Articles

Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards

Gregory Shaffer†

---

† Assistant Professor of Law, University of Wisconsin Law School. An earlier version of this Article was presented at the Structure and Organization of Government Conference held at the University of Wisconsin-Madison on April 24, 1999. Thanks to Colin Bennett, Peter Carstensen, Fred Cate, Howard Erlanger, Henry Farrill, John Kidwell, Neil Komesar, Joel Reidenberg, Marc Rotenberg, Gerald Thain, Frank Turkheimer, and Eric White for their comments on earlier drafts. Thanks also to Nicholas Long and Matthew Kim-Miller, who provided me with invaluable research assistance. Yet despite the help, all errors, of course, remain my own.

INTRODUCTION

Almost daily we are subject to phone calls, mail, or electronic communications from organizations trying to sell us services or solicit our money. How do they get our numbers? How do they learn our habits? Who is compiling, selling, and swapping information about us? It has been estimated that, on average, companies trade and transfer personal information about every U.S. resident every five seconds.[1] How may we review and control the use of this data when technological advances permit rapid, low-cost compilation, storage, and transfer of personal data?

Much of the compilation and transfer of personal information that is a daily occurrence in the United States is illegal in Europe. On October 24, 1998, European Union (EU) Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data ("EU Directive")[2] became effective. The EU

1. *See* JEFFREY ROTHFEDER, PRIVACY FOR SALE 17 (1992) (noting that "there are upwards of five billion records now in the United States that describe each resident's whereabouts and other personal minutiae"). Since the publication of Rothfeder's book in 1992, the frequency of transfer of personal information is likely much greater, given advances in technology. Technological advances permitting rapid, low-cost compilation, storage, and transfer of personal data are a central cause of threats to personal privacy. The impact of technological change on data privacy protection has been addressed in many works, a summary of which is provided in PRISCILLA REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 10–15 (1995).

2. Parliament and Council Directive 95/46/EC of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 1 [hereinafter EU Directive]. Although the EU Directive was adopted and published in the Official Journal of the European Community on October 24, 1995, pursuant to article 32(1) of the EU Directive, it did not become effective until "a period of three years from the date of its adoption"—that is, on October 24, 1998. *Id.*

The term "European Union" (EU) is used in this Article, as opposed to the term "European Community" (EC). The name of the regional European entity has changed over time as Europe has

Directive mandates significant regulatory controls over business processing and use of personal data. The EU Directive also provides that the European Commission may ban data transfers to third countries that do not ensure "an adequate level of protection" of data privacy rights.[3] The United States has taken an ad hoc, patchwork approach to data privacy protection, which does not appear "adequate" under the EU Directive's criteria.[4] United States governmental representatives have reacted vehemently to the prospect of a European ban on data transfers to the United States.[5]

---

integrated. Originally, the term used was the European Economic Community (EEC), formed pursuant to the 1957 Treaty Establishing the European Economic Community, Mar. 25, 1957, 798 U.N.T.S. 11 ("EEC Treaty"). The Treaty of European Union (TEU) of 1992, Feb. 7 1992, O.J. (C 224) 1, [1992] 1 C.M.L.R. 719, changed the name of the European Economic Community to the European Community, to designate that the European Community had integrated beyond purely economic matters. The TEU also created three separate pillars of activities for the regional bloc. The first pillar concerned all traditional EC matters, as expanded by the TEU to cover European economic and monetary union in particular. The second and third pillars (respectively named Common Foreign and Security Policy, and Justice and Home Affairs) concerned matters not previously within the competence of the EC institutions. The term that encompasses all three pillars is the European Union (EU). Technically, the EU Directive was enacted by the EC institutions governed under the first pillar. Community authorities and news commentators most often use the broader terms EU and European Union, and these terms are thus used in this Article. The EEC Treaty, as amended, can be found at Nov. 10, 1997, O.J. (C 340) 1 (1997) [hereinafter EC Treaty].

3. Article 25 of the EU Directive provides:

Principles

1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.
2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.
3. The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.
4. Where the Commission finds, under the procedure provided for in Article 31 (2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.
5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.
6. The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals. Member States shall take the measures necessary to comply with the Commission's decision.

EU Directive, *supra* note 2, art. 25.

4. *See infra* Sections III.C and V.C concerning U.S.-EU negotiations over the adequacy of U.S. privacy protections.

5. *See infra* Section III.C.

Americans can now look to European law for responses to this Article's initial concerns. Yet this is not because U.S. legislators will see its virtues and adopt its remedies, or because the European model is necessarily the right one. Rather, in a globalizing economy, European regulation casts a net wider than Europe.[6] In a globalizing economy, European law also constrains U.S. domestic privacy policies and practices.[7] This Article explores how. For example, in order to avoid a trade conflict, U.S. regulators promote enhanced data privacy "self-regulation" by businesses. In order to avoid EU data transfer restrictions, U.S. businesses implement new internal data privacy practices with an eye on the EU criteria. Through the publicity given to the EU Directive, U.S. privacy advocates press for businesses to adopt more stringent internal practices and for legislators to enact additional legislation. Privacy advocates' efforts, however, are not without contention. The war over privacy standards is fought not just between Europe and the United States. It is a civil war as well, fought within the United States itself, with European law changing the balance of power on the fields where U.S. interest groups clash.

This Article examines the ongoing dispute between the United States and the European Union over the regulation of data privacy protection from the perspectives of transnational regulatory conflict and interdependence.[8] It

---

6. Increased cross-border activity gives rise to jurisdictional conflicts. As information technologies multiply, computing power and usage expand, cross-border mergers, acquisitions, joint ventures, and investments increase, and companies generally expand their markets beyond national borders, cross-border flows of data proliferate. Information does not respect boundaries, whether national, natural, or personal. Multiple states assert jurisdictional authority over information flows because they affect citizens and other residents within them. Data flows implicate the laws where they are generated and the laws where they are received. In the age of Internet postings, this potentially triggers the application of every national, state, and local data processing law in the world. For analysis of the potential conflicting exercise by multiple authorities of prescriptive jurisdiction over Internet transmissions, see Jane C. Ginsberg, *Copyright Without Borders? Choice of Forum and Choice of Law for Copyright Infringement in Cyberspace*, 15 CARDOZO ARTS & ENT. L.J. 153, 156–59 (1997); Jane C. Ginsberg, *Extraterritoriality and Multiterritoriality in Copyright Infringement*, 37 VA. J. INT'L L. 587, 590 (1997); and Allan Stein, *The Unexceptional Problem of Jurisdiction in Cyberspace*, 32 INT'L LAW. 1167 (1998). For a Canadian outlook, see Pierre Trudel, *Jurisdiction over the Internet: A Canadian Perspective*, 32 INT'L LAW. 1027 (1998).

7. The sociologist Anthony Giddens characterizes globalization processes as "the intensification of worldwide social relations which link distant localities in such a way that local happenings are shaped by events occurring many miles away and vice versa." ANTHONY GIDDENS, THE CONSEQUENCES OF MODERNITY 64 (1990). For a recent analysis of the phenomena of "globalization," see DAVID HELD ET AL., GLOBAL TRANSFORMATIONS: POLITICS, ECONOMICS AND CULTURE (1999). The authors define globalization as "a process (or set of processes) which embodies a transformation in the spatial organization of social relations and transactions—assessed in terms of their extensity, intensity, velocity and impact—generating transcontinental or interregional flows and networks of activity, interaction, and the exercise of power." *Id.* at 16.

8. The inter-state battle between the United States and the European Union over data privacy protection affects intra-state skirmishes. For analysis of the growing importance of regulatory competition, coordination, and interdependence, see generally ABRAM CHAYES & ANTONIA HANDLER CHAYES, THE NEW SOVEREIGNTY: COMPLIANCE WITH INTERNATIONAL REGULATORY AGREEMENTS (1995); INTERNATIONAL REGULATORY COMPETITION AND COORDINATION (William Bratton et al. eds., 1996); and Anne-Marie Slaughter, *The Real New World Order*, FOREIGN AFF., Sept./Oct. 1997, at 183–97. For analysis of the effects of globalization on domestic politics, see generally INTERNATIONALIZATION AND DOMESTIC POLITICS (Robert Keohane & Helen Milner eds., 1996). For an earlier assessment of the impact of interdependence in international relations, see generally ROBERT KEOHANE & JOSEPH NYE, POWER AND INTERDEPENDENCE: WORLD POLITICS IN TRANSITION (1977).

assesses the impact of this conflict and interdependence on the behavior of private parties—particularly U.S. businesses operating in multiple jurisdictions. In an age of economic globalization, while many are concerned that national standards will be lowered to stimulate national competitiveness, this Article assesses the conditions under which cross-border economic exchange can help leverage standards upward, even in a powerful state such as the United States.

