRAZIONE AMMINISTRATIVA EUROPEA (2003); Giacinto della Cananea, *The European Union's Mixed Administrative Proceedings*, 68 LAW & CONTEMP. PROBS. (forthcoming Winter 2004).

54. For a description of comitology committees, see BIGNAMI, *supra* note 11, at 7–13; ELLEN VOS, INSTITUTIONAL FRAMEWORKS OF COMMUNITY HEALTH AND SAFETY LEGISLATION: COMMITTEES, AGENCIES AND PRIVATE BODIES 113 (1999).

governments on the other.[55] In what is known as "vertical federalism," the federal legislature passes laws but Länder governments are responsible for their day-to-day administration through enforcement decisions, the distribution of benefits, and the adoption of minor rules. Yet even in vertical federalism, government powers are split not shared. While the federal government has many tools for supervising Länder authorities, checking and possibly reversing individual administrative determinations is not one of them.[56]

Rather, European networks and their legalization through mixed procedure resemble decisionmaking in the international sphere through what Anne-Marie Slaughter calls "transgovernmental networks."[57] What are the similarities? Slaughter defines networks as: "a pattern of regular and purposive relations among like government units working across the borders that divide countries from one another and that demarcate the 'domestic' from the 'international' sphere."[58] In the case of transgovernmental networks, those government units are regulators—officials that staff national executive branches—and their relations are aimed at exchanging information, improving enforcement, and harmonizing regulatory standards.[59] According to Kal Raustiala, Slaughter, and a number of other scholars, the design and effect of such networks is to create convergence among national regulatory systems as well as to improve compliance with norms set down in treaties and other international instruments.[60] Slaughter contrasts networks with "traditional international organizations" like the World Trade Organization, where heads of state meet and sign treaties. She also paints networks as an alternative to a future world government "in which a set of global institutions perched above nation-states [enforce] global rules."[61]

European mixed procedure bears some of the same hallmark traits of transgovernmental networks: regulatory relations across national borders that have the purpose and effect of producing convergence in the day-to-day interpretation and enforcement of European norms. Furthermore,

55. *See generally* DAVID P. CURRIE, THE CONSTITUTION OF THE FEDERAL REPUBLIC OF GERMANY 69–76 (1994).

56. *Id. See also* Peter Lerche, *Principles of German Federalism in* GERMANY AND ITS BASIC LAW: PAST, PRESENT AND FUTURE: A GERMAN-AMERICAN SYMPOSIUM 71, 76–77 (Paul Kirchhof & Donald P. Kommers eds., 1993).

57. SLAUGHTER, *supra* note 9, at 40, 50. Slaughter recognizes the EU as one very important example of government by networks of ministers and regulators. With the exception of European agencies, however, she does not single out any particular form of European network.

58. *Id.* at 14.

59. *See id.* at 45–61.

60. *See* Kal Raustiala*, The Architecture of International Cooperation: Transgovernmental Networks and the Future of International Law*, 43 VA. J. INT'L L. 1 (2002); SLAUGHTER, *supra* note 9, at 171–95.

61. SLAUGHTER, *supra* note 9, at 6–7.

like transnational networks, mixed procedure is an alternative to the equivalent of "world government" in the European sphere, namely the concentration of implementation and enforcement powers in the hands of the European Commission (direct administration). Because of these common attributes—cooperation and harmonization without central government—we might expect that the reasons that give rise to mixed procedure in the European Union can also explain the emergence of transgovernmental networks in other regions of the world and globally. And because, in both European and transgovernmental networks, national regulators retain authority yet also belong to networks that condition how they exercise that authority, we can extrapolate from the normative consequences of mixed procedure to those of other transgovernmental networks.

Certain characteristics also set mixed procedure apart from generic transgovernmental networks. First, mixed procedure is a highly formal, legalized version of regulatory network. The law codifies the relationship between national and supranational officials by setting down a sequence comprised of national decision, notification to other national regulators and the Commission, and dispute resolution through a comitology committee should any of the other regulators disagree with the initial national decision. The law also specifies the network's powers and the types of decisions to be issued. By contrast, the information-sharing and harmonization activities of regulators in global networks often occur on an informal basis, without a legal instrument setting down the procedures and powers of the network.[62] Often, but not always. As Slaughter demonstrates, many transgovernmental networks are created by international treaty or executive agreement and are tasked with implementing the goals set down in the founding instrument; hence the law plays a similar role in their creation and operation as in European mixed procedure.[63] Furthermore, David Zaring shows that transgovernmental networks that start off as purely informal, ad hoc organizations over time can acquire a more formal basis: written rules of committee procedure, publication of the standards developed by the network, and procedures for consulting the public on such standards.[64] Zaring focuses on the Basle Committee on Banking Supervision and the International Organization of Securities Commissioners, but the same logic could very well drive the legalization of networks in other policy arenas. While, on the whole, law plays a

62. *Id.* at 48 (describing International Organization of Securities Commissioners, Basel Committee, and International Network for Environmental Compliance and Enforcement).

63. *Id.* at 45–48, 153–54.

64. *See* David Zaring, *Informal Procedure, Hard and Soft, in International Administration*, 5 CHI. J. INT'L L. (forthcoming 2005) (manuscript at 10,18, on file with author).

greater role in mixed procedure than in generic transgovernmental networks, this difference is not as significant as it appears at first glance.

A more important and fundamental difference between mixed procedure and other regulatory networks is the existence of authoritative supranational institutions in Europe that can resolve differences over the interpretation and application of the law governing the network. The European Commission, the Court of Justice, and the Court of First Instance are without equivalents in other regional or international regimes. As I have argued elsewhere, it is important to avoid exaggerating their powers in light of their limited resources, the incremental process through which their authority is being established, and the persistence of national administrative and judicial autonomy.[65] Nonetheless, the Commission and the European Courts are extraordinary institutions when compared to the institutions of international regimes; therefore, rights and duties under the law of European networks bind officials and citizens in a way that those set down in the law of global networks cannot.

2. Administration of Information Privacy Law

The application and enforcement of European information privacy law rests exclusively on indirect administration. The Commission does not have power to elaborate and enforce directly the provisions of the Data Protection Directive. The Directive, however, contains many of the institutional devices discussed earlier to curb national discretion in indirect administration. A number of provisions facilitate the development of common privacy norms and enforcement practices throughout the European Union. The Directive requires that each Member State establish, if not already in place, an independent privacy authority.[66] That government body is at the heart of an elaborate system laid down in the Directive for the enforcement of privacy rights. The independent privacy authority must establish a notification system for certain types of data processing operations; vet data processing operations that pose special risks to privacy through a licensing system; enforce information privacy law through inspections and administrative actions against suspected offenders; and receive complaints alleging the breach of privacy rights from individuals or associations that represent such individuals.[67] Furthermore, national privacy regulators are to encourage corporations and other enti-

65. *See* Francesca Bignami, *The Challenge of Cooperative Regulatory Relations after Enlargement*, *in* LAW AND GOVERANCE IN AN ENLARGED EUROPEAN UNION 97 (George A. Bermann & Katherina Pistor eds., 2004)

66. Directive, *supra* note 5, at art. 28 (Supervisory authority).

67. *Id.* at art. 18 (Obligation to notify the Supervisory authority), art. 19 (Contents of notification), art. 20 (Prior checking), art. 28 (Supervisory authority).

ties that deal in personal information to develop codes of conduct.[68] Moving to the Directive's provisions on national judiciaries, individuals must be able to go to court to vindicate their information privacy rights and they must be compensated fully for the damage suffered.[69]

The Data Protection Directive also employs mixed procedure to fetter national discretion. This it does in one limited area of application and enforcement of European privacy law: international data transfers. Under the Directive, Member States must ensure that when personal information is transferred to third countries (countries outside the European Union), those countries provide "an adequate level of protection" for information privacy. Adequacy is assessed by reference to the rights guaranteed under European information privacy law.[70] A mixed procedure is triggered in two distinct circumstances: a national privacy authority decides to block a transfer because it finds that a third country fails to ensure an adequate level of protection;[71] or, conversely, a national privacy authority decides to permit a transfer to an inadequate country (inadequate according to the national privacy authority) because special protections are in place.[72]

Consider the example of a country with widespread identity theft because its regulators fail to require security measures of information users. In the first type of mixed procedure, a national privacy authority that discovered the problem would be obliged to make a finding of inadequacy and block transfers of personal information to that country. The same privacy authority would be required to report its finding to the Commission, which in turn could initiate action to block data transfers to that country in all Member States or could enter into negotiations with that country with the intent of improving its privacy guarantees.[73] The Directive contemplates a Commission decision of adequacy upon completion of the negotiations, which would be valid in all Member States. In theory and in practice, however, the Commission adequacy determination can come at any time and not necessarily as the product of bilateral negotiations. Both courses of Commission action are entirely discretionary. Even though a Member State may find that citizens' privacy rights are abused by a third country, the Commission may or may not require that other Member States also block transfers of personal information to that third country and may or may not enter into negotiations with that

68. *Id.* at art. 27.
69. *Id.* at art. 22 (Remedies), art. 23 (Liabilities).
70. *Id.* at art. 25.1.
71. *Id.* at art. 25.
72. *Id.* at art. 26.
73. *Id.* at art. 25.3–25.5.

third country.[74] Furthermore, both decisions may be initiated by the Commission alone, not exclusively by the Member States, and therefore they do not represent necessarily the culmination of a mixed procedure.[75]

The second type of mixed procedure involves the decision to allow transfers of personal information to inadequate third countries. Even if a third country does not guarantee an adequate level of privacy protection, Member States may authorize transfers on six separate grounds listed in the Data Protection Directive.[76] Those grounds are: (1) the individual has consented "unambiguously" to the proposed transfer of her personal information; (2) the transfer is necessary for performance of a contract between the individual and the business; (3) the transfer of the personal information is necessary for the entry into or performance of a contract between the business and a third party for the individual's benefit; (4) the transfer is justified on "important public interest grounds" or for purposes of a lawsuit; (5) the transfer of the personal information is necessary to protect the "vital interests" of the individual; or (6) the transfer is from a database to which the public routinely has access because of national laws on access to documents. Member States are permitted to authorize transfers on additional grounds, not specifically enumerated in the Directive, but in such cases they must notify the Commission and the other Member States.[77] In the example of a country with an identity theft problem, a Member State might decide to permit a transfer if a contract between the corporation and the receiving party renders that party liable in tort for any loss or theft of the personal information. Such a decision would have to be notified to the Commission and the other Member States.[78] If either the Commission or another Member State objected to the transfer, the matter would be taken up by the Commission, which would make the final decision on whether to permit the transfer.[79]

---

74. The Commission's citizen rights guide explains the procedure in the following manner:

> Where a non-EU country does not ensure an adequate level of protection, the Directive requires the blocking of specific transfers. Member States must inform the Commission of any such blocking measures, and this triggers a Community procedure to ensure that any Member State's decision to block a particular transfer is either extended to the EU as a whole, or reversed.

EUROPEAN COMMISSION, DATA PROTECTION IN THE EUROPEAN UNION 12, *at*: http://europa.eu.int/comm/internal_market/privacy/docs/guide/guide-ukingdom_en.pdf

75. Directive, *supra* note 5, at art. 25, 26.4 (giving Commission as well as Member States the right of initiative).

76. *Id.* at art. 26.1.

77. *Id.* at art. 26.2–26.3.

78. *Id.* at art. 26.

79. *Id.* at art. 26.3.

In both types of mixed procedure, the Commission must act together with a comitology committee of Member State representatives and must seek the opinion of a working party of national privacy authorities.[80] In other words, the Commission does not act alone but rather must respect the preferences of national regulators responsible for information privacy in the Member States. The role of the comitology committee is typical of virtually all areas in which the Commission is delegated powers of implementation by the Council and Parliament. The working party of national privacy authorities, on the other hand, is fairly unusual and reflects the decision in favor of independent regulators to enforce privacy rights at the national level. Hence the need to incorporate their expertise and preferences at the European level through a committee of their own. Such committees exist in only a handful of other European policy areas such as securities and telecommunications.[81]

3. Italian Implementation

To understand and evaluate the European regulation of information privacy, it is important to consider national laws and institutions. The Data Protection Directive, like all directives, does not have immediate effect but requires that the Member States pass implementing laws. Like the vast majority of directives, it leaves the Member States with considerable discretion as to how to implement its provisions. On the ground, both the substantive and procedural guarantees contained in the Directive vary considerably from one Member State to another. The normative assessment of European networks, which comes in Part Four of the Article, also depends on the Member State. European democracies have developed different laws to guarantee rights and democratic accountability in government by bureaucrats. Thus the liberal democratic tradition and the challenge posed to that tradition by the plural, fragmented world of European regulatory networks vary considerably from one country to the next.

To fully explore these questions, I examine the Italian case. A number of criteria informed the choice of Italy as the national case. First,

80. *Id.* at arts. 30.1(b), 31. The committee of Member State representatives is a management committee, meaning that a qualified majority of the national regulators on the committee is required to oppose a Commission decision and send the decision to the Council for a vote. In regulatory committees, by contrast, only a blocking minority of national regulators is necessary to force the Commission to send the decision to the Council. In other words, in the data protection area, national regulators on the committee influence the Commission but not to the same extent as they do in fields with regulatory committees.

81. *See* Rosa M. Lastra, *The Governance Structure for Financial Regulation and Supervision in Europe*, 10 COLUM. J. EUR. L. 49, 62 (2003) (securities); David Lazer & Viktor Mayer-Schönberger, *Governing Networks: Telecommunication Deregulation in Europe and the United States*, 27 BROOK. J. INT'L L. 819, 847–49 (2002) (telecommunications).

Italy has the longest experience with the Data Protection Directive. It was the first Member State to pass implementing legislation, back in 1996, well before the deadline for implementation expired.[82] Second, Italian law is representative of the many Member States whose administrative law was influenced by the Napoleonic model in which a specialized court reviews administrative action (the *droit administratif* tradition).[83] Third, my knowledge of the Italian language enabled me to examine directly the legal sources and therefore rendered the case study not only more manageable but also more rigorous.