Although the site for this Article's analysis is the issue of data privacy, the issue is far from unique. Globalization processes affect broad areas of law, raising the concern that national standards are being lowered on account of global competitive pressures. Affected areas, to name a few, include environmental,[9] labor,[10] consumer,[11] health,[12] tax,[13] financial,[14] and securities law.[15] This Article explores the intricacies of how external pressures affect the

9. *See generally* DAVID VOGEL, TRADING UP: CONSUMER AND ENVIRONMENTAL REGULATION IN A GLOBAL ECONOMY 5–8 (1995) (assessing how firms adapting to more stringent regulation in jurisdictions with large markets can facilitate a raising of standards globally); Daniel Esty & Damien Geradin, *Market Access, Competitiveness, and Harmonization: Environmental Protection in Regional Trade Agreements*, 21 HARV. ENVTL. L. REV. 265 (1997) (discussing the relationship between trade liberalization and environmental protection); Richard Revesz, *Federalism and Environmental Regulation: Lessons for the European Union and the International Community*, 83 VA. L. REV. 1331 (1997) (challenging the race to the bottom argument); Thomas Schoenbaum, *International Trade and Protection of the Environment: The Continuing Search for Reconciliation*, 91 AM. J. INT'L L. 268 (1997) (examining the current state of conflict between trade regulation and environmental protection); Richard Stewart, *Environmental Regulation and International Competitiveness*, 102 YALE L.J. 2039 (1993) (setting forth, among other matters, rationales for international harmonization of standards); Peter Swire, *The Race to Laxity and the Race to Undesirability: Explaining Failures in Competition Among Jurisdictions in Environmental Law*, 14 YALE L. & POL'Y REV. 67 (1996) (analyzing the positive effects of regulation by multiple jurisdictions, preventing a race to the bottom).

10. *See generally* Lance Compa, *Labor Rights and Labor Standards in International Trade*, 25 LAW & POL'Y INT'L BUS. 165 (1993) (providing an overview of the current situation); Brian Langille, *General Reflections on the Relationship of Trade and Labor (Or: Fair Trade is Free Trade's Destiny)*, *in* 2 FAIR TRADE AND HARMONIZATION: PREREQUISITES FOR FREE TRADE? 231 (Jagdish Bhagwati & Robert Hudec eds., 1996); Katherine Van Wezel Stone, *Labor and the Global Economy: Four Approaches to Transnational Labor Regulation*, 16 MICH J. INT'L L. 987 (1995) (examining different approaches to preserve labor protection in a globalizing economy).

11. *See generally* Donald King, *Globalization Thinking: Commercial and Consumer Law Illustrations*, 39 ST. LOUIS U. L.J. 865 (1995) (examining different levels of policy determination in reaction to global processes).

12. *See generally* Joseph Contrera, *The Food and Drug Administration and the International Conference on Harmonization: How Harmonious Will International Pharmaceutical Regulations Become?*, 8 ADMIN. L.J. AM. U. 927 (1995) (describing the effects of harmonization efforts on U.S. regimes); Bryan Walser, *Shared Technical Decisionmaking and the Disaggregation of Sovereignty: International Regulatory Policy, Expert Communities, and the Multinational Pharmaceutical Industry*, 72 TUL. L. REV. 1597 (1998) (discussing the role of transatlantic experts in reforming domestic regulations).

13. *See generally* David E. Spencer, *OECD Report Cracks Down on Harmful Tax Competition*, 9 J. INT'L TAX'N 26 (1998) (discussing governmental concerns over foreign tax havens being used to circumvent domestic tax policy).

14. *See generally* Christopher Mailander, *Financial Innovation, Domestic Regulation and the International Marketplace: Lessons on Meeting Globalization's Challenge Drawn from the International Bond Market*, 31 GEO. WASH. J. INT'L L. & ECON. 341 (1998) (concerning the impact of globalization on the regulation of the bond market).

15. *See generally* Stephen Choi & Andrew Guzman, *National Laws, International Money: Regulation in a Global Capital Market*, 65 FORDHAM L. REV. 1855 (1997) (suggesting possible ways to bring about positive developments in securities regulation in a global market); Uri Geiger, *The Case for the Harmonization of Securities Disclosure Rules in the Global Market*, 1997 COLUM. BUS. L. REV. 241

stakes of local actors, who in turn incite changes in domestic policy and practice. It shows how foreign and domestic policies are increasingly enmeshed, so that the traditional distinctions between the domestic and the foreign in the United States, and between the internal and the external in the European Union, are misleading.[16] This Article combines its empirical analysis with an exploration of five central themes that are relevant to broad domains of law.

First, data privacy protection can be assured through the actions of alternative institutions, be they legislatures, regulatory bodies, courts, or markets. While the United States purports to rely more on market mechanisms, the European Union relies more on state regulation. In a globalizing economy, however, the actions of these institutions have impacts beyond national borders. Under-regulation by the United States jeopardizes the privacy interests of EU residents. Over-regulation by the European Union limits the commercial operations of U.S.-based enterprises. Foreign regulation can, in particular, affect domestic actors' appreciation of their stakes and their political leverage. EU regulatory policy can thereby affect U.S. policies and commercial practices, and vice-versa. I refer to this as *the theme of transnational institutional interdependence.*[17]

Second, while academic analysts and foreign nationalists note how the United States effectively exports its culture and norms abroad,[18] U.S. policy and practices are also affected by developments in other powerful states. In the case of data privacy, EU policy and practice places pressure on U.S. regulators and businesses to adapt U.S. data privacy policy and practice. State power (in particular through the use of market power) is a central determinant of cross-border negotiations over not only trade liberalization, but also over levels of social regulation. I refer to this as *the theme of foreign market power.*

(arguing that disclosure regimes must be harmonized); Jane Kang, *The Regulation of Global Futures Markets: Is Harmonization Possible or Even Desirable?*, 17 NW. J. INT'L L. & BUS. 242 (1996) (contending that regulatory diversity has positive effects); Amir Licht, *Regulatory Arbitrage for Real: International Securities Regulation in a World of Interacting Securities Markets*, 38 VA. J. INT'L L. 563 (1998) (discussing how regulatory regimes can undermine each other).

16. For presentations of the notions of transnational "governance" as opposed to "government," see generally GLOBAL GOVERNANCE: DRAWING INSIGHTS FROM THE ENVIRONMENTAL EXPERIENCE (Oran R. Young ed., 1997); and GOVERNANCE WITHOUT GOVERNMENT: ORDER AND CHANGE IN WORLD POLITICS (James N. Rosenau & Ernst-Otto Czempiel eds., 1992) [hereinafter GOVERNANCE WITHOUT GOVERNMENT]. As Rosenau states "Governance . . . is a more encompassing phenomenon than government. It embraces government institutions, but it also subsumes informal, non-governmental mechanisms whereby persons and organizations within its purview move ahead, satisfy their needs and fulfill their wants." James N. Rosenau, *Governance, Order, and Change in World Politics*, *in* GOVERNANCE WITHOUT GOVERNMENT, *supra*, at 1, 4. This Article, however, is more in the tradition of "law and society" scholarship, which addresses the interactions of law and social phenomena, giving rise to what University of Wisconsin Professor Stuart Macaulay, among others, calls "law-in-action." For an introduction to "law and society" scholarship, see generally LAW & SOCIETY: READINGS ON THE SOCIAL STUDY OF LAW (Stuart Macaulay et al. eds., 1995). *See also* Stuart Macaulay, *Law and the Behavioral Sciences: Is There Any There There?*, 6 L. & POL'Y 149 (1984) (noting some of the achievements of law and society scholarship and responding to critiques from critical legal studies scholars).

17. *See infra* Section II.E and Part V.

18. *See, e.g.*, MALCOLM WATERS, GLOBALIZATION 16 (1995) (stating that "[t]he most imitated society becomes easy to specify: 'United States society'" (citation omitted)).

Foreign market power provides leverage for influencing regulatory policies and private practices in other countries. This Article examines the role of market power in both intra-European negotiations over data privacy protection (Section I.A) and U.S.-EU negotiations (Section III.A).

Third, the U.S.-EU dispute demonstrates that individual European countries, in transferring authority to EU institutions, enhance their autonomy and influence vis-à-vis other powerful states, in particular the United States. By pooling their sovereignty over regulatory policy and acting collectively, European states increase their leverage in bargaining with the United States. I refer to this as *the theme of reallocated sovereignty*. That is, sovereignty is not lost; it is rather allocated among different levels of social organization. Perhaps counter-intuitively, the autonomy of local actors can be enhanced by allocating decision-making authority to a higher level of social organization, such as from individual European Member States to the European Union.[19]

Fourth, globalization critics often decry that globalizing processes pressure governments to reduce social protection requirements so as to reduce the costs of national enterprises and thereby enhance their competitiveness in the global market. Yet the case of data privacy protection shows that foreign regulatory requirements for greater social protection can be used as leverage to increase protection in the United States, not to reduce it. Globalization is not a one-way path "racing to the bottom." In fact, while it is not a race to anywhere in particular, it can (more likely than not) give rise to a ratcheting up of national standards. This is particularly the case where foreign regulation has externalities, as is the case with data privacy protection.[20] That is, lax regulation in one jurisdiction affects residents in other jurisdictions who, in turn, pressure their state representatives to make use of state market power to challenge foreign activities prejudicing their interests. I refer to this as *the theme of trading up*.[21] This is particularly the case with social regulations that

19. *See infra* Section III.A. To provide another example, by joining the World Trade Organization, smaller states may benefit from WTO rules to constrain the U.S.'s exercise of its market power to coerce them into adopting U.S.-prescribed policies. For a presentation of sovereignty as an allocation of jurisdictional authority between different levels of social organization, see Joel Trachtman, *Reflections on the Nature of the State: Sovereignty, Power and Responsibility*, 20 CAN.-U.S. L.J. 399, 400 (1994) [hereinafter Trachtman, *Reflections*] ("Sovereignty, viewed as an allocation of power and responsibility, is never lost, but only reallocated."). *See also* Joel Trachtman, *International Regulatory Competition, Externalization, and Jurisdiction*, 34 HARV. INT'L L.J. 47 (1993).

20. In economics, the term "externalities" refers to costs or benefits "that accrue to parties other than the firms that produce them." PAUL R. KRUGMAN & MAURICE OBSTFELD, INTERNATIONAL ECONOMICS: THEORY AND POLICY 280 (4th ed. 1997) (focusing on the case of positive externalities). An example of a negative externality is environmental pollution whose costs are not absorbed by the polluting firm or by the consumers of its products (that is, in the prices of the goods sold), but rather imposed on neighboring residents and other third parties. An example of a positive externality is the results of research that are not fully appropriated by the firm engaging in the research, but rather also benefit third parties.

21. *See infra* Parts V and VI. David Vogel, in his book TRADING UP, refers to the ratcheting up of domestic regulation on account of trade liberalization and economic integration as the "California effect." The size of the California market enables California to take a leading role in enhancing standards throughout the United States. Firms that wish to sell in the California market must adapt their product standards and (though to a lesser extent) production methods to its regulatory requirements. On the other pole, the ratcheting down of social protections in a "race to the bottom" in order to attract investment and enhance the competitiveness of local firms is referred to as the "Delaware effect."

broadly affect national lifestyles (from air quality controls to data privacy regulation). These social protections can often be viewed, in economic terms, as luxury goods whose demand increases disproportionately vis-à-vis the demand for other goods as income levels rise.[22]

Fifth, contrary to common perceptions, international trade liberalization rules appear not to constrain significantly the ability of governments to require greater social protection in many areas, including that of data privacy. On the contrary, they limit the ability of other states, such as the United States, to threaten retaliation against jurisdictions with high data privacy protections, such as the European Union, if they enforce their regulations against U.S. commercial interests. I refer to this as *the theme of WTO supra-national constraints.*[23] In this way, international trade rules provide the European Union with a shield against U.S. threats to retaliate against the EU Directive's application, thereby further facilitating the EU Directive's extra-jurisdictional impact.

***

Parts I and II of this Article introduce the U.S. and EU approaches to data privacy protection, the United States purportedly focusing more on market regulation and the European Union on government regulation. Part I introduces the EU Directive's regulatory approach to data privacy protection. It first examines the EU Directive's relation to efforts to enhance trade liberalization within the European Union, assessing how the demand to ensure free data transfers in Europe permitted a leveraging upward of European data privacy requirements. It then considers the additional costs imposed on

Vogel's book focuses on the effects of trade liberalization on environmental protection, which, in his view, exemplifies the California effect. *See* VOGEL, *supra* note 9, at 5–8. The analysis in Vogel's book, however, focuses on the role of large exporting firms that, once they adapt to higher foreign standards to sell and operate in a foreign market, support the raising of domestic standards because they would have a competitive advantage over local firms. This is not the case in the U.S.-EU dispute over data privacy. Rather, as described in Part V, *infra*, U.S. firms (large and small) oppose legislation raising U.S. data privacy requirements, but are nonetheless being pressed to raise their U.S. data protection standards on account of direct pressure from foreign authorities. That pressure in turn, changes the stakes of domestic actors in the United States, affecting U.S. political and regulatory processes and business practices. *See infra* Part V.

22. As used in this Article, the term "luxury goods" refers to those goods whose demand increases proportionately more than the demand for other goods when individual income increases. *See* JAMES GWARTNEY & RICHARD STROUP, ECONOMICS: PRIVATE AND PUBLIC CHOICE 457 (1997). Income elasticity "measures the responsiveness of the demand for a good to change in income." *Id.* A luxury good is formally defined, in economic terms, as a good with an income elasticity of greater than one. That is, a 10% increase in income will lead to a greater than 10% increase in the demand for a luxury good, holding prices constant. Data privacy regulation and environmental regulation can be viewed as luxury goods in the sense that individuals are more likely to demand (and pay the price for) their protections when individuals' incomes rise, as compared to their demand for other goods (such as bread and potatoes). Other examples of luxury goods are recreational activities, air travel, and donations to charitable groups. *See id.* This factor is further explored in Part VI, *infra*.

23. *See infra* Part IV. The WTO refers to the World Trade Organization, the international organization based in Geneva, Switzerland, that oversees "the common institutional framework for the conduct of trade relations among its members." Final Act Embodying the Results of the Uruguay Round of Multilateral Trade Negotiations, Marrakesh Agreement Establishing the World Trade Organization, Apr. 15, 1994, art. II, 33 I.L.M. 1143, 1144 (1994).

businesses and consumers by these requirements, which help explain U.S. businesses' confrontational response to the EU Directive. It concludes by presenting the EU Directive's controversial provision providing for a ban on data transfers to the United States and other third countries whose data privacy protection laws are not "adequate." Part II surveys the state of data privacy protection in the United States applying to acts of government and of the private sector, as well as problems with this U.S. public-private distinction. It examines the alternative and complementary roles of legislatures, courts, and markets in the United States in protecting individual privacy from third-party exploitation of personal information.[24] In particular, it assesses how different default rules can affect private ordering of data privacy protection in the U.S. market, shifting the allocation of costs and benefits among businesses and consumers. Part II critiques single jurisdictional analysis for failing to account for extra-jurisdictional impacts, as EU law can help shape U.S. default rules in the area of data privacy.

Parts III and IV address EU-U.S. negotiations over data privacy in the context of international trade rules that potentially constrain EU and U.S. actions. Part III examines the multiple means available under the EU Directive for the European Union to restrict data transfers to the United States, and the ongoing negotiations between U.S. and EU authorities to resolve conflicts over the adequacy of U.S. data privacy protection. Part IV places these transatlantic negotiations within the context of the multilateral trade liberalization rules of the World Trade Organization (WTO). It addresses the legitimacy of the EU Directive under international trade rules were the EU Directive to be challenged by the United States before the WTO's Dispute Settlement Body, as the United States has implicitly threatened. It examines the constraints international trade rules place not only on the European Union in applying the EU Directive, but also on the United States in responding to its application.

Parts V and VI address the impact of the EU regulation on purely domestic U.S. practices and examine the factors that permit regulatory requirements to be leveraged upward in this area. Part V assesses how the practices of a powerful country such as the United States are affected by the policies of another powerful entity, the European Union. It evaluates the EU Directive's impact on privacy protection efforts in the United States through providing opportunities for U.S. privacy advocates and service providers, pressuring U.S. regulators, and constraining U.S. business practice. Part VI, the Article's conclusion, assesses the factors that permit foreign policies to raise some domestic social protections in the United States, such as data privacy protection, but not others.

---

24. In such examination, this part assesses the benefits and detriments of decision-making authority through alternative institutional processes—whether the political process, the market process, or the adjudicative process. This is sometimes referred to as "comparative institutional analysis." For a cogent presentation of comparative institutional analysis, see NEIL K. KOMESAR, IMPERFECT ALTERNATIVES: CHOOSING INSTITUTIONS IN LAW, ECONOMICS, AND PUBLIC POLICY 3 (1994).