In implementing the Directive, the Italian government chose to minimize the notification and authorization components of the regulatory scheme.[84] Corporations, government agencies, and other entities are not required, for the most part, to submit their information collection and analysis operations to the Italian privacy authority (*Garante per la protezione dei dati personali* or *Garante*) for review and approval before such operations may commence. The privacy rights and duties set down in the Italian legislation operate as standards that data users are expected to follow or else risk administrative injunctions and fines, criminal prosecutions, and civil actions.[85]

The Italian regulatory scheme's reliance on legal duties and sanctions rather than licensing and screening applies to international data

82. Legge 31 dicembre 1996 n. 675, Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali [Law No. 675 of Dec. 31, 1996, Protection of Individuals and Other Subjects with Regard to the Processing of Personal Data], Gazz. Uff., no. 5 (Jan. 8, 1997) (Italy). Subsequent to the enactment of this legislation a number of significant amending regulations were promulgated. *See* Decreto Legislative 26 febbraio 1999 n. 51 [Decree-Law No. 51 of Feb. 26, 1999], Gazz. Uff., no. 56 (Mar. 9, 1999) (Italy); Decreto Legislativo 28 dicembre 2001 n. 467 [Decree-Law No. 467 of Dec. 28, 2001], Gazz. Uff., no. 5 (Jan. 8, 1997) (Italy). In 2003, the entire corpus of legislation was systematized and modified slightly in the Personal Data Protection Code. *See* Decreto Legislativo 30 giugno 2003 n. 196, Codice in materia di protezione dei dati personali [Decree-Law No. 196 of June 30, 2003, Personal Data Protection Code], Gazz. Uff., no. 174 (July 29, 2003) (Italy).

83. Those Member States include France, Spain, Greece, and Belgium. *See* JOHN HENRY MERRYMAN, THE CIVIL LAW TRADITION: AN INTRODUCTION TO THE LEGAL SYSTEMS OF WESTERN EUROPE AND LATIN AMERICA (2d ed. 1985); L. NEVILLE BROWN & JOHN S. BELL, FRENCH ADMINISTRATIVE LAW 1–8 (5th ed. 1998).

84. For the original requirements enacted in 1996, see Law No. 675 of Dec. 31, 1996, art. 7 (notification) and art. 22.1 (authorization). For the current requirements, see Decree-Law No. 196 of June 30, 2003, Personal Data Protection Code, at art. 26 (authorization for private sector use of sensitive data).

85. Personal Data Protection Code, at arts. 141–72. On the differences among Member States, the British case is instructive. The UK, unlike Italy, requires notification for many classes of personal information but does not require prior authorization. Moreover, the British Information Commissioner has the power to enjoin illegal personal information operations but does not have the power to impose administrative fines for the initial breach of privacy law. *See* HEATHER ROWE, DATA PROTECTION ACT 1998: A PRACTICAL GUIDE 95–103 (notification), 117–22 (enforcement powers) (1999).

transfers. Corporations and other entities are bound by the duty to stop transfers of personal information to inadequate third countries:

> [I]t shall be prohibited to transfer personal data that are the subject of processing from the State's territory to countries outside the European Union, temporarily or not, and in any form and by any means whatsoever, if the laws of the country of destination or transit of the data do not ensure an adequate level of protection of individuals. Account shall also be taken of the methods used for the transfer and the envisaged processing operations, the relevant purposes, nature of the data and security measures.[86]

If the Garante suspects that a corporation or other entity has breached this duty, it may undertake an investigation and impose certain restrictions on, or block altogether, future international data transfers of the same type.[87] Failure to comply with the Garante's administrative injunction can lead to criminal prosecution and imprisonment of three months to two years.[88] Moreover, individuals harmed by the transfer of their personal information in violation of the law may sue for material damages and emotional distress (*danni non-patrimoniali*) and may claim compensation for emotional distress regardless of whether they can also show physical or economic harm.[89] Lastly, in extreme cases, the Garante can refer breaches to the public prosecutor directly, without first taking administrative action, and the public prosecutor may bring a criminal action against the offending corporation for imprisonment between one and three years.[90] Any administrative or judicial decision to impose a sanction for transfer of personal information to an inadequate third country would have to be notified to the European Commission under the Data Protection Directive and could give rise to the mixed procedure described earlier.[91]

Tracking the Directive, the Italian law enumerates exceptions to the ban on transfers to third countries with inadequate privacy safeguards.[92] The Italian legislation also provides that the Garante may allow such transfers on grounds other than those specifically enumerated in the

86. Personal Data Protection Code, at art. 45.

87. *Id.* at arts. 143, 150, 154.

88. *Id.* at art. 170.

89. *Id.* at art. 15. *See also* S.S. Sica, *Le tutele civili*, *in* IL CODICE DEI DATI PERSONALI: TEMI E PROBLEMI 541 (Francesco Cardarelli et al. eds., 2004) (explaining system of tortious liability for infringement of privacy rights).

90. Personal Data Protection Code, at art. 167.2.

91. Directive, *supra* note 5, at arts. 25–26; *see also supra* text accompanying notes 72–79.

92. *Id.* at art. 43.

legislation, such as privacy-protecting contractual terms.[93] These exceptions can come either in the form of an individual authorization (*autorizzazione*), giving the corporation assurances in advance of a particular transfer that the Garante will not take enforcement action, or in the form of a block authorization (*autorizzazione generale*), permitting certain classes of transfers[94] Under the Data Protection Directive, such exceptions must be notified to the European Commission and could give rise to the mixed procedure outlined above.

II. Experience with the Regulation of International Data Transfers

To date, the Commission has issued adequacy decisions for five countries and two territories of the UK: Hungary, Switzerland, the United States, Canada, Argentina, Guernsey, and the Isle of Man.[95] In the case of the two decisions applicable to the United States, the adequacy findings apply not to the overall regulatory framework for privacy but to the transfer of airline passenger data to the U.S. government and to certain "Safe Harbor Principles" which, if adopted by firms, guarantee compliance with the Directive's requirements. The Commission has also issued two decisions specifying standard contract clauses which, if adopted by the parties to a data transfer, guarantee privacy rights regardless of the public regulatory regime.[96] The Garante implemented most of the earlier Commission decisions through block authorizations (*autorizzazioni generali*). Firms and public entities that export to Hungary, Switzerland, Canada, Argentina, or the United States (respecting the

93. *Id.* at art. 44.

94. *Id.* at arts. 40–41. Authorizations are a standard form of administrative action in Italy. *See, e.g.,* Aldo Sandulli, *Il Procedimento*, *in* 2 Trattato di Diritto Amministrativo: Diritto Amministrativo Generale 1035, 1271 (Sabino Cassese ed., 2d ed. 2003).

95. Commission Decision 2000/519/EC, 2000 O.J. (L 215) 4 (Hungary); Commission Decision 2000/518/EC, 2000 O.J. (L 215) 1 (Switzerland); Commission Decision 520/2000/EC, 2000 O.J. (L 215) 7 (U.S. Safe Harbor Principles); Commission Decision 2004/535/EC, 2004 O.J. (L 235) 11 (transfers of airline passenger data to U.S. government); Commission Decision 2002/2/EC, 2002 O.J. (L 2) 13 (Canada); Commission Decision 2003/490/EC, 2003 O.J. (L 168) 19 (Argentina); Commission Decision 2003/821/EC, 2003 O.J. (L 308) 27 (Guernsey); Commission Decision 2004/411/EC, 2004 O.J. (L 151) 48 (Isle of Man).

96. Commission Decision 2001/497/EC, 2001 O.J. (L 181) 19; Commission Decision 2002/16/EC, 2002 O.J. (L 6) 52. The first standard contract contains terms on the duties of information exporting firms and those of information importing firms; individuals whose personal information is transferred have a right to sue to enforce the contract, as third-party beneficiaries. The second standard contract contains similar terms but applies in cases in which a third country firm processes data on the behalf of an information exporting firm. *See generally*, Christopher Kuner, European Data Privacy Law and Online Business 146–56 (2003).

Safe Harbor Principles) or that include the standard clauses in their contracts (regardless of destination country) can rest assured that they are in compliance with Italian information privacy law. The Garante has not yet issued block authorizations for some of the more recent Commission decisions. Nevertheless, corporations and other entities can transfer airline passenger data to the U.S. government and all classes of personal information to Argentina, Guernsey, and the Isle of Man because, under European law, individuals may rely on Commission decisions even in the absence of an Italian implementing act.[97]

In addition, the working party of European privacy authorities, established under Article 29 of the Directive, has issued a number of opinions which have not yet resulted in Commission adequacy determinations. In one recent opinion, the working party approved of the Australian government's system of privacy for airline passenger data and, most likely, a Commission adequacy decision will follow.[98] In the other opinions, the working party expressed reservations about the foreign privacy regimes under consideration and the Commission is engaged in bilateral negotiations to obtain additional safeguards in those countries. One involves the general regulation of information privacy in Australia.[99] The other concerns Canada's protection of airline passenger data when transferred to the government for purposes of surveillance and counter-terrorism measures.[100]

When the Data Protection Directive was first drafted, Member States expected that, initially, national government officials would assess privacy in third countries and then, over time, any dissatisfaction would percolate up to the Commission. As they said in the negotiations on the Directive:

> [This Article] gives a certain degree of flexibility to the Member States. Initially, it is for them to decide, following procedures that they will choose themselves, on the adequate level of protection in

97. *See* CRAIG & DE BÚRCA, *supra* note 6, at 189 (describing direct effect of decisions).

98. *See* Opinion 1/2004 on the Level of Protection Ensured in Australia for the Transmission of Passenger Name Record Data From Airlines, Op. Working Party on the Prot. of Individuals with Regard to the Processing of Pers. Data, 10031/03/EN WP 85 (Jan. 16, 2004) (approving Australian system of protection of airline passenger data).

99. *See* Opinion 3/2001 on the Level of Protection of the Australian Privacy Amendment (Private Sector) Act 2000, Op. Working Party on the Prot. of Individuals with Regard to the Processing of Pers. Data, 5095/00 WP 40 final (Jan. 26, 2001). The Commission is negotiating with Australia to secure additional privacy safeguards. E-mail from European Commission, DG Markt, Unit Data Protection (Dec. 18, 2002) (on file with author).

100. *See* Opinion 3/2004 on the Level of Protection Ensured in Canada for the Transmission of Passenger Name Records and Advanced Passenger Information from Airlines, Op. Working Party on the Prot. of Individuals with Regard to the Processing of Pers. Data, 10037/04/EN WP 88 (Feb. 11, 2004).

> third countries, taking into account certain criteria enumerated in [Article 25.2]. In a later phase, a Community procedure will be launched in order to ensure a common approach which is well-structured in this area.[101]

Yet these expectations have not been met. In neither type of mixed procedure have national regulators been active in specifying the conditions for data transfers to particular third countries and in blocking transfers that fail to satisfy such conditions.

No Member State has ever notified the Commission, pursuant to Article 25 of the Directive, of a decision to block a data transfer because of adequacy problems.[102] Each of the Commission adequacy decisions surveyed above was initiated not by a Member State but rather by the Commission or the third country itself.[103] Therefore the first type of mixed procedure established under the Data Protection Directive is, in practice, a dead letter.

The second type of mixed procedure, the authorization of transfers to inadequate third countries, has seen more use but still is insignificant in light of the volume of trade with countries lacking information privacy legislation altogether or with less extensive safeguards for privacy rights. According to figures reported in December 2002, over four years after the Directive had come into force, national authorities had notified the Commission on seventeen occasions of special authorizations permitting personal information to be exported to inadequate third countries.[104] Most of these notifications involved contracts that, according to the national privacy regulator, guaranteed individual privacy rights. Spain was the most active, with eight notifications, followed by Finland with four,

101. Council Doc. 9957/94, Rapport du Groupe des questions économiques (Protection des données) en date des 6/7 octobre 1994 au Comité des Représentants Permanents [Report of Working Party on Economic Questions (Data Protection) dating from Oct. 6–7, 1994 to the Committee of Permanent Representatives, Brussels], 12 (Oct. 18, 1994) (on file with author).

102. E-mail from European Commission, DG Markt, Unit Data Protection (Nov. 17, 2004) (on file with author); E-mail from European Commission, DG Markt, Unit Data Protection (Dec. 18, 2002) (on file with author).

103. In the case of Argentina, the Argentine government sought an adequacy decision from the Commission. *See* Opinion 4/2002 on the level of protection of personal data in Argentina, Op. Working Party on the Prot. of Individuals with Regard to the Processing of Pers. Data, MARKT 11081/02/EN WP 63, at 2 (Oct. 3, 2002). The Commission initiated adequacy proceedings for Switzerland and Hungary because both had ratified the Council of Europe Convention, thus providing prima facie evidence of adequacy, and both showed some interest in obtaining adequacy decisions. In the case of Canada and the United States, both governments initiated discussions with the Commission with an eye to avoiding trade disruptions. *See* e-mail from European Commission, DG Markt, Unit Data Protection (Dec. 18, 2002) (on file with author).

104. E-mail from European Commission, DG Markt, Unit Data Protection (Dec. 18, 2002) (on file with author).

Portugal with three, and Germany and the Netherlands each with one. None of these notifications, however, resulted in further action at the European level, since neither the Member States nor the Commission raised objections that would trigger a comitology procedure.

In 2003, the Commission recognized that the enforcement of European privacy rights in the international trade context was disappointing. In a report on the implementation of the Data Protection Directive, the Commission criticized national privacy authorities. According to the report, "[m]any unauthorised and possibly illegal transfers are being made to destinations or recipients not guaranteeing adequate protection."[105]

The Commission called the number of notifications under the second type of mixed procedure, i.e., transfers to countries without adequate privacy laws, "derisory by comparison with what might reasonably be expected."[106] It believed that transfers to countries without adequate privacy safeguards were being made and that national authorities had failed to clamp down, either by prohibiting the potentially illegal transfers or by requiring special guarantees. In a subsequent letter, the Commission urged national privacy authorities to ensure that authorizations allowing export of personal information to inadequate third countries were notified to the Commission and other Member States.[107] In other words, the Commission called upon national regulators to put into practice the second type of mixed procedure foreseen in the Directive. The Commission identified three related goals: improving the level of protection for Europeans' personal information outside the European Union; increasing awareness among national regulators and the Commission of the circumstances surrounding third country transfers; and facilitating the exchange of best practices when personal information is sent to inadequate third countries.[108]

Since the Commission issued the letter, notifications have improved slightly. Between August 2003 and October 2004, thirty-three transfers to countries without adequate information privacy safeguards were approved by national authorities and notified to the Commission.[109] Over the period of one year, thirty-three notifications is considerable when

105. Report from the Commission: First Report on the Implementation of the Data Protection Directive (95/46/EC), COM(2003) 265 final at 19.