I. EU DATA PRIVACY RULES AND THEIR IMPACT ON BUSINESS

This part first explores the link between trade liberalization and data privacy protection within the European Union itself (Section A). It then presents the controls imposed by the EU Directive to protect data privacy (Section B), and the costs of these controls on business and consumers (Section C). It concludes by examining the EU threat to ban data transfers to the United States on account of "inadequate" U.S. protections (Section D).

A. *Trading Up in the European Union: The Link Between Data Privacy Protection and EU Trade Liberalization*

Among the ironies inherent in the U.S.-EU dispute is that the original purpose of the EU Directive was not just to increase data privacy protection within the European Union.[25] It was also to ensure the uninhibited flow of data within the European Union from the threat of unilateral bans by individual EU Member States[26] on account of their differing data privacy protection regimes. The European Union, as a bloc, is now in a similar position of threatening to cut off data flows to the United States.

The EU Directive was negotiated within the context of the threat of data transfer bans from certain EU Member States with protective data privacy laws (such as France and Germany) to other EU Member States with less stringent laws (such as Italy),[27] at a time when EU Member States were attempting to create a single integrated market.[28] By requiring similar data privacy protection throughout the European Union, the EU Directive concurrently removed the threat to unhindered data flows between Member States. As reflected in the EU Directive's preamble, the effort to promote trade liberalization and ward off threats to it was an inherent part of the EU scheme. The preamble provides:

---

25. Background to the passage of the EU Directive is provided in Graham Pearce & Nicholas Platten, *Achieving Personal Data Protection in the European Union*, 36 J. COMMON MKT. STUD. 529 (1998).

26. "Member States" is the term used to refer to the 15 countries that make up the European Union.

27. France, for example, under French domestic law, prohibited the transfer of data from a French subsidiary of an Italian parent corporation to Italy because of the lack of an omnibus data privacy law in Italy. France also prohibited the transfer of patient records to Belgium. *See* Fred H. Cate, *The EU Data Protection Directive, Information Privacy, and the Public Interest*, 80 IOWA L. REV. 431, 438 (1995) (citing Déliberation no. 89-78 du 11 juillet 1989, *reprinted in* Commission nationale de l'informatique et des libertés, 10e Rapport au president de la Republique et au Parlement 1989, at 32–34 (1990) [hereinafter CNIL Rapport] (discussing the Italian transfer), and Déliberation no. 89-98 du 26 septembre 1989, *reprinted in* CNIL Rapport, 35–37 (discussing the Belgian transfer)). Member States have also refused to transmit data to EU institutions on privacy grounds. For example, Germany has refused to transmit census data to EU authorities, and France has refused to transfer information relating to the beneficiaries of subsidies. *See* Spiros Simitis, *From the Market to the Polis: The EU Directive on the Protection of Personal Data*, 80 IOWA L. REV. 445, 467 (1995) (citing Hessischer Datenschutzbeauftragter, 18 Tätigkeitsbericht 27–28, 43–45 (1989)).

28. *See* Nick Platten, *Background to the History of the Directive*, *in* EC DATA PROTECTION DIRECTIVE 13, 23 (David Bainbridge ed., 1996).

> (7) Whereas the difference in levels of protection of the rights and freedoms of individuals, notably the right to privacy, with regard to the processing of personal data afforded in the Member States may prevent the transmission of such data from the territory of one Member State to that of another Member State; whereas this difference may therefore constitute an obstacle to the pursuit of a number of economic activities at Community level . . .
>
> (8) Whereas, in order to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of individuals with regard to the processing of such data must be equivalent in all Member States . . .
>
> (9) Whereas, given the equivalent protection resulting from the approximation of national laws, the Member States will no longer be able to inhibit the free movement between them of personal data on grounds relating to protection of the rights and freedoms of individuals, and in particular the right to privacy . . . .[29]

To ensure the economic benefits of trade liberalization through the creation of a single "internal market," EU Member States collectively agreed to guarantee more stringent protections of data privacy.

From a practical standpoint, the goals of protecting individual privacy and ensuring trade liberalization within the European Union were inseparable.[30] The link, however, was not because data protection and free data flows naturally go hand in hand.[31] Rather, they were inseparable for political reasons. While the European Union could have mandated that no individual Member State block data transfers regardless of the extent of privacy protection in any other Member State, this was inconceivable from a practical standpoint. First, regulation in a Member State with less stringent data privacy controls has potentially significant externalities, thereby affecting residents in other Member States. Germany's more stringent controls over data collection and transfer would be of little avail if German companies could freely transfer information across the border to Italy, which did not enforce

---

29. EU Directive, *supra* note 2, pmbl.

30. The link between market regulation and higher social protection standards in Europe is not limited to data privacy protection. Article 95 of the Treaty Establishing the European Community mandates that harmonization measures "concerning health, safety, environmental and consumer protection" needed to complete the internal market shall "take as a base a high level of protection." EC Treaty, supra note 2, art. 95. As Christian Joerges states, the upward harmonization requirement under article 95 "has in fact been achieved." Christian Joerges, *Bureaucratic Nightmare, Technocratic Regime and Dream of Good Transnational Governance, in* EU COMMITTEES: SOCIAL REGULATION, LAW AND POLITICS 5 (Christian Joerges & Ellen Vos eds., 1999). European market integration has, for the most part, not resulted in deregulation, but rather in re-regulation at multiple levels of governance. The link between increased intra-European economic exchange and the growth of EU legislation is traced in Alec Stone Sweet & James A. Caporaso, *From Free Trade to Supranational Polity: The European Court and Integration, in* EUROPEAN INTEGRATION AND SUPRANATIONAL GOVERNANCE 92–133 (Wayne Sandholtz & Alec Stone Sweet eds., 1998).

31. The natural connection between free data flows and data privacy protection is sometimes maintained by privacy advocates. Marc Rotenberg of Electronic Privacy Information Center (EPIC), a non-profit advocacy group based in Washington D.C., affirmatively cites the statement by an early leading European advocate of data privacy protection, Jan Freese, who proclaimed that "'[p]rivacy protection is necessary to ensure the free flow of information.'" Comments from Marc Rotenberg on an earlier draft of this Article, Apr. 14, 1999 (on file with author). Many trade academics, however, maintain that harmonization is typically sub-optimal and should be avoided in favor of mutual recognition by states of each other's standards. *See, e.g.*, Alan O. Sykes, *The (Limited) Role of Regulatory Harmonization in International Goods and Services Markets*, 2 J. INT'L. ECON. L. 49 (1999) (noting that cooperation is necessary where production results in cross-border impacts).

similar controls. European Union Member States' institutional approaches to data privacy protection were thus interdependent.

Second, and most importantly, the most powerful states in the European Union—Germany and France—demanded greater data privacy protection.[32] Because access to their markets was important, these Member States exercised considerable leverage in the negotiation of EU trade liberalization rules. They would have blocked a requirement of free transferability of data without concomitant data privacy protection requirements. Had only a small country such as Greece or Portugal favored increased privacy protection, there would have been little pressure for requiring protection throughout the European Union. It was the convergence of interests of powerful states, backed by large markets, to both facilitate free information flows and retain stringent data privacy controls that permitted the EU Directive to go forward. It was France and Germany's political exploitation of market power that enabled protection to be traded up in the European Union.[33]

As a result, the EU Directive has twin "objects," which are set forth in its first article. Paragraph 1 of article 1 provides that "Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data."[34] Paragraph 2 provides that "Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1."[35] Only by ensuring the protection of "fundamental" privacy rights throughout the

---

32. The background of Germany's data privacy laws is presented in COLIN BENNETT, REGULATING PRIVACY: DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES 74–82 (1992). For analysis of the development of data protection laws in Europe since the 1970s, see Viktor Mayer-Schonberger, *Generational Development of Data Protection in Europe*, *in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 219 (Philip Agre & Marc Rotenberg eds., 1998). A survey of privacy laws throughout the world has been compiled by the Global Internet Liberty Campaign (GILC). *See* GLOBAL INTERNET LIBERTY CAMPAIGN, PRIVACY AND HUMAN RIGHTS 1998: INTERNATIONAL SURVEY OF PRIVACY LAWS AND DEVELOPMENTS (1998). GILC is funded by the Open Society Institute, a foundation created by the financier George Soros.

33. Albert Hirschman has noted that the essence of economic power is the capacity to obstruct commercial exchange. *See* ALBERT HIRSCHMAN, NATIONAL POWER AND THE STRUCTURE OF FOREIGN TRADE 16–17 (1945). A state's large market provides it with leverage over other states' domestic policies because access to its market matters. I refer to this as "market power" because it stems from the threat, implicit or explicit, of a denial of market access. In Hirschman's words: "Thus, the power to interrupt commercial or financial relations with any country, considered as an attribute of national sovereignty, is the root cause of the influence or power position which a country acquires in other countries." *Id.* at 16. He continues:

> What we have called the influence effect of foreign trade derives from the fact that the trade conducted between country A, on the one hand, and countries B, C, D, etc., on the other, is worth *something* to B, C, D, etc., and that they would therefore consent to grant A certain advantages—military, political, economic—in order to retain the possibility of trading with A.

Id. at 17. Because Germany and France had important markets, their threat to cut off data flows to smaller states was significant. Smaller states did not have countervailing leverage. For a description of the important role played by powerful Member States in the raising of environmental standards in the European Union, see VOGEL, *supra* note 9, at 24–97.

34. EU Directive, *supra* note 2, art. 1.

35. *Id.*

European Union could the European Union ensure the "free" transferability of data.

B. *Rights and Obligations: The EU Directive's Regulatory Controls over Data Processing*

The European Union takes more of a legislative approach to data privacy protection than the United States, which relies more on private ordering through market processes.[36] The EU Directive is noteworthy for its broad scope of coverage of private sector activities and its creation of ex ante and ex post controls over business processing and use of personal data. This section provides an overview of the EU Directive's significant protections.

The EU Directive's first striking feature is that—except for public security, criminal law, and related exceptions[37]—it covers all processing of all personal data by whatever means, and is not limited by business sector or field of use.[38] While U.S. regulation of data processing by the private sector is limited to specific sectors and limited categories of information, the EU Directive covers all private sector processing of personal data.[39]

Second, the EU Directive imposes ex ante controls on data "controllers,"[40] setting forth what enterprises must do before they process data. The EU Directive requires controllers to inform the data subject of the "identity of the controller of the data" and its representative (if any), the "purposes of the processing," and other necessary information to ensure fair processing, including the "recipients or categories of recipients of the data," except where the data subject "already" has such information.[41] The data can

---

36. For the U.S. approach, see *infra* Sections II.A–B.

37. The EU Directive does not apply "to processing operations concerning public security, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in area of criminal law." EU Directive, *supra* note 2, art. 3(2). It also does not cover processing operations for "purely personal or household activity." *Id.* EU Member States considered that public security and criminal law matters remain within the sole competence of the Member States. *See id.* art. 13; *see also* Simitis, *supra* note 27, at 453–54. An excellent overview of EU law is provided in JOSEPHINE SHAW, LAW OF THE EUROPEAN UNION (1996).

38. The term "processing" is broadly defined to include "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction." EU Directive, *supra* note 2, art. 2.

39. As regards the United States, see *infra* Section II.B. As regards EU regulation of private sector use of data, as Simitis notes, "it was not the processing of personal data by the government that led to the intervention of the Commission, but rather the collection and retrieval by private enterprises and persons." Simitis, *supra* note 27, at 452.

40. The term "controller" is broadly defined to include any "natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data." EU Directive, *supra* note 2, art. 2(d).

41. *Id.* art. 10. This is all to be done "as early as possible in the relationship and preferably at the first point of contact." MASONS SOLICITORS, HANDBOOK ON COST EFFECTIVE COMPLIANCE WITH THE DIRECTIVE 95/46/EC, at 40 (1998), *available at* <http://europa.eu.int/comm/dg15/en/media/dataprot/studies/masons.htm/europa.eu.int/comm/en/media/datapost> (visited Mar. 30, 1999). This obligation, however, no longer applies where the data subject already has such information. *See id.* This implies that the data subject only needs to be provided such information once, and not each time information is collected from him.

only be processed and used for the purposes specified, so that enterprises are prohibited from even collecting information unnecessary for these purposes.[42]

Some controls, however, are subject to exceptions, providing flexibility for many business operations—more flexibility than many privacy advocates would like.[43] For example, the EU Directive prohibits data controllers from processing information unless the "data subject" "unambiguously" consents to the processing.[44] However, this requirement is subject to five specified exceptions, the last of which is relatively flexible for non-sensitive information used for ordinary servicing of clients.[45]

---

42. *See* EU Directive, *supra* note 2, art. 6. Article 6(1)(b) provides that "personal data must be . . . collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes." *Id.* This is sometimes referred to as the "finality" principle. *See* Colin J. Bennett & Charles D. Raab, *The Adequacy of Privacy: The European Union Data Protection Directive and the North American Response*, 13 INFO. SOC'Y 245, 250 (1997).

43. *See* Simitis, *supra* note 27, at 457. Not surprisingly, affected businesses engaged in considerable lobbying in an attempt to make the EU Directive more flexible. *See* Platten, *supra* note 28, at 27–28.

44. There is some ambiguity in the EU Directive's reference in article 7(a) to "unambiguous" consent, which applies to the processing of *all* information. The term "consent" is defined to mean "any freely given specific and informed indication of [the data subject's] wishes by which the data subject signifies his agreement to personal data relating to him being processed." EU Directive, *supra* note 2, art. 2(h). According to the EU Working Party formed pursuant to article 30 of the EU Directive:

> [B]ecause the consent must be unambiguous, any doubt about the fact that consent has been given would also render the exemption inapplicable. This is likely to mean that many situations where consent is implied (for example, because an individual has been made aware of a transfer and has not objected) would not qualify for this exemption. The exemption could, however, be useful in cases where the transferor has direct contact with the data subject and where the necessary information could be easily provided and unambiguous consent obtained. This may often be the case for transfers undertaken in the context of providing insurance, for example.

Directorate General XV Data Protection Working Party, *Working Document: Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive, adopted* July 24, 1998, at 24 [hereinafter *Transfers of Personal Data to Third Countries*]. One American attorney noted:

> In practice, except for sensitive information as specified in article 8 of the Directive . . . many companies may interpret the term "unambiguous consent" to include only a clearly presented "opt out" right in respect of non-sensitive information, so that individuals must negatively check a box indicating their objection in order to block processing of data about them.

Interview with Scott Blackmer, Partner at Wilmer, Cutler & Pickering, in Washington, D.C. (Mar. 27, 1999) (concerning company practices in light of the EU Directive).

45. The EU Directive provides that, even where unambiguous consent is not obtained, controllers may process information if the processing is (i) "necessary for the performance of a contract to which the data subject is party" (implicitly a form of consent), (ii) "necessary for compliance with a legal obligation," (iii) "necessary in order to protect the vital interests of the data subject," (iv) "necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed," or (v) "necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1(1)." EU Directive, *supra* note 2, art. 7. Under this latter exception, set forth in article 7(f), many companies avoid obtaining consent (or provide only an "opt out" right) for use of non-sensitive information for ordinary servicing of clients. *See* Interview with Scott Blackmer, *supra* note 44. Similarly, Bainbridge writes:

> In the vast majority of cases, controllers will be able to rely on [alternatives] (b) to (f) and will not require the consent of each and every data subject whose personal data are to be processed. That Article 7 suggests that there may be circumstances in which the data subject's consent will be required is misleading and it is difficult to envisage situations

Nonetheless, the EU Directive specifically requires that individuals "be informed before personal data are disclosed for the first time to third parties for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses."[46] The data controller or his representative must expressly inform the individual of the identity of the parties or categories of parties to which the data may be sold or the consent is deemed invalid.[47] So informed, individuals are less likely to grant consent.

Moreover, where sensitive information is at stake, Member States must prohibit processing or require that processing may only take place if the individual "opts in" to the processing, such as actively checking a box indicating his or her agreement.[48] This covers all "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of data concerning health or sex life."[49] The EU Directive also grants individuals the right to challenge any decision significantly affecting him or her that is based on an automatic processing of data, including decisions involving creditworthiness or employment.[50]

---

where one of the conditions in (b) and (f) does not apply.

David Bainbridge, *Legal Analysis of the Directive*, *in* EC DATA PROTECTION DIRECTIVE, *supra* note 28, at 35, 54 [hereinafter Bainbridge, *Legal Analysis*]. Even Bainbridge, however, subsequently states that "[t]he data subject's consent under Article 7(a) will be required where disclosure is made for other purposes, such as by passing on the data subject's details to an associated company or third party for the purposes of marketing." David Bainbridge, *Banking and Financial Services*, *in* EC DATA PROTECTION DIRECTIVE, *supra* note 28, at 153, 159 [hereinafter Bainbridge, *Banking*]. Moreover, Member State officials may interpret the term "necessary" (used in each of the above listed alternatives) in a more limiting manner than does Bainbridge.