106. *Id.*

107. Note from European Commission Internal Market DG to Member States and Data Protection Authorities, MARKT/E4/LCN/ck D (2003) 270 (Aug. 21, 2003), *available at* http://europa.eu.int/comm/internal_market/privacy/docs/lawreport/notification-art-26_en.pdf.

108. *Id.*

109. E-mail from European Commission, DG Markt, Media and Data Protection Unit (Nov. 17, 2004) (on file with author). Some of the notifications involved multiple companies within the same parent company and therefore the actual number of authorizations granted by national privacy authorities is slightly higher.

compared with the seventeen notifications from the previous four years. Yet in light of the volume of trade between the European Union and the rest of the world, much of which does not follow the European approach to information privacy, it is still difficult to believe that Europeans' privacy is protected when their data is transferred abroad.

III. EXPLAINING NETWORKS

Why do government regulators decide to forego exclusive power over policy decisions and join networks? For even though networks are not as constraining as a hypothetical world government, they nonetheless curb national autonomy and limit sovereignty. By creating the expectation that their officials will reveal their national policies and enforcement practices and will cooperate with other officials by assisting foreign enforcement actions and adopting "best practice" regulatory standards, governments renounce unilateral control over policymaking in their territories. To translate the question into the European context: Why, when Member States draft European legislation, do they establish networks, i.e., mixed procedure, rather than retain powers of implementation for themselves, i.e., classic indirect administration? This section develops an explanation for the European privacy case by drawing on the theory of European integration and records from the negotiation of the Data Protection Directive. The section concludes by developing the implications for transgovernmental networks beyond Europe.

A. *The European Privacy Network*

The European privacy network has remarkably few powers and responsibilities under the Data Protection Directive.[110] The network is tasked only with administering international data transfers. Yet the Data Protection Directive seeks to protect information privacy and regulate information collection, analysis, and transfer in a vast array of economic sectors and areas of government activity. Any number of areas of national application of the Directive could have benefited from the harmonizing effect of a European network.[111] The Directive could have

110. The point of comparison is other fields such as food safety and telecommunications and the powers that might be expected given the objective need for harmonization in the information privacy field.

111. In fall 2002, the Commission called for comments on the implementation of the Data Protection Directive. The companies and trade associations that responded were unanimous in calling for greater uniformity among the Member States in their application of the Directive. *See* Bundesverband der Deutschen Industrie & Bundesvereinigung der Deutschen Arbeitgeberverbände, Joint Position on the Online Consultation by the European Commission (DG Internal Market) on Application of Data Protection Directive 95/46/EC (Sept. 4, 2002), *available at*

required the Member States to notify the Commission of national rules governing matters such as the conditions for obtaining individual consent to the collection of personal information and could have allowed the Commission, acting together with other Member States, to object.[112] Countries that require authorization for sensitive data could have been required to notify the Commission and other Member States when they granted or denied authorizations, as is the case for genetically modified organisms.[113] The same type of procedure could have been put into place for national investigations and sanctions, as exists in food safety law[114] and competition law.[115] After all, a corporation alleged to have breached privacy rights in one Member State might very well have breached them elsewhere, in which case the duty to inform is vital. Or in the absence of Commission notification, the same investigation might be undertaken in

http://europa.eu.int/comm/internal_market/privacy/docs/lawreport/paper/bda_en.pdf (calling for greater uniformity on the question of whether personal data covers both natural persons and firms, on conditions for obtaining consent, on a firm's place of establishment for purposes of determining applicable law, and on notification procedures); Confederation of British Industry, Comments on Directive 95/46 re data protection (Aug. 30, 2002), *available at* http://europa.eu.int/comm/internal_market/privacy/docs/lawreport/paper/cbi_en.pdf (calling for greater uniformity on obtaining consent); Covington & Burling, Comments on Implementation and Application of the 1995 Data Protection Directive, *available at* http://europa.eu.int/comm/internal_market/privacy/docs/lawreport/paper/covington-burling_en.pdf (recommending uniformity in the definitions of personal data and establishment and calling for a greater role of the art. 29 working party in eliminating inconsistent interpretations at the national level); Prof. Dr. Büllesbach, Chief Data Protection Officer, Daimler Chrysler, Presentation before the European Commission (Sept. 30, 2002) (calling for uniformity on question of whether Directive protects both natural persons and firms, consent, sensitive data, establishment, notification requirements, and third country transfers); UNICE, Implementation of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data of 24 October 1995 (August 30, 2002) *available at* http://europa.eu.int/comm/internal_market/privacy/docs/lawreport/paper/unice_en.pdf (calling attention to disparities in levels of data protection generally and definitions of consent and sensitive data in particular).

112. Such notification duties are common in European law. For instance, Member States are required to notify the Commission of new technical standards for industrial goods, and the Commission or other Member States may object on the grounds that they create barriers to trade which are not justified for legitimate public policy reasons. *See* Council Directive 83/189/EEC, arts. 8–9, 1983 O.J. (L 109) 8.

113. *See* Damian Chalmers, *Risk, Anxiety and the European Mediation of the Politics of Life: The European Food Safety Authority and the Government of Biotechnology*, Paper presented to the Harvard European Law Association 4–6 (Oct. 29, 2004), http://www.law.harvard.edu/students/orgs/hela/papers/chalmerssocialregulation112.doc.

114. In the event of an outbreak of disease in livestock, national authorities must take protective measures and notify the Commission and other Member States. If the Commission or other Member States find the measures inadequate, the matter goes to a comitology procedure, and more protective measures may be adopted. *See* Council Directive 90/425/EEC, art. 10, 1990 O.J. (L 224) 29.

115. Commission Notice on Cooperation between National Competition Authorities and the Commission in Handling Cases Falling within the Scope of Articles 85 or 86 of the EC Treaty, point 49, 1997 O.J. (C 313) 3.

multiple jurisdictions, creating the risk of conflicting administrative and judicial decisions and the duplication of efforts.

Why, then, were so few powers delegated to the European privacy network? A number of political scientists have examined the institutional choices made in the Treaties and in European laws.[116] Their research has addressed several questions of institutional design: the decision in the founding Treaties to delegate powers of proposal and enforcement to the Commission and to require the Council to act by unanimity in certain policy areas but by qualified majority in other areas;[117] the choice, when drafting European laws, to delegate rulemaking powers to the Commission alone or to the Commission acting together with a committee of national regulators; and the decision, if the Commission is required to act together with a committee of national regulators, to give the committee significant power, i.e., regulatory or management committees, or very little power, i.e., advisory committees.[118] The political science literature has largely ignored the phenomenon of mixed procedure. But a similar choice is made when Member States decide to retain exclusive power over the application and enforcement of European law through indirect administration or to allow the Commission and other national regulators, sitting on comitology committees, to supervise their government officials through mixed procedure.

In the political science literature on European integration a number of explanations have been advanced for delegations of power to supranational institutions like the Commission or intergovernmental bodies like the Council of Ministers and comitology committees. According to some, such institutions offer superior information on technical policy matters, above and beyond what can be generated by national administrations.[119] In a related argument, Mark Pollack has found evidence that powers are delegated to the Commission and other European institutions when speedy and efficient Europe-wide decisionmaking is needed.[120] Giandomenico Majone and Andrew Moravcsik have separately advanced the hypothesis that transfers of power to the Commission or intergovernmental bodies are driven by the need for credible commitments.[121]

116. *See* ANDREW MORAVCSIK, THE CHOICE FOR EUROPE: SOCIAL PURPOSE AND STATE POWER FROM MESSINA TO MAASTRICHT 73 (1998); MARK A. POLLACK, THE ENGINES OF EUROPEAN INTEGRATION: DELEGATION, AGENCY, AND AGENDA SETTING IN THE EU 19–74 (2003).

117. *See* MORAVCSIK, *supra* note 116, at 67.

118. *See* POLLACK, *supra* note 117, at 3, 114–130.

119. *See* Giandomenico Majone, *The New European Agencies: Regulation by Information*, 4 J. EUR. PUB. POL'Y 262, 263 (1997).

120. *See* POLLACK, *supra* note 117, at 107.

121. Giandomenico Majone, *Two Logics of Delegation: Agency and Fiduciary Relations in EU Governance*, 2 EUR. UNION POL. 103 (2001); MORAVCSIK, *supra* note 116, at 73 (1998).

That is, in pursuing mutually beneficial policies such as free trade, Member States operate in a classic prisoner's dilemma game in which, over time, they might be tempted to defect from the free trade line. To reassure the other parties to the strategic interaction that they will not defect, Member States commit themselves to the policy by giving powers of monitoring, sanctioning, and future decisionmaking to institutions with some degree of independence from national governments.

The information privacy case can be explained by neither the expertise nor the speed theories. Both would have predicted more extensive transfers of authority in the Data Protection Directive. Protecting privacy rights in the highly complex and rapidly changing field of information technology is extremely challenging; supranational mechanisms that afforded the prospect of expert and speedy solutions should have been attractive to the Member States. Such mechanisms, however, did not materialize in the Data Protection Directive. Rather, the Member States which negotiated the Directive were extremely reluctant to transfer policymaking authority to the European privacy network.

The privacy network's limited powers are consistent, instead, with the credible commitments theory. The Directive was highly contentious, with the result that even after five years of bargaining, the text ultimately adopted was so open-ended that it could accommodate most of the existing differences among the Member States.[122] In other words, the Member States entered the negotiations on the Directive with vastly different preferences for information privacy.[123] Because they had opposing views on the importance of privacy as a civil liberty, they were in no rush to credibly commit to a future stream of decisionmaking through networks. Moreover, to the extent that certain Member States had strong preferences for or against information privacy, they were unwilling to make concessions in other policy areas to induce opposing Member States to adopt their position in the Directive.[124] Additionally, the policy on which the Member States were in agreement—the free movement of personal

See also Andrew Moravcsik, *Taking Preferences Seriously: A Liberal Theory of International Politics*, 51 INT'L ORG. 513 (1997) (Moravcsik articulating his theory of liberal institutionalism for international relations more generally).

122. *See* Simitis, *Data Protection in the European Union*, *supra* note 34, at 111–12; Simitis, *From the Market to the Polis*, *supra* note 15, at 457–58.

123. The European Parliament is absent from my account of the politics of the Directive because, at the time, it was not very influential. During the period when most of the drafting decisions were made, the Parliament only had powers of cooperation on harmonization measures, not powers of co-decision. *See* CRAIG & DE BÚRCA, *supra* note 6, at 140–47 (describing difference between cooperation and co-decision).

124. On the use of linkages across policy areas to induce agreement and bargains in international negotiations, *see, e.g.*, Christina L. Davis, *International Institutions and Issue Linkage: Building Support for Agricultural Trade Liberalization*, 98 AM. POL. SCI. REV. 1 (2004).

information throughout the European Union to facilitate commerce—was not threatened by national differences in privacy regulation. In the entire history of the field, which stretches back to the first German and Swedish legislation in the early 1970s, information transfers from one jurisdiction to another jurisdiction had been blocked because of privacy concerns in only a handful of cases.[125]

The bargaining history of the Directive contains significant evidence for this hypothesis.[126] First, the record shows that the Member States actively opposed the Commission's attempt to shift policymaking authority to European institutions, namely the Commission and a comitology committee. Although the Commission originally proposed an extensive role for European institutions, the Member States subsequently reduced that role to a minimum.

The first version of the Directive, published by the Commission in 1990, gave the Commission rulemaking authority in all areas covered by the Directive.[127] Furthermore, an advisory committee would have monitored the Commission, meaning that the Member States would have had relatively little influence over the Commission.[128] Therefore, had the initial proposal gone through, the Commission would have been able to harmonize everything from notification and authorization processes to the specific requirements for obtaining consumer consent and securing personal data, with only a marginal role for the Member States.

---

125. *See infra* text accompanying note 154.

126. Negotiations on the Directive began with the publication of the Commission's proposal on September 13, 1990, Communication on the Protection of Individuals, *supra* note 36, COM(90)314 final-SYN 287 (basic directive proposal) and 288 (sector-specific telecommunications privacy proposal), and ended with the publication of the Directive on October 24, 1995. I obtained access to the Council records by filing an access to documents request. The record includes minutes from at least twenty-five meetings of national civil servants (Working Party on Economic Questions (Data Protection)), four meetings of high-ranking diplomats from Member State permanent representations to the European Union (COREPER), and two meetings of national ministers (Council of Ministers). The record also includes numerous working documents circulated between the meetings.

127. Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data, art. 29, 1990 O.J. (C 277) 3 ("The Commission shall . . . adopt such technical measures as are necessary to apply this Directive to the specific characteristics of certain sectors having regard to the state of the art in this field and to the codes of conduct.").

128. *Id.* at art. 30. There are three types of committees of national representatives created to supervise the Commission when it implements European laws: advisory, management, and regulatory committees. The main difference is the degree of control they have over Commission decisionmaking. With an advisory committee, the Commission must simply "take into account" the committee's opinion. A management committee has a veto power over Commission decisions, meaning that it may vote against a Commission decision, while a regulatory committee has the power of assent, meaning that it must vote in favor of a Commission decision. BIGNAMI, *supra* note 11, at 8–13 (describing different types of comitology committees).

Over the course of the Council deliberations, however, the Member States all but eliminated the Commission's powers. In the Council, the Member State representatives who worked on the Directive for almost five years disagreed on many things, but the Commission's powers was not one of them. From the very beginning, they were unanimous on the need for a stronger comitology committee of Member State representatives to discipline the Commission.[129] Ultimately, a compromise was reached with the European Parliament, generally more supportive of the Commission position, in which a management committee with the power to veto the Commission's implementing measures was instituted.[130] Furthermore, toward the very end of the negotiations in the Council, at the point when the Directive was escalated from the technical working party to the Committee of Permanent Representatives (COREPER), the Commission's executive powers were eliminated at France's insistence.[131] All that was left was the power to regulate international data transfers through the mixed procedure analyzed in this Article.