In addition, the EU Directive provides that Member States may restrict the scope of protections where necessary to safeguard national security, defense, public security, an important economic or financial interest of a Member State, the data subject, or the rights and freedoms of others. *See* EU Directive, *supra* note 2, art. 13(1). For a discussion of these exceptions, see Simitis, *supra* note 27, at 457.

46. EU Directive, *supra* note 2, art. 14(b). In other words, even if individuals grant informed consent to the processing of personal information, at which time they are informed of the recipients or categories of recipients of the data, they may still subsequently object (i.e., opt out) of the transfer of this information for direct marketing purposes. *See Transfers of Personal Data to Third Countries*, *supra* note 44, at 7.

47. *See* EU Directive, *supra* note 2, art. 10(c). Bainbridge, however, argues that it may be sufficient simply to raise awareness among consumers of their right to apply to have their names removed from mailing lists under a "mailing preference scheme." Bainbridge, *Legal Analysis*, *supra* note 45, at 66; *see also* David Bainbridge, *Perspectives on the Directive: Recipients and Third Parties*, *in* EC DATA PROTECTION DIRECTIVE, *supra* note 28, at 115, 148–49.

48. *See* EU Directive, *supra* note 2, art. 8(1). This absolute prohibition is, however, subject to certain limited exceptions. The most important of these is set forth in article 8(2), which provides: "Paragraph 1 shall not apply where: (a) the data subject has given his *explicit consent* to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent." EU Directive, *supra* note 2, art. 8(2) (emphasis added). The term "explicit" consent is understood to require that an individual must clearly grant consent by "opting in" to the scheme. *See* Interview with Scott Blackmer, *supra* note 44.

49. EU Directive, *supra* note 2, art. 8(1).

50. Article 15(1) provides:

> Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct,

Third, the EU Directive imposes ex post controls on enterprises, granting individuals rights to monitor and challenge the use of personal information after it is processed. The EU Directive guarantees individuals a permanent right of access, without constraint or excessive delay or expense, to obtain copies of the data about them, have it corrected, and receive confirmation of the purposes of the processing and the identity of third-party recipients or categories of recipients.[51] Individuals are thus enabled to trace which third parties hold personal information about them, verify how they are using it, and enjoin uses that do not conform to those specified in the controller's initial notice.

Finally, the EU Directive grants individuals significant enforcement rights.[52] The EU Directive requires Member States to provide a judicial remedy for infringements of data privacy rights, including the right to receive damages.[53] Individuals can also challenge the data's accuracy and collection procedures and block its further processing and transfer.[54] To support effective enforcement, Member States must designate an independent public authority "responsible for monitoring the application within its territory" of the EU Directive's provisions.[55] Supervisory authorities are granted significant powers, including the power to investigate processing operations, to deliver "opinions before processing operations are carried out," to order "the blocking, erasure or destruction of data," to impose "a temporary or definitive ban on processing," and "to engage in legal proceedings" against violators of the rights guaranteed by the EU Directive.[56] Individuals and consumer advocacy groups have the right to lodge claims before supervisory authorities, which must investigate them and inform the complainant of the investigation's

---

etc.

Id. art. 15(1).

51. *See id.* art. 12. Bainbridge, however, points out that in the United Kingdom data users can charge a fee of up to £10 which can act "as a large disincentive" for individuals to seek access. Bainbridge, *Legal Analysis*, *supra* note 45, at 78.

52. Enforcement of the EU Directive will inevitably determine how effective it will be in accomplishing privacy advocates' practical goals. There is evidence of enforcement under prior Member State laws. *See supra* note 27. Section V.B, *infra*, points out additional ways in which the EU Directive may be implemented.

53 *See* EU Directive, *supra* note 2, arts. 22–23.

54. *See id.* art. 12.

55. *Id.* art. 28.

56. *Id.* In addition, the controller must notify the national supervisory authority before conducting any automatic processing unless the "categories of processing operations . . . are unlikely . . . to affect adversely the rights and freedoms of the data subjects," or where the controller "appoints a personal data protection official" in compliance with national legal requirements. *Id.* art. 18. The contents of the notification are specified in article 19 and include, at a minimum, the name and address of the controller, the purpose of the processing, a description of the data or categories of data to be processed, the recipients or categories of recipients to whom the data may be processed, any proposed transfers of data to third countries, and measures to ensure the data's security. *See id.* art. 19. Member States are to "determine the processing information likely to present specific risks to the rights and freedoms of data subjects," and "check that these processing operations are examined prior to the start thereof." *Id.* art. 20. Processing operations subject to prior notification must be publicized in a national register maintained by the supervising authority and be subject to inspection by any person. *See id.* art. 21.

outcome.[57] Sanctions may, depending on Member State law, include civil and criminal fines and imprisonment.[58]

C. *Privacy at a Price: The Costs of EU Requirements on European Business Operations*

Regulation is not without cost. Existing data privacy requirements in certain Member States already impose costs on businesses operating in them. The EU Directive attempts to ensure that these costs will be imposed throughout the European Union, and potentially throughout the world. From the perspective of U.S. businesses, the EU Directive threatens not only U.S. sovereignty; more fundamentally, it constrains the sovereignty of private business decision-making.

First, the EU Directive requires businesses to retain detailed information concerning the data's use and to respond promptly to all inquiries concerning it. This demands personnel time, including time to review and revise all company practices, retain records, and respond to client information requests. The British Bankers' Association (BBA) has maintained that simply compiling and safeguarding the required information and providing it to inquiring customers will cost each major bank on average "in excess of 150 pounds" per customer request and that, in aggregate, the provision of such information to customers will cost each bank "millions" of pounds.[59] The Commission, on the other hand, appointed independent consultants to conduct a detailed cost-benefit study, which concluded that the financial impact would be minimal.[60]

Second, where informed consent is required, individuals may refuse to grant it. If most consumers refuse to grant consent they could in theory be worse off collectively because enterprises would have less information in determining how to tailor goods and services at low cost to satisfy consumers' desires. In other words, consumers could face a collective action problem. They could, in theory, collectively benefit if all provide personal information

---

57. *See id.* art. 28(4).

58. The nature of the sanctions will be defined by national law. The EU Directive merely requires Member States to impose sanctions for infringement of the national provisions implementing the EU Directive. *See id.* art. 24.

59. *See* FRED CATE, PRIVACY IN THE INFORMATION AGE 42–43 & n.64 (1997) (citing The Home Office Consultation Paper on the Implementation of the EU Data Protection Directive—The British Bankers' Association Response, Annex I (costs)). Marc Rotenberg of EPIC counters that credit reports mandated by the Federal Credit Reporting Act are available in the United States for US $8. *See* Telephone Interview with Marc Rotenberg, EPIC (Apr. 14, 1999); *see also* Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681j(a)(1)(a)(i) (1994) (limiting the charge to "not exceed $8").

60. *See* David Bainbridge, *Preface* to EC DATA PROTECTION DIRECTIVE, *supra* note 28, at vii–viii (referring to the Commission's solicited study); Pearce & Platten, *supra* note 25, at 537. While businesses will incur additional transaction costs in adapting to new consent requirements, these should be minor and short-term. Such transaction costs would include the costs of creating and using new consent forms and purchasing software to differentiate between consenting and non-consenting individuals in respect of type of use and/or onward transfer of personal information.

to producers, but most might refrain because of a low but potentially catastrophic risk to a few.[61]

Third, where individuals withhold consent, businesses seek to obtain information through more costly means.[62] By impeding businesses from obtaining information, more stringent privacy protection reduces their efficiency. For example, privacy protection makes it more difficult for firms to obtain information about job applicants' past performance.[63] Privacy protection can also reduce enterprises' ability to make quick, informed contracting decisions, such as whether to grant customers credit. The EU Directive not only increases businesses' transaction costs to obtain information, but it also reduces businesses' productivity when they fail to obtain it, resulting in increased operating costs.

Fourth, where individuals object to the processing and transfer of personal data, businesses forego revenue from its sale to direct marketing companies. Direct marketing companies, which depend on personal data sales, similarly lose revenue from selling this data to other commercial enterprises. These opportunity costs are reflected in a comparison of revenue generated from direct marketing in Europe and the United States. In 1997, direct marketing sales in the United States exceeded $1.2 trillion dollars, almost ten times the amount of direct marketing sales in Europe, which totaled approximately $125 billion dollars.[64] The U.S. direct marketing industry

---

61. A majority of individuals could refuse to grant consent because of a small risk of major harm resulting from an infringement of their privacy. There are, however, significant weaknesses in this argument. First, this collective action problem is mitigated through the payment of consideration for personal information. Individuals will usually provide information for a price, thereby obtaining some of the profit for themselves. *See infra* note 74 and accompanying text. Second, to the extent that producers used the information to engage in price discrimination, some consumers would benefit and others would be prejudiced. Third, where producers operate in a monopolistic or oligopolistic market, they can maintain higher prices and retain all or much of the increased profit for themselves. Fourth, individuals face risks other than such catastrophic risks as impaired reputation, job dismissal, or rejection of insurance coverage. Many individuals object to the nuisance of being bombarded with unsolicited marketing information, whether by phone or mail.

62. Businesses may still be able to "get the information they need," but only "if they can afford the expense." Stephen Baker, *Europe's Privacy Cops*, BUS. WK., Nov. 2, 1998, at 20.

63. As Judge Richard Posner writes:

> Much of the demand for privacy . . . concerns discreditable information concerning past or present criminal activity or moral conduct at variance with a person's professed moral standards. And often the motive for concealment is . . . to mislead those with whom he transacts. Other private information that people wish to conceal, while not strictly discreditable, would if revealed correct misapprehensions that the individual is trying to exploit.

Richard A. Posner, *The Right to Privacy*, 12 GA. L. REV. 393, 399 (1978). Posner takes a utilitarian perspective on privacy. He implies that the primary rationale for individuals to demand privacy protection is to achieve instrumental goals of influencing others. Posner's conception does not recognize a non-utilitarian interest in retaining one's sense of personhood and autonomy. The utilitarian argument for not recognizing privacy can also be turned on its head. That is, it can be argued that privacy protection is required so that individuals will not be manipulated by others, especially by powerful business interests.

64. *See* Thomas Weyr, *Merger To Give DM Industry Stronger Voice in Europe*, DM NEWS, May 12, 1997, at 8; *see also* Jeff Wilkins, *Internet Direct Marketing*, E-BUS. ADVISOR, Sept. 1, 1998, at 32. The Direct Marketing Association (DMA) refers to the figure of "nearly $1.4 trillion in annual sales here in the United States" for 1998. *The DMA Submits Comments, Concerns on 'Safe Harbor' for Data Flows Between United States and Europe*, PR NEWSWIRE, Nov. 19, 1998. The DMA notes that

reportedly grew by seven percent in 1998 and expects to maintain a seven percent annual growth through 2002.[65] The EU direct marketing industry and its growth prospects are minute in comparison.[66]

To some commentators, the EU Directive views privacy as a "fundamental right[] and freedom[]"[67] that overrides commercial concerns over regulatory costs. As Spiros Simitis, a former data protection commissioner in the German state of Hesse and chair of the Council of Europe's Data Protection Experts Committee, states, "when we speak of data protection within the European Union, we speak of the necessity to respect the fundamental rights of the citizens. Therefore, data protection may be a subject on which you can have different answers to the various problems, but *it is not a subject you can bargain about.*"[68]

The concept of "fundamental rights," however, is problematic when advocates give "rights" an infinite value, eliminating the possibility of any cost-benefit analysis involving competing values. These values could include commercial property interests, efficiency concerns, the availability of low-cost goods and services, freedom of expression, protection against crime, and other matters for legislatures, regulators, courts, and markets to take into account.[69] Moreover, the "non-negotiability" of rights both reduces efficiency and raises equity concerns. Efficiency is reduced because privacy interests are not balanced against other societal concerns, including access to low-cost goods. Equality can be undermined to the extent those with privileged access to information can disproportionately benefit when information is not readily available. In addition, with second-best information, individuals may base

---

telemarketing ($58 billion in sales in 1997) and direct mail ($37 billion in sales in 1997) are the most successful forms of direct marketing. *See* Wilkins, *supra*; *see also* DIRECT MKTG. ASS'N, ECONOMIC IMPACT: U.S. DIRECT MARKETING TODAY, 1998 UPDATE 11 (1998) (on file with author) (maintaining that, in 1998, 24.6 million workers were "employed throughout the U.S. economy as a result of direct marketing activities").

65. *See Direct Hit*, ECONOMIST, Jan. 9, 1999, at 55 (noting that "the industry was worth $163 billion in 1998" in the North American market). Direct marketing constituted almost three-fifths of all U.S. spending on advertising in 1998. *See id.*

66. While other factors, including cultural influences and other relevant legislation such as the EC Distant Selling Directive, *see* Parliament Directive 97/7/EC, 1997 O.J. (L 144) 19 (May 20, 1997), may contribute to the discrepancy, data privacy protection regulations surely hamper direct marketing activities in Europe.

67. EU Directive, *supra* note 2, art. 1. There has been much debate about what the "right" protects. In his classic work *Privacy and Freedom*, Alan Westin defines the term "information privacy" to mean "the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others." ALAN WESTIN, PRIVACY AND FREEDOM 7 (1967). The multiple, competing purposes behind data protection goals, including such humanistic concerns as protecting personal autonomy and integrity, are presented in BENNETT, *supra* note 32, at 22–37. *See also* REGAN, *supra* note 1, at 24–42, 212–43 (critiquing purely individualistic grounds for protecting privacy and offering complementary collective social grounds).

68. Spiros Simitis, Unpublished Address on Information Privacy and the Public Interest (Oct. 6, 1994), *quoted in* CATE, *supra* note 59, at 42 (emphasis added).

69. As for the need to balance competing social concerns, see generally AMITAI ETZIONI, THE LIMITS OF PRIVACY (1999). For example, while privacy advocates protested against Microsoft's use of a serial number in Microsoft Office documents as a threat to individual privacy, it was a Microsoft serial number that allegedly permitted law enforcement officials to trace the transmission of the "Melissa" computer virus to a software programmer in New Jersey. *See* John Markoff, *When Privacy Is More Perilous Than the Lack of It*, N.Y. TIMES, Apr. 4, 1999, at 3.

decisions on stereotypes, prejudicing those from a particular race or ethnic group.[70]

In practice, the EU Directive balances other concerns against privacy interests. The EU Directive creates exceptions for concerns such as "public security, defense, State security . . . and the activities of the State in areas of criminal law."[71] The EU Directive also provides for "exemptions or derogations" for "processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression,"[72] as well as a limited exception for scientific research.[73] Privacy rights advocates nonetheless tend to employ a fundamental rights discourse to attempt to enhance the relative importance of their concerns vis-à-vis others. The debate should be over the relative importance of privacy values compared to others, and the role of individual participation in decisions concerning their personal information.

There are, in short, identifiable costs to recognizing stringent data privacy rights, both in terms of efficiency and equity. For businesses, these costs include compliance, transaction, operating, and opportunity costs. Businesses ultimately factor these costs into the prices charged consumers. The prices of goods and services on the EU market are, in principle, higher on average than they would be without the EU data privacy requirements. As addressed in Part II, however, businesses' unregulated exploitation of personal data arguably poses much severer equity and efficiency concerns. Moreover, rules facilitating individual participation and the pricing of information mitigate these equity and efficiency concerns.[74]

---

70. The EU Directive places specific limits on "the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs." EU Directive, *supra* note 2, art. 8. It thereby attempts to limit decision-making based on the use of such stereotypes. Moreover, the lack of privacy protection arguably facilitates the creation of racial and ethnic profiles based on stereotypes. In practice, businesses are using personal data to create these very racial and ethnic profiles. *See infra* note 100 and accompanying text.

71. EU Directive, *supra* note 2, art. 3(2).

72. *Id.* art. 9.

73. *See id.* art. 13(2).

74. If paid for their personal information, consumers are more likely to consent to its transfer. Consideration can take many forms, including cash discounts, rebates, increased services, and warranties. By imposing a requirement that businesses receive the prior informed consent of individuals before processing personal information, the EU Directive may facilitate this pricing of personal information. Such pricing stimulates efficiency gains where businesses internalize privacy costs in the price of goods sold. Pricing also shifts some of the benefits from exploiting personal information to individuals. This distributional shift is arguably more equitable. Nonetheless, manipulation of individuals through gift offers still raises concerns. *See, e.g.*, *Direct Ripples Flow into a Steady Stream*, PRECISION MARKETING, Aug. 16, 1999, at 10 (stating that discounts, gifts, and sweepstakes have encouraged wary Hungarian consumers to divulge information); Robert D. Hof et al., *A New Era of Bright Hopes and Terrible Fears: Companies That Can "Blast You Out of Your Place" Abound*, BUS. WK., Oct. 4, 1999, at 84 (describing the personalized coupons that supermarkets give to customers who use loyalty cards that collect information); Jeff Kunerth, *Trust, Privacy Endangered: Society's Advances in Technology Could Threaten Way of Life*, HOUS. CHRON., Aug. 22, 1999, at 16 (giving examples of computers, Internet access, and e-mail accounts being given to people who release data).