The Member States also watered down the powers of the European privacy network in the area of international data transfers. As explained previously, the procedure established under the Directive allows national regulators to authorize transfers to third countries and then gives the Commission and Member States the opportunity to object. The initial versions of the Directive afforded greater protection for the right to object, giving European actors—the Commission and other Member States

129. *See* Council Doc. 8268/91, Results of Deliberations (Travaux) of Working Party on "Economic Questions" (Data Protection) (Sept. 19, 1991). At this meeting, a large number of Member States advocated a regulatory committee. By late 1994, all of the Member States, with the exception of Belgium, were in favor of the strongest form of regulatory committee (type IIIB), with Belgium advocating the slightly weaker form (type IIIA). *See* Council Doc. 10957/94, Summary Minutes from the 1628th Meeting of the Committee of Permanent Representatives in Brussels (Nov. 14, 1994). At the time, the only difference between the two types of regulatory committee was that, if a IIIB committee did not give its assent and the Commission's proposed measure was sent to the Council, the Council could simply veto the measure rather than having to agree on an alternative to the Commission's measure.

130. Data Protection Directive, *supra* note 5, at art. 31. The UK wanted to reject the European Parliament's amendment establishing a management committee, which would have required further negotiations with the Parliament on a so-called "conciliation committee." However, the UK was out-numbered by the other delegations. Council Doc. 9016/95 EXT 2(f), Summary Minutes of the 1662th meeting of the Committee of Permanent Representatives, First Part, Brussels (July 13, 1995).

131. Council Doc. 11369/94, Report of the Committee of Permanent Representatives of November 24, 1994 to the Internal Market Council of Ministers of December 8, 1994. In this report, COREPER pointed out that the Commission under the existing version had extensive powers of execution and that, in France's view, such powers should be eliminated. In the Council's version of the Directive, officially adopted on February 24, 1995, the Commission's general rulemaking authority had vanished. *See* Communication of the Commission to the European Parliament concerning the Council's common position, SEC (95) 303 final-COD 287 (Feb. 24, 1995).

on the comitology committee—a greater role in the national decision on transfers of personal information abroad. In the Commission's first proposal, a national decision to allow a transfer to an inadequate third country could only take effect ten days after notification to the Commission, to allow time for either the Commission or other Member States to object before the transfer occurred.[132] In the Commission's second proposal, the ten-day guarantee was replaced by a vaguer Member State duty to notify the Commission and other Member States in "good time of its proposal to grant authorization."[133] By the time the Council had finished deliberating, the waiting period had disappeared altogether. Under the Directive, Member States must simply notify the Commission *after* the authorization has been granted.[134] The record of the Council negotiations shows that this last modification was made after the UK, Denmark, Ireland, and Sweden objected that the third country procedure was too "heavy" and "bureaucratic."[135]

Second, the record demonstrates extreme disagreement among national representatives on privacy, lending support to the hypothesis that the Member States' opposition to sharing power in an administrative network was driven by disagreement over the substance of information privacy policy.[136] On one extreme was the UK, supported to various degrees by Ireland, the Netherlands, Denmark, Finland, Norway, and Sweden. This northern bloc did not see the need for a Data Protection Directive and would have preferred to rely simply on the Council of Europe Convention.[137] The northern bloc, joined sometimes by other

132. Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data, art. 25.1, 1990 O.J. C 277 (3).

133. Amended Proposal for a Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data, art. 27.2, 1992 O.J. (C 311) 30.

134. Data Protection Directive, *supra* note 5, at art. 26.3.

135. Council Doc. 7500/94, COREPER Report to the Internal Market Council 10 (June 9, 1994); Council Doc. 9951/94, Working Document of Secretary General of the Council to the attention of the delegations, 43–44 (Oct. 12, 1994); Council Doc. 9957/94, *supra* note 101; Council Doc. 10957/94, *supra* note 129.

136. *See* the remarks of Irish delegation on lack of a common "legal philosophy" in Résultats des travaux du Groupe des "Questions économiques" (Protection des données) en date du 25 février 1991 [Results of the Working Party on Economic Questions (Data Protection) dating from Feb. 25, 1991], Doc. No. 5207/91, Restreint ECO 32, at 6 (Mar. 14, 1991) (on file with author).

137. As late as October 1993, three years after the first Commission proposal was introduced, Denmark, Ireland, the Netherlands, and the UK continued to object to a Data Protection Directive and preferred the less detailed Council of Europe Convention. *See* Extrait du Projet de Compte Rendu Sommaire de la 1582ème réunion du Comité des Représentants Permanents (1ère partie) tenue à Bruxelles le jeudi 14 octobre 1993, Point 11 de l'ordre du jour [Excerpt from the Summary Draft Minutes of the 1582nd Meeting of the Committee of Permanent Representatives (Part I) Held in Brussels on Thursday, Oct. 14, 1993, Point 11 in

Member States, opposed a number of vital aspects of the Directive: the inclusion of manual data in the definition of personal data,[138] notification of data processing operations,[139] authorization for sensitive personal information,[140] the broad definition of sensitive personal information,[141] the procedure for third country transfers,[142] the type of information to be provided to citizens on how their personal information was being used,[143] and the prohibition on decisions based exclusively on automatic data processing.[144] Throughout, the northern bloc criticized the Directive as bureaucratic, burdensome, and impractical.[145] In the end, in fact, the UK abstained from the final vote in the Council to express its opposition to

---

the Order of the Day], Doc. No. 9186/93, Ext 1, Restreint, CRS/CRP 34 ECO 248, (Oct. 21, 1993) (on file with author).

138. *See, e.g.*, Résultats des travaux du Group "Questions économiques" (Protection des données) en dates des 5/6 octobre 1992 [Results of the Working Party on Economic Questions (Data Protection) dating from Oct. 5–6, 1992], Doc. No. 9388/92, Restreint ECO 220, at 6 n.16 (Oct. 20, 1992) (Ireland, Spain, Portugal, and the UK objecting to the inclusion of manual data in the definition of personal data) (on file with author).

139. *See, e.g.*, Résultats des travaux du Groupe des "Questions économiques" (Protection des données) en date du 20 et 21 fevrier 1992 [Results of the Working Party on Economic Questions (Data Protection) dating from Feb. 20–21, 1992], Doc. No. 4981/92, Restreint ECO 33, at 3–5 (May 9, 1992) (UK, Ireland, the Netherlands and Denmark objecting to notification) (on file with author).

140. *See, e.g.*, Résultats des travaux du Groupe des "Questions économiques" (Protection des données) en date du 19 March 1992 [Results of the Working Party on Economic Questions (Data Protection) dating from Mar. 19, 1992], Doc. No. 5490/92 ECO 50 (Apr. 7, 1992) (on file with author) (Germany, the Netherlands, the UK, and Ireland objecting to authorization).

141. *See, e.g.*, Résultats des travaux du Groupe des "Questions économiques" (Protection des données) en date du 29 octobre 1992 [Results of the Working Party on Economic Questions (Data Protection) dating from Oct. 29, 1992], Doc. No. 9918/92 Restreint ECO 246, at 2 (Nov. 11, 1992) (on file with author) (the UK objecting to definition of sensitive data); Note from the President dated 10 May 1994 to Permanent Representatives Committee, Doc. No. 6856/94, Restreint ECO 1030, at 10 (May 18, 1994) (on file with author) (Germany, the Netherlands, Denmark, Ireland, the UK, Portugal, and Greece opposing an exhaustive list of sensitive data because of different national laws).

142. *See* Council Doc. 7500/94, *supra* note 135 (UK, Denmark, Ireland, and Sweden objecting).

143. *See* Note from the President dated May 10, 1994 to Permanent Representatives Committee, Doc. No. 6856/94, Restreint ECO 1030, at 15 (May 18, 1994) (on file with author) (Germany, Denmark, Ireland, the Netherlands, and the UK objecting to the list of information to be given to the data subject).

144. *See, e.g.*, Résultats des Travaux du Groupe des questions économiques (Protection des données) en date du 29 et 30 mai 1994 [Results of the Working Party on Economic Questions (Data Protection) dating from May 29–30, 1994], Doc. No. 7993/94, at 5 (June 23, 1994) (on file with author) (Denmark, Ireland, and the UK objecting to inclusion of article on automatic data processing).

145. *See, e.g.*, Council Doc. 9957/94, *supra* note 101. (Denmark, Ireland, the UK, supported by Finland, Norway, and Sweden objecting to notification because it was too "bureaucratic").

the Directive.[146] On the other side of all these issues was a bloc consisting of France, Italy, Belgium, Spain, and Luxembourg. The result was that the final version of the Directive included principles such as authorization but such principles allowed for so many exceptions that Member States could sidestep them entirely in their implementation of the Directive.

One puzzle of this history is that notwithstanding the radical differences separating the Member States, at no point did either camp use the possibility of bargaining and linkages with other policy domains to prevail. On neither side were preferences strong enough to push through one vision of privacy rights or the other. One explanation might be that privacy rights often come into conflict with government surveillance and other public initiatives. Therefore, even governments with extensive privacy regimes at home might not have had a strong interest once in Brussels in creating a tough Europe-wide privacy scheme.

A third type of evidence in the bargaining history supports the credible commitment hypothesis. From the Council record, it appears that the common interest that was shared by the Member States—free trade—did not require extensive harmonization of national privacy laws through the Directive. The national representatives in the Council did not express significant concern that the free circulation of personal information, vital to commerce in the common market, would be hindered by disparate regulatory regimes. A word of explanation is necessary because this claim goes contrary to the common wisdom regarding the Directive.[147] The Directive was passed as a common market measure, meaning that it was based on the powers of the European Community under Article 95 (ex-Article 100A) of the EC Treaty to harmonize national legislation that impedes the functioning of the common market.[148] The case for a Directive, however, rested heavily on the failure of a number of Member States to ratify the Council of Europe Convention, which contains a series of very general standards for the storage, use, and transfer of electronic personal information.[149] In 1981, immediately after the Convention had been signed, the Commission called upon the Member States to ratify it, adding that "if all the Member States do not within a reasonable time sign and ratify the Convention, the Commission reserves

146. Draft Minutes of the 1827th meeting of the Council (General Affairs) held in Brussels on Monday, 6 February 1995, Doc. No. 4734/1/95 REV1 Limite PV/CONS 4, at 9 (Jan, 19, 1996) (on file with author).

147. *See, e.g.*, Patrick J. Murray, *The Adequacy Standard Under Directive 95/46/EC: Does US Data Protection Meet This Standard?*, 21 FORDHAM INT'L L.J. 932, 935–38 (1998).

148. *See* Data Protection Directive, *supra* note 5, at preamble. The Directive was passed before the EC Treaty was renumbered by the Amsterdam Treaty of 1997 and therefore at the time its legal basis was article 100A.

149. *See* Communication on the Protection of Individuals, *supra* note 36, at 15.

the right to propose that the Council adopt an instrument on the basis of the EEC Treaty."[150] Nearly ten years later, two of the original Member States—Italy and Belgium—still did not have privacy legislation, and the three Member States that had since joined—Greece, Spain, and Portugal—had not adopted privacy legislation.[151] It appears, therefore, that when the Commission and the Member States began negotiations they agreed on the need to put into place some form of domestic privacy legislation, but not on the need for a single, harmonized set of national laws.

Another piece of the historical record that suggests that free trade was not the primary concern underlying the harmonization provisions in the Directive was the dispute over legal basis. Member States were divided over whether ex-Article 100A was the appropriate legal basis for the Directive or whether, as a human rights measure, the Directive fell under the general purpose provision of the EC Treaty, ex-Article 235.[152] (Ex-Article 235, now Article 308, is similar in purpose and effect to the U.S. Constitution's Necessary and Proper Clause.) This dispute suggests that a number of Member States did not believe that the primary intent or effect of the Directive was to facilitate trade.[153] Finally, even though information privacy was not a new policy area and national laws had existed for two decades, in remarkably few instances had national authorities taken action to stop transfers to other European countries.[154]

---

150. *Id.* at 14.

151. *Id.*

152. Doc. No. 5207/91, Restreint ECO 32, *supra* note 136 (Ireland, Belgium and the UK objecting to legal basis); Letter from Permanent Representative of Belgium to the CE, to N. Ersboll, the Secretary General of the Council of CE (Feb. or Mar. 2001) (questioning whether the Community has competence to legislate in this area given that it is a matter of human rights covered in Art. 8, ECHR and Convention 108, and requesting an opinion from Legal Services of the Council); Doc No. 9388/92, Restreint ECO 220, *supra* note 138 (Germany and Belgium objecting to legal basis of Directive); Résultats des travaux du Groupe des "Questions économiques" (Protection des données) en date du 19 et 20 juin 1991 [Results of the Working Party on Economic Questions (Data Protection) dating from June 19–20, 1991] Doc. No.7284/91, Restreint ECO 93 (July 19,1991) (on file with author) (delivering opinion of Council's Legal Service on the appropriate legal basis for the Directive).

153. Of course, disputes over the legal basis for European measures are often thinly veiled disputes over the desirability of the measure. Measures adopted under ex-Article 100A can be adopted by qualified majority, whereas measures adopted under ex-Article 235 require unanimity. Nevertheless, it is significant that the legal basis argument was made on the record: national representatives could credibly claim that the Directive was primarily about human rights and not trade.

154. A literature search turns up three episodes. First, France had blocked a data transfer to Italy. Fiat-France wished to transfer employee information to Fiat headquarters in Italy but the transfer was blocked by the French privacy authority (CNIL). According to CNIL, the personal information of Fiat's French employees would not be protected adequately once transferred to Italy because, at the time, Italy did not have a data protection law. Only after Fiat-France and Fiat-Italy had signed a contract in which Fiat-Italy undertook to respect the

Indeed the three salient episodes in the literature all involved transfers to countries without any information privacy legislation, not countries with inadequate legislation.[155]

The last category of evidence in the Council record for the credible commitment explanation is the link between opposition to European institutions and a strong national position on information privacy. The minutes from the Council indicate that France was the main proponent of eliminating the Commission's implementing powers.[156] France is a country with a long-standing tradition of privacy as a basic liberty and with an extensive government regulatory scheme. Although hardly dispositive, France's opposition is consistent with the credible commitment hypothesis. One plausible reason for why France opposed conferring powers to a European privacy network was that the French regulation of privacy was at odds with the approach elsewhere.

The other Member State with a strong view on privacy—on the opposite end of the policy spectrum from France—was also a vocal opponent of transferring administrative authority to European institutions. At the eleventh hour, the UK requested further negotiations with the European Parliament because it believed that the comitology committee's powers over the Commission were not substantial enough. In response to a parliamentary amendment, the Commission had reduced the powers of the comitology committee in the final version of the Directive.[157] However, the other Member States did not wish to compromise their legislative deal over the comitology issue and they approved the Directive as it stood. The UK's resistance on the institutional issue is significant. UK preferences on the substance of privacy policy were diametrically opposed to those of France, but its preferences on procedure were similar. Unlike France, the UK was skeptical of information privacy and believed that other values, such as freedom of the press and effective administration, were more important. Like France, the UK opposed transferring powers to an institutional process that could

French law on privacy, did CNIL permit the transfer. *See* Paul M. Schwartz, *European Data Protection Law and Restrictions on International Data Flows*, 80 IOWA L. REV. 471, 491–92 (1995). The other two episodes involve transfers of data from Sweden to the UK. In the first, the Swedish Data Inspection Board refused to grant a license to public authorities seeking to transfer health data on the Swedish population to the UK for the manufacture of plastic health cards. In the second case, the Data Inspection Board denied a license to an exporter seeking to transfer the information to the UK for the production of a catalogue. *See* Jon Bing, *Transnational Data Flows and the Scandinavian Data Protection Legislation*, 24 SCANDINAVIAN STUD. L. 65 (1980).

155. *See* Schwartz *supra* note 154; Bing, *supra* note 154.

156. Council Doc. 11369/94, *supra* note 131.

157. *See supra* notes 118–120 and accompanying text.

be taken over by supranational and national regulators with very different policy commitments.

In summary, Member States resisted giving the European privacy network extensive powers because of their disagreement on the substance of information privacy policy. As a result, primary responsibility for interpreting and enforcing the Data Protection Directive rests with national administrations, not European institutions. Member States simply did not trust the Commission, acting with other Member States, to protect privacy rights and to strike the correct balance between civil liberties and the information needs of government and the market.

Even though European networks generate regulatory convergence, their very formation presupposes a certain degree of consensus among governments. Therefore, to explain the emergence of this form of European governance, it is not enough to analyze what might be accomplished through the creation of networks. Rather, it is necessary to examine the broader economic, social, and political dynamics that lead to common national preferences in the first place or that enable some government officials to induce other officials, through bargaining, to adopt their preferences.

B. *Implications for Transgovernmental Networks*

Inferences may be drawn for transgovernmental networks in other regional organizations and the international realm. The experience of the European privacy network suggests that the rise of transnational networks is as much an indicator of convergence as it is a generator of convergence. In other words, even though we might observe that transnational networks cause information exchange and regulatory convergence, the mere desire for such exchange and convergence does not cause the networks. This form of governance rests upon a deeper consensus among the participating officials on the desirability of certain public policies; alternatively, networks are created when certain participating governments can gain advantages from adopting the regulatory approach of other governments, advantages such as attracting investor capital.

It is important to take care in generalizing from European to transnational networks. The credible commitment and loss of national control associated with transnational networks, even those created by international agreement, is not nearly as significant as that which characterizes European networks.[158] The reason for this difference is the power of the European Commission, backed up by the European Courts and the European judicial system. In European networks, national governments

158. SLAUGHTER, *supra* note 9, at 153–54.

retain extensive powers, but when disputes arise among them or among Commission officials and national regulators, the Commission has the legal authority to step in. Nevertheless, to participate in a transnational network is to cede some degree of control over domestic policymaking. Regulators give other national regulators the power to examine and criticize their domestic laws and administrative practices. This transfer of power carries potentially significant costs in the form of loss of reputation in global markets and in dealings with other States in the international realm. Before they tie their hands through networks, government officials must reach some agreement on the policies to be pursued by the networks.

IV. EVALUATING NETWORKS

How does network governance fare when matched against principles of liberal democracy? To what extent are the individual rights and democratic accountability guaranteed by the administrative law of liberal democracy protected when regulators share their powers with other national regulators? This section assesses the European privacy network from the perspective of Italian liberal democracy. The question of whether the mixed procedure for international data transfers respects these basic values is divided into two parts.[159] First, I examine the sequence of decisions anticipated in the text of the Directive and I determine whether this sequences affords individuals the traditional guarantees of Italian administrative law. Second, I repeat the normative exercise for the actual administrative practice of international data transfers, which departs significantly from the text of the Directive. The section concludes by suggesting some implications for networks in the global realm.

A. *The Law of the European Privacy Network: The Italian Case*

The Data Protection Directive and the Italian implementing legislation envision a complex sequence of decisions by national and supranational regulators before personal information may be transferred outside the European Union. The interaction of the two legal frameworks is set forth below, organized under each of the Directive's two provisions on third country transfers, Articles 25 and 26. In both cases, the decisionmaking occurs in three stages, the first and last being made at the

159. For purposes of this section, democratic accountability is defined as the link between bureaucrats and elected officials, voters, and the general public.

domestic level, the middle stage at the European level. The statutory provisions that authorize regulators to act at each stage are provided in the citations.

Initial Domestic Administrative Action	European Review	Domestic Implementation of EU Decision
Article 25 (Transfer to adequate third countries)		
An administrative decision to block a particular data transfer or enjoin future data transfers based on a finding that the third country is inadequate. Technically, this would be issued as an order (*provvedimento*) of the Garante.[160]	Commission negotiations with the third country found "inadequate" by the Garante leads to a change in the country's privacy regime and the Commission acting in conjunction with the working party and comitology committee issues a decision finding that the country is "adequate."[161]	The Garante gives effect to the Commission decision with a general authorization (*autorizzazione generale*) allowing transfers to the third country to which transfers previously prohibited.[162]
Initial Domestic Administrative Action	European Review	Domestic Implementation of EU Decision
Article 26 (Exceptions to adequacy principle)		
An administrative decision to authorize a data transfer based on a finding that the particulars of the transaction will guarantee privacy, regardless of the adequacy of the third country's privacy laws. This would be issued by the Garante as an individual authorization (*autorizzazione*).[163] An administrative rule authorizing certain types of transfers, regardless of the adequacy of the third country's privacy laws. This would issued by the Garante as a general authorization (*autorizzazione generale*).[164]	Commission, acting in conjunction with the comitology committee, issues a decision finding that the safeguards deemed by the Garante to guarantee privacy are not protective enough.[165]	The Garante gives effect to the Commission decision by revoking the specific authorization (*autorizzazione*) permitting a third country transfer or the general authorization (*autorizzazione generale*) permitting a class of transfers.[166]

160. Decreto Legislativo 30 giugno 2003 n. 196, Codice in materia di protezione dei dati personali [Decree-Law No. 196 of June 30, 2003, Personal Data Protection Code], art. 154, Gazz. Uff., no. 174 (July 29, 2003) (Italy).

161. Data Protection Directive, *supra* note 5, at art. 25.6.

162. Decree-Law No. 196 of June 30, 2003, Personal Data Protection Code, at art. 44.

163. *Id.* at art. 44.

164. *Id.*

165. Data Protection Directive, *supra* note 5, at art. 26.3.

166. Personal Data Protection Code, at art. 44.

Italian and European administrative law principles, applied by Italian and European administrative bodies and courts to this procedure, appear to guarantee individual rights fairly effectively. For present purposes, individual rights are defined as the opportunity to participate in administrative determinations and the ability to challenge such determinations in an independent judicial forum. Generally speaking, a strong right to participate in administrative decisionmaking does not exist in *droit administratif* systems.[167] Rather, individual rights are protected through the availability of review in an independent forum, which in countries like France and Italy is a separate branch of government administration and is not part of the ordinary judicial system.[168] In Italy, however, decisionmaking by government administration has become increasingly proceduralized over the past decade. A law passed in 1990 guarantees, in addition to review in an independent forum, the right of participation in administrative adjudications: affected individuals have a right to examine the administrative record, submit written arguments and evidence, and receive a decision in writing which gives reasons and shows that their position was considered.[169]

The Garante adheres to the requirements of the 1990 law.[170] Therefore, a firm that opposed a proposed order blocking an international data transfer (first type of administrative action) or an individual who opposed a proposed order allowing such a transfer (second type of administrative action) would have the opportunity to persuade the Garante otherwise in an administrative proceeding. Even in rulemaking, which in Italian and continental law more generally is considered a matter of discretionary policymaking and does not give rise to legal rights of individual participation, the Garante has a reputation for consulting the community of interested parties. Therefore, a firm or individual with opinions on a rule permitting a certain class of transfers (third type of administrative action) would probably be heard, albeit in a very loose sense of the word.

If the Garante's determination triggers review by the Commission and a comitology committee—the European phase of the administrative proceeding—individual participation would be guaranteed only if the European determination turned on the particular facts of an individual

167. On the traditional approach, see Giacinto della Cananea, *Beyond the State: The Europeanization and Globalization of Procedural Administrative Law*, 9 EUR. PUB. L. 563, 566 (2003).

168. *See* L. NEVILLE BROWN & JOHN S. BELL, FRENCH ADMINISTRATIVE LAW 213–50 (5th ed. 1998); MANUALE DI DIRITTO PUBBLICO 434–46 (Sabino Cassese et al. eds., 2001).

169. Legge 7 agosto 1990 n. 241 [Law No. 241 of Aug. 7, 1990], Gazz. Uff. no. 192 (Aug. 18, 1990) (Italy). *See* Sandulli, *supra* note 94, at 1035, 1057–59.

170. *See* Regolamento 28 giugno 2000 n. 1 [Regulation No. 1 of June 28, 2000], Gazz. Uff. no. 162 (July 13, 2000) (Italy).

data transfer.[171] This would occur most likely if the Garante had approved a foreign transfer based on a contract submitted by an individual firm (second type of administrative action). Otherwise, neither the Data Protection Directive nor the general background law governing comitology require that individuals be allowed to make submissions or argue their case before the Commission and the committee.[172] Thus, if an Italian determination involving a general assessment of a third country's adequacy (first type of administrative action) or a model contract (third type of administrative action) were then submitted to Europe-wide review, individuals would not have a right to participate. In the abstract, this might be objectionable. But if the benchmark is the state of affairs at the national level in the absence of mixed procedure, the lack of participation is not cause for concern. As discussed earlier, a strong right of participation in administrative proceedings does not exist in Italy, especially in what is considered discretionary policymaking. Discretionary policymaking is the vast majority of what European institutions do in the international privacy arena.

Neither does the particular sequence of administration decisions anticipated in the Data Protection Directive appear to compromise access to judicial review. Although Italy does not yet have actual experience with challenges to administrative determinations under these provisions, it is clear that judicial review would be available under standard principles of Italian administrative law.[173] Assume for the moment that the Garante's decision does not trigger a comitology proceeding. If the decision were of the first or second type, judicial review would be easy to obtain. The Italian concept of "legitimate interest" (*interesse legittimo*), which serves as a functional equivalent of standing in U.S. law would include the financial interest of a data-exporting firm in challenging a

171. *See* Case C-269/90, Hauptzollamt München-Mitte v. Technische Universität München, 1991 E.C.R. I-5469.

172. *See* Council Decision 1999/468/EC of 28 June 1999 Laying Down the Procedures for the Exercise of Implementing Powers Conferred on the Commission, 1999 O.J. (L 184) 23 [hereinafter Comitology Decision].

173. The Italian data protection legislation modifies background Italian administrative law by specifying that all challenges to the Garante's decisions, regardless of whether they involve "subjective rights" or "legitimate interests" are to be brought in the civil courts. Decreto Legislativo 30 giugno 2003 n. 196, Codice in materia di protezione dei dati personali [Decree-Law No. 196 of June 30, 2003, Personal Data Protection Code], art. 152, Gazz. Uff., no. 174 (July 29, 2003) (Italy). Both "legitimate interests" and "subjective rights" serve as the functional equivalent of standing in U.S. law. The difference is that a "legitimate interest" must be vindicated in a specialized administrative court, while a "subjective right" must be vindicated in an ordinary civil court. The Italian data protection law therefore improves the availability of judicial review by avoiding the time-consuming process of deciding in which court—civil or administrative—to bring a suit. Furthermore, the civil courts are generally believed to be less deferential to the government than administrative courts and hence individual rights should be better protected under this scheme.

prohibition on an international transfer.[174] Likewise, an individual seeking to challenge an authorization allowing the transfer of her personal information would be found, in all likelihood, to have the "subjective right" (*diritto soggettivo*) necessary to do so. Under Italian administrative law, such a right exists because privacy rights are considered fundamental and the breach of privacy rights can lead to material injury and emotional distress.[175]

If the decision were a rule allowing a class of information transfers, it would be more difficult to obtain judicial review (third type of administrative action). In Italian law, individuals generally are not believed to have interests that can be adversely affected by administrative rulemaking and vindicated through judicial review.[176] Potential challengers would have to wait until the rule was applied to a specific case, for example if the Garante denied, based on a general authorization, an individual petition seeking to block an international transfer.

Now assume that the Garante's decision triggers a European proceeding which results in an opposite determination. That is, the Italian authorities prohibit data transfers to a third country but, after negotiations by the Commission, that third country is found to be adequate. The Garante, therefore, must issue a general authorization implementing the European decision and permitting such transfers (first type of administrative action). Or the Garante authorizes transfers to "inadequate" third countries, which on review by the Commission and comitology committee are found to lack adequate privacy safeguards. The Garante,

174. In the early history of Italian administrative law, only "subjective rights," rights guaranteed under the Civil Code, were protected against state action. Individuals could bring suits against government in ordinary civil courts and obtain damages for claims which, to translate into the common law, sounded in property, contract, or tort. In 1889, the Council of State (*Consiglio di Stato*) was given the power to review government acts for lawfulness. Today, individuals can bring challenges to administrative acts, even if they have not suffered an injury to their person or property that is recognized under the Civil Code. The remedy is not damages but an order annulling the administrative act. Nonetheless, an individual seeking to challenge such an act still needs a "legitimate interest" in the procedural and substantive regularity of the act. The example often used to illustrate the concept is a civil service exam which was not administered according to the letter of the law. The applicants do not have a subjective right in being employed by the state, but they do have a legitimate interest in ensuring that the exam was administered fairly. *See* Marcello Clarich, *La Giustizia*, *in* 2 TRATTATO DI DIRITTO AMMINISTRATIVO, *supra* note 94, at 2021, 2055–58, 2069–73.

175. *See* Giorgio Resta, *Il diritto alla protezione dei dati personali*, *in* IL CODICE DEI DATI PERSONALI: TEMI E PROBLEMI *supra*, note 89 (stating that data protection is considered a fundamental rights and thus receives all the judicial guarantees generally afforded to fundamental rights); Salvatore Sica, *Le tutele civili*, *in* IL CODICE DEI DATI PERSONALI: TEMI E PROBLEMI, *supra*, note 89 (describing tort liability for infringement of privacy rights).

176. Jacques Ziller, *Le contrôle du pouvoir réglementaire en Europe*, 9 L'ACTUALITÉ JURIDIQUE DROIT ADMINISTRATIF 635, 642 (1999).

therefore, is required to revoke the individual or general authorization (second and third type of administrative action).

In the second type of proceeding, in which an initial Italian determination favorable to a particular individual is reversed by the Commission, either the Commission's decision would be amenable to review in the Court of Justice or the Garante's implementing decision could be challenged in the Italian courts. One case involving such a proceeding, in which the distribution of agricultural subsidies was at issue, demonstrated some confusion as to which court—an Italian court or the European Court of Justice—was responsible for hearing the challenge to the decision. The Italian court held that the challenge should be brought in the Court of Justice. The Court of Justice ruled that the matter was for Italian courts and possibly the Court of Justice through a preliminary reference from an Italian court. Thus the Court of Justice directed the plaintiffs to bring their action below.[177] A growing body of Court of Justice case law, however, is setting down the criteria for dividing jurisdiction over such administrative proceedings.[178] Any shortcomings, therefore, in access to judicial review can be put down to the growing pains of a new European polity rather than the particularities of network governance.

Otherwise, in the first and third types of proceedings, the Commission's reversal would not be amenable to review immediately but at a later stage, when applied by the Garante to permit or prohibit a specific third country transfer. That is because the Commission's decision to permit transfers to an "adequate" third country or to stop certain types of transfers whose terms fail to protect privacy are general determinations. Neither European nor Italian law permits such general rules to be challenged in the abstract; an individual would have to wait until the rule was applied to her case.[179] Later on, an individual who disputed the Commission's finding and considered that her personal information was being transferred to an inadequate third country could object in Italian court (first type of proceeding). Likewise, a corporation that sought to transfer personal information abroad using a standard-form contract that had

177. Case C-97/91, Oleificio Borelli SpA v. Commission, 1992 E.C.R. I-6313. *See* della Cananea, *supra* note 53 (manuscript at 201, on file with author) (discussing the Borelli case).

178. This is the Court's case law on whether a decision is of "direct" concern to an individual and therefore is reviewable in the Court of Justice. *See* CRAIG & DE BÚRCA, *supra* note 6, at 518.

179. *See* CRAIG & DE BÚRCA, *supra* note 6, at 486–503 (stating that parties must be "individually concerned" by European acts to have standing before the European Court of Justice); Bernardo Giorgio Mattarella, *L'Attività*, *in* 1 TRATTATO DI DIRITTO AMMINISTRATIVO: DIRITTO AMMINISTRATIVO GENERALE 699, 753 (Sabino Cassese ed., 2003) (stating that, under Italian law, broadly applicable administrative acts such as general authorizations and rules can only be challenged when applied in concrete cases).

been vetoed by the Commission could go to Italian court to challenge the Commission's veto (third type of proceeding).[180]

On balance, it does not appear that this novel administrative structure, based on a sequence of decisions made by different national and supranational officials, prevents individuals from seeking review of administrative decisions in the courts. Although to a French or American jurist the Italian law on access to judicial review might appear quite restrictive, the fact remains that administrative decisions may be challenged regardless of whether European regulators intervene or the Garante acts alone.[181] Likewise, the intensity of judicial review, that is how carefully administrative decisions are scrutinized on substantive grounds such as lawfulness and reasonableness does not appear to suffer. Italian courts and the European Court of Justice employ similar grounds of judicial review and give similar deference to administration. Therefore, the partial transfer of judicial review powers to the Court of Justice, implicit in the preliminary reference procedure, does not lower standards of judicial review.[182]

The European privacy network also satisfies the conventional administrative law principle of transparency. Transparency signifies the right to know which bureaucrats decide what—part of the basic rule of law guarantee that citizens are to be governed by laws and the principled application of laws, not men. Transparency also means the right to learn of the considerations and documents that inform final administrative decisions.

Mixed procedure in the Data Protection Directive and myriad other European laws represents a codification of regulatory networks; such networks have always assisted in the implementation of European law but, in the past, they often existed on an informal basis. Two elements of the network are codified: the vertical relationship between national regulators and other national regulators and the Commission and the horizontal relationship between national regulators sitting on European

180. *See generally* TREVOR C. HARTLEY, EUROPEAN UNION LAW IN A GLOBAL CONTEXT: TEXT, CASES, AND MATERIALS 361–62 (2004) (discussing circumstances under which measures are not of "direct concern" and thus must be challenged in national court, not the European Courts).

181. For a comparison of the more liberal standing rules for challenging regulations in France as compared to Italy, see Ziller, *supra* note 176, at 640 (1999).

182. Both the Italian courts and the European Court of Justice recognize that government officials should enjoy significant discretion in reaching administrative decisions. In Italy, deference to discretionary government decisions is particularly strong on technical matters. *See* François Lafarge, *Le contrôle des décisions de l'administration en Italie*, 9 L'ACTUALITÉ JURIDIQUE DROIT ADMINISTRATIF, 678, 685 (1999). The Court of Justice, likewise, allows the Commission a significant "margin of evaluation" (*marge d'appréciation*) on both policy and scientific matters and will only annul a decision if there is a "manifest error of evaluation" (*erreur manifest d'appréciation*). *See* CRAIG & DE BÚRCA, *supra* note 6, at 537–39.

committees and the Commission. This shift from informal practice to law, by definition, is good for transparency. By virtue of codification, European citizens know that networks, not their national government officials acting alone, are responsible for the application and enforcement of European laws. In addition, the parties to administrative proceedings like the decision to allow or block international data transfers know the sequence of national and supranational decisions to expect before a determination will become final.

Further, in mixed procedure, regulators are under a duty to notify the parties of the many decisions that are made in the course of the proceeding, and they must give access to some of the background documents that inform those decisions. The Italian Data Protection Code combined with background principles of Italian public law require that the Garante notify all parties named in blocking or authorizing orders (first and second types of administrative action) and that the Garante publish all general authorizations (third type of administrative action) in the Italian equivalent of the U.S. Federal Register (*Gazzetta Ufficiale*).[183] If the matter is reviewed by European officials, the outcome is published in the Official Journal of the European Union. Moreover, some of the background documents that informed the European phase of the proceeding would be available under the European access to documents law.[184] And, if the Garante's decision were reversed on the grounds that a country offered adequate privacy guarantees (first type of administrative proceeding) or a standard contract failed to guarantee adequately privacy (third type of administrative proceeding), the Garante would promulgate an Italian rule that would be published in the *Gazzetta Ufficiale*.[185] If a specific applicant were prohibited from transferring personal information

183. *See* Bernardo Giorgio Mattarella, *Il Provvedimento*, *in* 1 TRATTATO DI DIRITTO AMMINISTRATIVO, *supra* note 179, at 797, 879–80.

184. *See* Council and Eur. Parl. Regulation 1049/2001/EC of 30 May 2001 Regarding Public Access to European Parliament, Council and Commission Documents, 2001 O.J. (L 145) 43 [hereinafter Access to Documents Law]; Comitology Decision, *supra* note 172, at arts. 7–8.

185. The formal transposition of Commission adequacy decisions into national law is uncommon among Member States. Under general principles of EU law, decisions are directly binding and therefore, formally speaking, it is not necessary to incorporate them into national law. Consequently, French, German, and British regulators do not adopt national implementing decisions; they assume that all members of the interested community keep abreast of Commission decisions. *See* Interview with André Albert, Magistrat au Bureau du Droit Civil Général, Ministère de Justice [Magistrate in the General Civil Law Bureau, Ministry of Justice] in Paris, Fr. (Oct. 21, 2002); Interview with Dr. Alexander Dix, Data Protection Commissioner for the Land of Brandenburg in Potsdam, Germany (July 7, 2003); Interview with David Smith, Assistant Commissioner, Information Commissioner's Office in Wilmslow, UK (Feb. 27, 2003). While this assumption might be perfectly valid, it appears that the Garante's practice is especially protective of the public's right to know, in particular those members of the public who are not aficionados of EU law or the EU system of government.

as a result of an adverse European determination (second type of administrative proceeding) the Garante, again, would issue an order reversing the previous Italian decision and notify the party.

Nothing in this sequence of national and European decisions compromises the Italian right to transparency. Indeed, in the European phase of the proceeding, Italian citizens gain greater insight into the determination than they would have if the privacy matter were handled by Italian regulators alone because the European access to documents law is more comprehensive than the equivalent Italian law.[186]

On accountability to elected officials and the general public, by contrast, the European privacy network is weak. For example, a trade union might be unhappy with the experience of transfers of employee data abroad because it believes that employers use such transfers to circumvent Italian labor laws and discriminate against employees. To which elected official does the trade union complain? As a first step, the trade union must ask Italian parliamentarians and members of government to pressure the Garante to ban such transfers. A broader assault, however, is also necessary because of the power of other national regulators and the Commission to reverse the Garante's decision. The Italian trade union, therefore, might decide to lobby hostile national governments and the European Commission through the European Trade Union Congress. Or it might put pressure on elected representatives in other national parliaments and the European Parliament to encourage their regulators to support the Garante's position. In a system of government in which powers are shared among multiple regulators, citizens must be able to mobilize in the diverse political worlds in which such regulators operate. Yet, as is commonly acknowledged by scholars and policymakers alike, this form of pan-European political action is far more resource-intensive than public campaigns at the national level alone.[187] Furthermore,

186. *Compare* Access to Documents Law, *supra* note 184, *with* Legge 8 guigno 1990 n. 142 [Law No. 142 of June 8, 1990], Gazz. Uff. no. 135 (June 12, 1990) (Italy). For a discussion of the Italian system, see PIERGIORGIO ALBERTI ET AL., PROCEDIMENTO AMMINISTRATIVO E DIRITTO DI ACCESSO AI DOCUMENTI: LEGGE 7 AGOSTO 1990, N. 241 E REGOLAMENTI DI ATTUAZIONE 535–69 (2d ed. 1995).

187. On the difficulties faced by conventional business and labor groups in mounting Europe-wide campaigns, see MICHAEL J. GORGES, EURO-CORPORATISM: INTEREST INTERMEDIATION IN THE EUROPEAN COMMUNITY 10 (1996). *See also* Alasdair R. Young, *Consumption Without Representation? Consumers in the Single Market in* PARTICIPATION AND POLICY MAKING IN THE EUROPEAN UNION 206, 220–25 (Helen Wallace & Alasdair R. Young eds., 1997) (describing difficulties faced by consumer movement). For a discussion of the difficulties encountered in the United States by "diffuse, unorganized groups" in organizing at the federal as opposed to state levels, see Matthew D. Adler & Seth F. Kreimer, The *New Etiquette of Federalism: New York, Printz, and Yeskey*, 1998 SUP. CT. REV. 71, 81 (1998); THEDA SKOCPOL, DIMINISHED DEMOCRACY: FROM MEMBERSHIP TO MANAGEMENT IN AMERICAN CIVIC LIFE 283 (2003).

Europe-wide political action on an issue like the right to privacy rests on a European identity that enables citizens, regardless of their nationality, to conceive of privacy as a commonly shared interest that warrants mobilization in Europe's many national arenas and at the supranational level. Again, however, scholars and policymakers recognize that such an identity does not exist yet in the European Union.[188] The hypothetical Italian trade union faces a stiff battle.

B. *The Administrative Practice of the European Privacy Network*

The reality of European regulation of international data transfers alters significantly the normative assessment of individual rights and democratic accountability. The law of the European privacy network set down in the Data Protection Directive anticipates an orderly succession of administrative decisions: the Garante issues an initial decision, which is reviewed by the Commission and comitology committee and results in another decision, which depending on the outcome is followed by a final Italian implementing act.[189] This procedure has proven to be pure fiction. The record does not contain a single episode of this kind. Rather, on international data transfers, the Italian approach like that of most other national privacy authorities has been to wait and see. The Garante has not used its powers to block or authorize data transfers. This is to the detriment of both individual citizens, whose privacy rights are not protected when their information is sent abroad, and commercial and public entities, which operate under conditions of legal uncertainty.[190] In the language of American administrative law, the Garante has failed to act.[191]

Action, instead, has come from European institutions, and it has come in two forms. First, the working party of national privacy authorities has developed common criteria for evaluating third country adequacy and standard data transfer contracts. These common criteria

188. *See* JOSEPH H. H. WEILER, *To Be a European Citizen: Eros and Civilization*, *in* THE CONSTITUTION OF EUROPE 324, 336–56 (1999). *See also* Andrew Scott, *Analysing the Democratic Deficit—Methodological Priors: A Comment on Moravcsik*, *in* INTEGRATION IN AN EXPANDING EUROPEAN UNION: REASSESSING THE FUNDAMENTALS 99, 101 (J.H.H. Weiler et al. eds., 2003).

189. *See supra* notes 159–166.

190. *See generally* Interview with Susannah Haan, Legal Adviser, Company Affairs, Data Protection Working Group, Confederation of British Industry in London, UK (Feb. 28, 2003) (describing difficulties of legal uncertainty for British firms and ascribing such uncertainty to the lack of administrative action on international data transfers).

191. *See generally* RICHARD J. PIERCE, JR., 3 ADMINISTRATIVE LAW TREATISE 1270 (4th ed. 2002).

are informal, taking the form of opinions[192] and working documents.[193] Second, as described earlier, the Commission has issued formal decisions finding foreign privacy laws adequate and approving model contracts for international data transfers.[194] Yet according to certain members of the private sector, formal action by the Commission has come too slowly.[195]

Inaction and informal action are both problematic in administrative law. Neither is susceptible to judicial review. In the face of inaction, courts are reluctant to dictate a particular course of action for an agency because they are aware of their institutional limits. By definition, informal action is difficult to discern. Even when it is identifiable, courts are reluctant to deprive agencies of this flexible mode of action by requiring agencies to meet ordinary standards of judicial review. In Italian administrative law, wariness of interfering with administration in such instances is expressed through the central legal concept of the "administrative act" (*atto* or *provvedimento*), defined as a formal decision binding on individuals outside the agency.[196] Judicial review is available only once an administrative act is promulgated, meaning that neither inaction nor informal action may be challenged in court. Indeed, the legal concept of an administrative act is so important that if the legislature wishes courts to intervene when agencies fail to act, it generally must write into the law that an administrative act is "presumed" after a certain time period following the relevant event (an individual complaint or application to the agency).[197] Likewise, under European law, it is unlikely that an opinion or working document would be considered an "act" amenable to review. It is also unlikely that the Commission's failure to make a determination on the adequacy of a third country or model contract could be

192. *See, e.g.*, Opinion 3/2001 on the Level of Protection of the Australian Privacy Amendment (Privacy Sector) Act 2000, Op. Working Party on the Prot. of Individuals with Regard to the Processing of Pers. Data, 5095/00/EN WP 40 final (Jan. 26, 2001).

193. *See* Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive, Working Doc. Working Party on the Prot. of Individuals with Regard to the Processing of Pers. Data, DG XV D/5025/98 WP 12 (July 24, 1998).

194. *See supra* notes 95–96.

195. *See* Interview with Susannah Haan, *supra* note 190.

196. *See* della Cananea, *supra* note 156; CASSESE ET AL., *supra* note 168. The administrative act is also central to German administrative law (*Verwaltungsakt*) and French administrative law (*acte administratif*). For a discussion of the difficulty of obtaining judicial review of informal action and inaction in U.S. administrative law, see generally JERRY L. MASHAW & DAVID L. HARFST, THE STRUGGLE FOR AUTO SAFETY (1990) (arguing that when the National Highway Safety Transportation Administration switched from rulemaking to recalls, a form of informal agency action, it became more difficult for courts to exercise judicial review); PIERCE, *supra* note 191, at 1270 (agency inaction presumptively unreviewable).

197. *See generally* Bernardo Giorgio Mattarella, *Il Provvedimento*, *in* 1 TRATTATO DI DIRITTO AMMINISTRATIVO, *supra* note 179, at 797, 894–96 (Sabino Cassese ed., 2d ed. 2003) (discussing problem of administrative "silence").

challenged before the European Courts.[198] When administrative action takes the form of inaction or informal action, the political process rather than courts must police for arbitrariness and illegality. In national systems, government agencies that fail to take the action necessary to implement certain statutory mandates or that informally implement statutes contrary to public opinion should expect to face pressure from elected officials.

The problem with the mixed procedure for international data transfers is twofold. First, the sharing of powers between national and European authorities appears to have generated even more of the judicially immune forms of administrative action (inaction and informal action) than occurs at the domestic level. National authorities, rather than experimenting based on their domestic experiences with information privacy—by blocking or authorizing certain transfers—have preferred inaction. Because it is so difficult to anticipate threats to privacy and devise measures that will adequately safeguard privacy rights once personal information leaves the European Union, national privacy commissioners have chosen to transfer responsibility to the European process. The European process, however, is inherently slow, meaning that inaction can persist for long periods.[199] In those periods, informal action—undertaken by the working party of national privacy authorities—prevails. The structure of privacy regulation, with a formal role for the comitology committee and an informal role for the working party, is somewhat unusual even for European policymaking. Nevertheless, informal action like that of the working party pervades the European regulatory system, both in the opinions given by numerous sector-specific advisory committees[200] and in the new form of European governance called the "Open Method of Coordination."[201] Therefore, the extent of informal action in the information privacy arena is likely to be replicated in other policy areas.

The second difficulty with the administrative practice of the European privacy network is that political accountability, which to some

198. *See generally* CRAIG & DE BÙRCA, *supra* note 6, at 483, 520 (setting down EU law on range of reviewable acts and conditions under which failure to act is reviewable).

199. *See generally* Fritz W. Scharpf, *The Joint-Decision Trap: Lessons from German Federalism and European Integration*, 66 PUB. ADMIN. 239 (1988).

200. *See, e.g.*, Commission Decision 73/306/EEC of 25 September 1973 Relating to the Setting up of a Consumers' Consultative Committee, 1973 O.J. (L 283) 18; Commission Decision 81/195/EEC of 16 March 1981 Setting Up, within the Advisory Committee on Seeds, a Special Section on the Approximation of Laws, 1981 O.J (L 88) 42; Commission Decision 2004/391/EC of 23 April 2004 on the Advisory Groups Dealing with Matters Covered by the Common Agricultural Policy, 2004 O.J. (L 120) 50.

201. *See generally* Grainne de Búrca, *The Constitutional Challenge of New Governance in the European Union*, 28 EUR. L. REV. 814 (2003).

extent compensates for the inability of courts to interfere under such circumstances, is weak in the European Union. As argued earlier, a system of shared powers requires that citizens be able to mobilize within the many different political communities in which regulators make their decisions, both national systems and the emerging supranational system in Brussels. Yet Europe-wide campaigns are extremely costly and difficult to mount, even for an organized group like labor, which unlike many other interest groups and citizen causes has a European federation (the European Trade Union Congress). Apart from the cost, the most fundamental difficulty is the lack of a European identity that would sustain concerted Europe-wide political action through the press, voting in parliamentary elections, lobbying, and other avenues for holding regulators accountable. While this form of the democratic deficit affects all types of European governance, it causes special problems for networks like this one that are associated with inaction and informal action. In such cases, the courts cannot enforce the administrative law of rights against bureaucrats *and* the democratic political process cannot hold administrators accountable.

Although my evaluation of the European privacy network focuses on rights and democratic accountability, a brief remark on effectiveness is warranted. This network is far less effective than would be expected by proponents of decentralized policymaking in the domestic and international spheres.[202] As the drafters of the Data Protection Directive themselves stated, the requirement of "adequacy" for international transfers of personal information was to serve as a general standard that would guide local regulators in their experiments with guaranteeing privacy.[203] Those experiments would gradually lead to a Europe-wide approach. The Commission repeated the hope that networks in the international data transfer area would facilitate information exchange and the development of "best practice."[204] This official articulation of the purposes and desired effects of the privacy network repeats verbatim the reasons that scholars have advanced in favor of decentralized and flexible administration: local experimentation and the discovery and rediscovery of best practices in a constantly changing social and economic

202. *See* Michael C. Dorf & Chuck F. Sabel, *A Constitution of Democratic Experimentalism*, 98 COLUM. L. REV. 267 (1998) (arguing for U.S. administrative law in which federal agencies set basic goals and state and local agencies experiment with implementation); Joanne Scott & David Trubeck, *Mind the Gap: Law and New Approaches to Governance in the EU*, 8 EUR. L.J. 1 (2002) (arguing that the "Open Method of Coordination" in the European Union will allow local diversity to persist at the same time that common standards are generated through exchange of best practices); SLAUGHTER, *supra* note 9, at 193 (arguing that transgovernmental networks produce experimentation and the emergence of best practices).

203. *See supra* note 101.

204. *See supra* notes 107–108.

environment. Yet the promise of networks has not been realized in the information privacy area.

Rather, the sharing of powers and responsibility in the privacy arena is associated with stasis and the related difficulties for liberal democratic ideals. The administrative action that has occurred has come from the center—the Commission's adequacy decisions—not the periphery. A number of possible explanations come to mind: foreign relations might require action from the political center; protecting information privacy might not be a domain in which local knowledge helps; safeguarding privacy once personal information is transferred abroad might be so difficult that neither national privacy authorities nor European administration are capable of taking action. I certainly do not claim that paralysis is intrinsic to the sharing and fragmentation of government powers through networks. I merely wish to suggest that, under certain circumstances, networks will not live up to the high expectations that have been set for them.

C. *Implications for Transgovernmental Networks*

The liberal democratic shortcomings of the European privacy network can inform our evaluation of other transgovernmental networks. In networks, decisionmaking power is shared by all nodes. Even though, outside the European Union, the authority to issue final, binding decisions rests with individual governments, practically speaking such decisions are made by national officials acting in concert. Rejecting network decisions, after-the-fact, through national democratic processes entails such high political and economic costs that only the United States and certain European countries can do so.[205]

Sharing power with other government officials is not, in and of itself, problematic. Access to global markets and foreign places brings immense benefits and to expect to be able to obtain such access without accommodating the citizens, practices, and laws of those foreign places is unrealistic. The European case, however, suggests that the network form of governance can fall short of liberal democratic values and points to strategies through which some of these shortcomings might be remedied. One important means of reconciling transgovernmental networks with principles of liberal democracy is their codification. As in the European privacy example, bringing the law to networks would render them

205. As Kal Raustiala argues, the regulatory model that emerges from transnational networks is influenced by "regulatory power" and therefore is likely to reflect the laws of the United States or a European state. As a result, the states that are powerful enough to reject the consensus view of transnational networks should also have less reason to do so. *See* Raustiala, *supra* note 60, at 61.

more visible to citizens. Codification would also inform the parties whose interests are directly implicated by network decisions of the division of powers between national and transnational regulators. This would bring certainty and predictability to members of the interested community, principles that are central to the rule of law ideal. Another improvement to transgovernmental networks suggested by the European example is the guarantee of public access to network documents. This would enable citizens to scrutinize the rationale for network decisions and would better equip them to hold their national regulators accountable.

The European case also points to problems with transnational networks that are less tractable. In light of the difficulties of popular mobilization across countries on issues like privacy, the policy decisions that result from transnational networks risk being compromises struck by government officials in isolation from the citizens whom they are supposed to represent. The hurdles to transnational mobilization—to putting pressure on all the regulators who share and exercise power in the network—are formidable.

While the inaction observed in the privacy case study cannot be generalized to other transgovernmental networks with any analytical rigor, this experience serves as a useful cautionary tale. Sometimes the distribution and fragmentation of power among numerous government units will not produce effective public action. Elaborating the conditions under which stalemate, rather than experimentation and best practice, will emerge is an area for future research in international law and the constitutional law of federalism.

The extent of informal action in the European privacy network is also instructive. The codification of the privacy network in the Data Protection Directive is an important step toward guaranteeing transparency in European administration. Yet the working party of national privacy authorities, which only has powers of informal action, has proven to be even more active than the Commission and the comitology committee on the issue of international data transfers. This suggests that because informal action is free from legal constraints and therefore easier to undertake, this mode of decisionmaking will continue to be attractive to transnational networks notwithstanding best efforts to the contrary.

V. The European Parliament and the Transatlantic Dispute over Information Privacy

This assessment of European networks would be radically incomplete without analyzing the role of the European Parliament in shaping and checking the decisions of European privacy regulators. In 1999, the European Parliament acquired formal powers over European administration.[206] Whenever the Commission is delegated powers of implementation under European law, it is generally required to act together with a comitology committee of national representatives, as in the case of international data transfers under the Data Protection Directive. That is, the Commission must send the proposed implementing decision to the committee of national regulators for deliberation and a vote. As of 1999, the Commission must, at the same time, send the proposal to the European Parliament. The European Parliament does not have a formal veto power, but it can pass resolutions approving or disapproving of the proposed decision and the Commission "shall re-examine the draft measur[e]" in light of the parliamentary resolution.[207]

From the perspective of the formal institutional prerequisites of democracy, this reform of European administration represents an improvement. In most Member States, parliaments have the power to approve or veto implementing rules proposed by their executive branches under enabling legislation. What in American administrative law is deemed an unconstitutional legislative veto, in European administrative law is considered a legitimate, constitutional device for checking government administration.[208] In conferring the European Parliament with the power to receive drafts and vote resolutions, European legislators nudged the European Union one step closer to a parliamentary democracy model.

Yet the European Parliament does not use this power.[209] The reasons for the Parliament's disinterest are fairly obvious. Hundreds of

206. Comitology Decision, *supra* note 172, at arts. 7–8. For a comprehensive analysis of this reform, see Koen Lenaerts & Amaryllis Verhoeven, *Towards a Legal Framework for Executive Rule-Making in the EU? The Contribution of the New Comitology Decision*, 37 Common Mkt. L. Rev. 645 (2000).

207. Comitology Decision, *supra* note 172, at art. 8.

208. *See, e.g.*, Adam Tompkins, *Delegated Legislation in the English Constitution*, *in* Delegated Legislation and the Role of Committees in the EC 101, 109–14 (Mads Andenas & Alexander Türk eds., 2000); Alexander Türk, *Delegated Legislation in German Constitutional Law*, *in* Delegated Legislation and the Role of Committees in the EC, *supra*, at 127, 162.

209. *See* Report from the Commission on the Working of Committees in 2002, 2003 O.J. (C 223 E) 16, 5 (noting that no European Parliament resolutions were based on the Comitology Decision, *supra* note 172, at art. 8, in 2002); Report from the Commission on the Working of Committees during 2001, 2003 O.J. (C 223 E) 1, 4 (noting the same for 2001); Report from

implementing decisions, generally involving highly technical issues, are proposed every year and European parliamentarians simply do not have the resources or the political will to follow and react to such developments.

The one exception to the rule of parliamentary disinterest is in the area of international information privacy. On two separate occasions, the European Parliament used its formal powers to oppose transfers of personal information to the United States that had been authorized by the Commission.[210] According to the Parliament, in neither case did the United States offer adequate protection for privacy. When the Data Protection Directive first came into force in 1998, a number of American companies feared that when they transferred European personal information to the United States, their information practices would run afoul of European law.[211] In response, the U.S. Department of Commerce initiated negotiations with the Commission under Article 25 of the Data Protection Directive. The two sides reached an agreement on privacy principles which, if adopted by U.S. organizations, would entitle those organiza-

---

the Commission on the Working of the Committees during 2000, 2002 O.J. (C 37) 2, 6 ((noting that the "Safe Harbor" resolution described below was the only time Parliament passed a resolution based on the Comitology Decision, *supra* note 172, at art. 8). The Commission report for 2003 has not been issued yet, but aside from the resolution on the EU–U.S. Passenger Name Records (PNR) agreement described below, it does not appear that the Parliament exercised its oversight powers in 2003 or 2004.

210. Even before the two episodes narrated in this section, the European Parliament expressed doubts as to the adequacy of privacy safeguards in the United States. In the late 1990s, the Parliament commissioned a number of reports on U.S. government surveillance and the potential threat posed by such surveillance to European privacy rights. *See* STEVE WRIGHT, AN APPRAISAL OF TECHNOLOGIES OF POLITICAL CONTROL (Scientific and Technological Options Assessment, Directorate Gen. for Research, Eur. Parl., Doc. No. PE 166.499, 1998); Duncan Campbell, *Part 2/5: The State of the Art in Communications Intelligence (COMINT) of Automated Processing for Intelligence Purposes of Intercepted Broadband Multi-Language Leased or Common Carrier Systems, and Its Applicability to COMINT Targeting and Selection, Including Speech Recognition*, *in* DEVELOPMENT OF SURVEILLANCE TECHNOLOGY AND RISK OF ABUSE OF ECONOMIC INFORMATION (Scientific and Technological Options Assessment, Directorate Gen. for Research, Eur. Parl., Doc. No. PE 168.184, 1999) [hereinafter DEVELOPMENT], *available at* http://www.europarl.eu.int/stoa/publi/pdf/98-14-01-2_en.pdf; Frank Leprevost, *Part 3/5: Encryption and Cryptosystems in Electronic Surveillance: a Survey of the Technology Assessment Issues*, *in* DEVELOPMENT, *supra*, *available at* http://www.europarl.eu.int/stoa/publi/pdf/98-14-01-3_en.pdf; Chris Elliot, *Part 4/5: The Legality of the Interception of Electronic Communications: A Concise Survey of the Principal Legal Issues and Instruments under International, European and National Law*,*in* DEVELOPMENT, *supra*, *available at* http://www.europarl.eu.int/stoa/publi/pdf/98-14-01-4_en.pdf; Nikos Bogolikos, *Part 5/5: The Perception of Economic Risks Arising from the Potential Vulnerability of Electronic Commercial Media to Interception*, *in* DEVELOPMENT, *supra*, *available at* http://www.europarl.eu.int/stoa/publi/pdf/98-14-01-5_en.pdf.

211. *See* Joel R. Reidenberg, *E-Commerce and Trans-Atlantic Privacy*, 38 HOUSTON L. REV. 717, 736 (2001); 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, 69–79.

tions to a "Safe Harbor" from European law and a presumption of "adequacy" under the Data Protection Directive.[212] The national representatives on the comitology committee approved the agreement and the Commission's proposed decision on adequacy. But when the Commission sent the proposed decision to the European Parliament, it faced strident criticism from parliamentarians who contended that the Safe Harbor Principles allowed for too many exceptions and did not incorporate a strong enforcement mechanism.[213] The Parliament passed a resolution opposing the Commission's proposed adequacy finding by a vote of 279 to 259.[214]

Another spat with the United States over privacy has provoked again the European Parliament to exercise its oversight powers. Following the terrorist attacks of September 11, 2001, the U.S. government began demanding access to passenger information stored by European airlines (Passenger Name Records or PNR). Airlines serving the transatlantic market were put in a bind. If airline companies complied with U.S. demands, they risked prosecution by European privacy authorities for failing to guarantee an adequate level of privacy protection; if they did not comply, they faced intrusive searches of their passengers and extensive delays on arrival in the United States.[215] As a stop-gap measure, the Commission and the U.S. Bureau of Customs and Border Protection (Customs Bureau) issued a joint statement in February 2003: the Customs Bureau had given guarantees sufficient to render the transfer of passenger data temporarily lawful under European law.[216] At the same time, the European Union and the United States launched negotiations on a bilateral agreement. In the course of the negotiations, the European Parliament passed two separate resolutions criticizing the Commission's handling of the negotiations and threatening to take the Commission to court.[217]

In December 2003, the two sides reached a tentative agreement: the Customs Bureau would afford European airline data certain privacy

212. *See* Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45,666 (July 24, 2000).

213. Steve R. Salbu, *The European Union Data Privacy Directive and International Relations*, 35 VAND. J. TRANSNAT'L L. 655 (2002).

214. *Id.* at 678–79.

215. *See* Christopher Patten, Address to the European Parliament (Apr. 21, 2004), *available at* http://europa.eu.int/comm/external_relations/news/patten/sp04_189.htm.

216. *Id.*

217. Eur. Parl. Resolution on Transfer of Personal Data by Airlines in the Case of Transatlantic Flights (P5_TA(2003)0097) (March 13, 2003), *available at* http://www.statewatch.org/news/2004/mar/ep-pnr-report.pdf; Eur. Parl. Resolution on Transfer of Personal Data by Airlines in the Case of Transatlantic Flights: State of Negotiations with the USA, 2004 O.J. (C 81 E) 105.

guarantees and the Commission would adopt a decision finding the U.S. system "adequate." But when the Commission forwarded the draft adequacy decision to the European Parliament, it met with staunch opposition. On March 31, 2004, the European Parliament voted a resolution condemning the Commission decision and the EU–U.S. agreement.[218] And, on April 21, 2004, the Parliament challenged the EU–U.S. agreement in the European Court of Justice.[219] In the eyes of the Parliament, its shortcomings were numerous: the purposes for which the Customs Bureau was permitted to use personal information were overbroad (not only preventing and combating "terrorism and related crimes" but an unspecified category of "other serious crimes, including organised crimes"); the Customs Bureau was allowed to collect an excessive amount of personal data on seemingly irrelevant matters such as voluntary and involuntary ticket upgrades; the retention period of eight years for the data was excessive; and the Chief Privacy Officer in the Department of Homeland Security did not have the independence necessary to enforce vigorously privacy rights.[220] The Commission's adequacy deci-

218. Eur. Parl. Resolution on the Draft Commission Decision Noting the Adequate Level of Protection Provided for Personal Data Contained in the Passenger Name Records (PNRs) Transferred to the US Bureau of Customs and Border Protection, (P5_TA(2004)0245) (March 31, 2004), *available at* http://www.statewatch.org/news/2004/mar/ep-pnr-report.pdf.

219. *See* Request for an Opinion Submitted by the Eur. Parl. under Art. 300(6) of the EC Treaty, 2004 O.J. (C 118) 1.

220. Eur. Parl. Resolution, *supra* note 217. The legal effect of the EU–U.S. agreement and the grounds of the European Parliament's lawsuit are more complicated than this brief summary suggests. The Commission negotiated an agreement with the U.S. government in order to issue an adequacy decision *and* to enter into a bilateral international agreement with the U.S. government. The second form of action is unusual in the international privacy field and was necessary because the Customs Bureau wished to access European PNR data located in airline databases in the European Union. A bilateral agreement, pursuant to the treaty-making powers of the European Community, would constitute a binding legal act. Such an act would give the European airlines that allowed the U.S. Customs Bureau access to their PNR data a ground for lawful data processing under Article 7(c) of the Data Protection Directive. ("Member States shall provide that personal data may be processed only if . . . processing is necessary for compliance with a legal obligation to which the controller is subject.") The treaty power under Article 300(3) of the EC Treaty provides that, as a rule, the Parliament must be consulted, but that if the treaty would alter internal European legislation the Parliament must give its assent. Given that the Parliament's role in the administrative part of the decision (the adequacy decision) is less significant than in the treaty-making part of the decision (European Community's entry into an international agreement with the United States), the case in the Court of Justice challenged only the international agreement. *See* Request for an Opinion, *supra* note 219. Parliament did so by requesting an opinion as to "whether an agreement envisaged is compatible with the provisions of this Treaty" under Art. 300(6) of the EC Treaty. The Parliament claimed that because the EU-U.S. agreement infringed and altered the guarantees of the Data Protection Directive, the Parliament should have had the right of assent, not simply consultation. *Id.* The Parliament also claimed that, regardless of the procedure, the agreement was invalid because it breached a fundamental principle of EU law, namely the right to privacy. Before the Court could rule on the Parliament's request for an opinion, the EU-U.S. agreement came into force. Therefore, the Parliament decided to with-

sion has since taken effect[221] and the European Parliament's legal challenge is pending in the Court of Justice.[222]

How do we explain this exceptional degree of parliamentary activism? Why has the European Parliament chosen to intervene in the information privacy field when, in other areas of European administration, the Commission routinely forwards proposed implementing measures and the Parliament routinely does nothing? Undoubtedly, part of the answer rests in the ease with which the seemingly technocratic issue of "data protection" can be reframed as an issue of fundamental importance to the European people. The privacy rights of citizens are imperiled. Such rights are not simply German, Italian, or French, they are European. Since the early 1970s, the Court of Justice has recognized a common set of fundamental rights shared by all citizens of the European Union, which today includes information privacy[223]; since the adoption of the Charter of Fundamental Rights in 2000, the European Union has a highly symbolic, written catalogue of rights, which includes the "right to the protection of personal data."[224] The right to the protection of personal data represents a deeply moral issue around which parliamentarians—and those who vote for them—can rally. When such basic rights are threatened by a powerful outsider like the United States, they become even more salient. Indeed, Parliament's championing of the European right to privacy is as much a reflection of an existing, common right as it is a creature of perceived difference with the United States.[225]

The Safe Harbor and the airline passenger data episodes are evidence of nascent democracy in the European system of administrative

---

draw its request for an opinion and to bring two new actions challenging the European legal acts through which the agreement had come into force. *See* Action brought on 27 July 2004 by the European Parliament against the Council of the European Union: Case C-317/04, 2004 OJ (C 228) 31; Action brought on 27 July 2004 by the European Parliament against the Commission of the European Communities: Case C-318/04, 2004 OJ (C 228) 32. The grounds of both actions are similar to those of the request for an opinion.

221. *See* Commission Decision 2004/535/EC of 14 May 2004 on the Adequate Protection of Personal Data Contained in the Passenger Name Record of Air Passengers Transferred to the United States Bureau of Customs and Border Protection, 2004 O.J. (L 235) 11.

222. *See* Action brought on 27 July 2004 by the European Parliament against the Council of the European Union: Case C-317/04, 2004 OJ (C 228) 31; Action brought on 27 July 2004 by the European Parliament against the Commission of the European Communities: Case C-318/04, 2004 OJ (C228) 32.

223. *See, e.g.*, Cases C-465/00, C-138/01, and C-138/01, Rechnungshof and others, 2003 E.C.R. I-4989, point 74.

224. Charter of Fundamental Rights of the European Union, art. 8, 2000 O.J. (C 364) 1.

225. Timothy Garton Ash argues similarly that an identity that spans the entire European Union will be based on "contrast with, if not outright opposition to, America." TIMOTHY GARTON ASH, FREE WORLD: AMERICA, EUROPE, AND THE SURPRISING FUTURE OF THE WEST 55 (2004).

networks. As a matter of the formal institutional prerequisites of democracy, participation of the directly elected legislative assembly in the administration of international data transfers can only be a good thing.[226] The transatlantic dispute over privacy also revealed a common European identity and contributed to the formation of that European identity. This too is good for democracy. A shared identity that transcends the nation satisfies one of the sociological preconditions of European democracy.[227] Such an identity enables citizens to mobilize irrespective of nationality in the many different political systems—national and supranational—in which European regulators operate. Currently, European citizens consider the European Parliament as a sideline to the important business of national government. And some would say for good reason. At present, the European Parliament is responsible for making seemingly insignificant decisions such as what types of sweet, dark substances can be called "chocolate" and how glass bottles should be recycled. The stand that the European Parliament took on privacy is just one of many debates that, over time, will render the European Parliament an important institution with real significance for European voters. As parliamentary votes and European elections are framed as choices on values and rights, democracy will follow.

But let us step back for a moment. What if the European Parliament had the power to veto Commission implementing decisions, not simply condemn such decisions in non-binding resolutions? The answer, quite simply, is that neither the Safe Harbor principles nor the PNR agreement would have been concluded. Conflict, not concession, was what the European democratic process demanded. In the early stages of the PNR dispute, the U.S. government's categorical and inflexible demands for information on European citizens created difference, which gave rise to a political opportunity for the European Parliament. The Parliament could take a stand on European values. Once this democratic process was triggered, transatlantic compromise was low on the European political agenda. To go back to transgovernmental networks, the rise of democracy in European networks was at odds with effective international cooperation through another network—the transatlantic one between the European Commission and the U.S. Customs Bureau. The constitutional transformation underway in the European Union holds out the promise of democratizing one of the world's most advanced examples of interna-

226. For a formal institutional definition of democracy and an analysis of democracy in the European Union from that perspective, see, e.g., Andrew Moravcsik, *In Defence of the 'Democratic Deficit': Reassessing Legitimacy in the European Union*, *in* INTEGRATION IN AN EXPANDING EUROPEAN UNION: REASSESSING THE FUNDAMENTALS 77 (J.H.H. Weiler et al. eds., 2003).

227. For a sociological definition of democracy, *see, e.g.*, Scott, *supra* note 188, at 102.

tional cooperation. Yet, at the same time, the changing nature of European politics is likely to frustrate cooperation in other arenas of global governance.

CONCLUSION

Europe and increasingly the world govern through networks. The case of the European network of information privacy regulators is instructive on a number of counts. Networks will emerge only if government officials agree on the underlying policy objectives of the network or if some States can derive significant benefits by adopting the policies of other States. We would predict, therefore, that networks and the beneficial effects of networks are more likely to emerge in certain policy areas than in others. Human rights, for instance, is an area in which transnational governance by networks of government prosecutors is unlikely to emerge. States disagree on how to define rights outside of flagrant abuses such as genocide. Even more important, governments and markets are not as ready to use incentives to induce States to adopt western approaches as they are in fields such as antitrust and intellectual property law.

The European experience also shows that, to some extent, networks can be brought under the disciplining force of the law. The mixed procedure established under the Data Protection Directive is one such example of bringing the law to informal transnational practice. In doing so, citizens can continue to enjoy many of the rights guaranteed under the administrative law of liberal democracies. Democratic accountability, however, suffers. With the possible exception of the United States and certain European States, the democratic process within a single country cannot hold network regulators accountable. Precisely because policymaking decisions are made not by national regulators acting alone but by all the officials in the network, political mobilization at the national level is not enough. Citizens must be capable of banding together and taking action in the multiple nations and political communities in which regulators operate, and yet citizens are divided by lack of resources and national identities.

Turning to administrative practice, the regulation of international data transfers demonstrates that sometimes inaction, not effective governance, can result from regulatory networks. Furthermore, even after the law is brought into a transgovernmental network, informal action may persist. In those instances, individual rights suffer. Compared with national administration, transnational inaction and informal action is particularly worrisome because of democracy's dysfunctions in the

transnational arena. The European Parliament's recent effort to protect the privacy of information transferred to the United States suggests that, under certain conditions, those dysfunctions might be overcome. The impact of nascent European democracy on other transnational networks and the communities served by them remains to be seen.