D. *Exporting Privacy Protection: The EU's Threat To Ban Data Transfers to the United States*

Article 25 of the EU Directive provides that the European Commission may decide, upon approval of a qualified majority vote of Member States,[75] to prohibit all data transfers to a third country, including the United States, if the Commission finds that the third country does not ensure "an adequate level of protection" of data privacy rights.[76] The meaning of the term "adequate" is not defined in the EU Directive, but is to be determined on a case-by-case basis. Pursuant to the EU Directive, the European Union formed a "Working Party for the Protection of Individuals with Regard to the Processing of Personal Data" to examine and report on the adequacy of third-country protections.[77]

---

75. The decision-making processes are set forth in article 31 of the EU Directive, which in turn refers to decisions by a qualified majority vote (QMV) of Member State representatives pursuant to the EC Treaty (as amended). *See* EU Directive, *supra* note 2, art. 31. Under this system, votes on decisions to be taken by QMV are weighted per country, so that larger countries such as Germany have more votes than smaller ones. Article 205 of the Treaty (article 148 at the time of the EU Directive's adoption) sets forth the number of votes that each Member State holds in the Council, and the number of votes required to adopt an act by QMV. *See* EC Treaty, *supra* note 2, art. 205. Sixty-one out of a total of 87 votes are required to pass an act by QMV following a Commission proposal. *See id.* Article 31 provides, in relevant part:

> 1. The Commission shall be assisted by a committee composed of the representatives of the Member States and chaired by the representative of the Commission.
> 2. The representative of the Commission shall submit to the committee a draft of the measures to be taken. The committee shall deliver its opinion on the draft within a time limit which the chairman may lay down according to the urgency of the matter.
> The opinion shall be delivered by the majority laid down in Article 148(2) of the Treaty [i.e. by QMV] . . . .
> The Commission shall adopt measures which shall apply immediately. However, if these measures are not in accordance with the opinion of the committee, they shall be communicated by the Commission to the Council forthwith. In that event:
> - the Commission shall defer application of the measures which it has decided for a period of three months from the date of communication,
> - the Council, acting by qualified majority, may take a different decision within the time limit referred to in the first indent.

EU Directive, *supra* note 2, art. 31.

This text implies that, if the Council fails to take a different decision by QMV within three months, the Commission may proceed to apply the measures that it has decided upon. In practice, however, it is doubtful that the Commission would act without the support of a qualified majority of Member States.

76. Article 25 is quoted in full in *supra* note 3. The United States is not specifically cited in the EU Directive. However, given the size of the U.S. market, the widespread use of data in the United States, the lack of comprehensive data privacy legislation in the United States, and the fact that the United States is the EU's largest trading partner, the European Union first entered into negotiations with the United States over data privacy protection standards and these negotiations have been by far the most intensive. The European Union is nonetheless also in discussions with other countries, particularly Japan. *See* Interview with Dr. Ulf Bruehann, Head of Unit on Free Movement of Information, Data Protection, and Related International Aspects DG XV, European Commission, in Brussels, Belg. (June 23, 1999).

77. The Working Party was formed pursuant to article 29 of the EU Directive. The duties of the Working Party are spelled out in article 30, which provides, in part:

> 1. The Working Party shall:
> (a) examine any question covering the application of the national measures adopted under this Directive in order to contribute to the uniform application of such

The Working Party, comprised of data protection commissioners from each EU Member State and members of the Commission, prepared a Discussion Document,[78] dated June 26, 1997, that identifies core principles under which the adequacy of a country's protections should be gauged. These principles, which are in line with the EU internal requirements, include the following: processing must be limited to a specific purpose; the purpose must be made known to the concerned individual, together with other information to ensure fair processing; the individual must have access to the data and the right to object to its processing; the individual must have procedural mechanisms available to enforce the protections effectively; the third-country data recipient must be prohibited from transferring the information to other countries that, in turn, do not afford "adequate" levels of protection.[79] Only countries whose data processing laws are found to be adequate will be placed on a "white list," and thereby shielded from the potential of a ban imposed on all transfers of personal data.[80]

II. U.S. DATA PRIVACY PROTECTION: DOES IT FAIL TO MEET THE EU DIRECTIVE'S CRITERIA?

Unlike the broad scope of coverage and the centralized standard-setting and enforcement features of the EU Directive, data privacy regulation in the United States is fragmented, ad hoc, and narrowly targeted to cover specific sectors and concerns. It is decentralized and uncoordinated, involving standard setting and enforcement by a wide variety of actors, including federal and state legislatures, agencies and courts, industry associations, individual companies, and market forces.[81] To a certain extent, the U.S. handling of data

---

measures;

(b) give the Commission an opinion on the level of protection in the Community and in third countries;

(c) advise the Commission on any proposed amendment of this Directive, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data and on any other proposed Community measures affecting such rights and freedoms;

(d) give an opinion on codes of conduct drawn up at Community level.

EU Directive, *supra* note 2, art. 30(1).

78. Since the EU Directive's signature, the Working Party on the Protection of Individuals has prepared a series of Discussion Documents giving its opinion on matters under the EU Directive relevant to third-country transfers. In July 1998, it incorporated these in its Working Document entitled *Transfers of Personal Data to Third Countries*, *supra* note 44.

79. *See id.* at 6.

80. *See* Al Gidari & Marie Aglion, *EU Directive on Privacy May Hinder E-Commerce*, NAT'L L.J., June 29, 1998, at B7 (referring to the "white list"). A general ban would nonetheless be subject to case-by-case exceptions upon a company's acceptance of specific conditions safeguarding the data subject's primary interests. *See infra* notes 225–226 and accompanying text.

81. The fragmented, decentralized nature of the U.S. regulatory process is described in STEVEN VOGEL, FREER MARKETS, MORE RULES: REGULATORY REFORM IN ADVANCED INDUSTRIALIZED COUNTRIES 217 (1996). As one *New York Times* correspondent states, the U.S. regulation of data privacy consists of "a hodgepodge of statutes and regulations enforced by various state and Federal agencies charged with oversight of other industries." Edmund L. Andrews, *European Law Aims To Protect Privacy of Personal Data*, N.Y. TIMES, Oct. 26, 1998, at A1.

privacy issues reflects Americans' traditional distrust of a centralized government.[82] United States legislation provides citizens with significantly greater protection against the collection and use of personal information by government, in particular the federal government, than by the private sector. While the EU Directive imposes legislation to condition market interactions, the United States relies less on government intervention in the private sector and more on market constraints.

This part begins with an overview of U.S. legal protection against data processing by government (Section A) and by the private sector (Section B), noting the problems with this public-private distinction (Section C). It then addresses, from a comparative institutional standpoint, the role of markets, legislatures, and courts in the regulation of data privacy protection in the United States (Section D). It concludes by examining the need for comparative institutional analysis to take account of extra-jurisdictional impacts on the operation of national institutions (Section E).

A. *U.S. Protections Against Data Processing by Government*

The Privacy Act of 1974 is the only federal omnibus act that protects informational privacy.[83] Yet despite the legislation's broad title, the Privacy Act only applies to data processing conducted by the federal government, not by state governments or the private sector. The Privacy Act obliges federal agencies to collect information to the greatest extent possible directly from the concerned individuals, to retain only relevant and necessary information, to maintain adequate and complete records, to provide individuals with a right of access to review and have their records corrected, and to establish safeguards to ensure the security of the information.[84] The Privacy Act also requires

82. In his analysis of American regulation, Bob Kagan discusses how it has been shaped by particular aspects of American culture, including "(1) a political culture that continues to reflect deep mistrust of governmental and business power, and (2) political structures—separation of powers, politically divided government, loosely disciplined political parties—that fragment governmental and Congressional power." Bob Kagan, *Introduction* to REGULATORY ENCOUNTERS: MULTINATIONAL CORPORATIONS AND AMERICAN ADVERSARIAL LEGALISM 16 (Bob Kagan & Lee Axelrad eds., 1998) (manuscript, on file with author) [hereinafter Kagan, *Regulatory Encounters*]. Kagan finds that the U.S. "style" of regulation is "uniquely legalistic, adversarial, and expensive." *Id.* at 3; *see also* Bob Kagan, *Adversarial Legalism and American Government*, *in* THE NEW POLITICS OF PUBLIC POLICY 88 (Marc Landy & Martin Levin eds., 1995) [hereinafter Kagan, *Adversarial Legalism*]. As discussed below, however, whereas the fragmented nature of U.S. data privacy regulation comports with Kagan's analysis (involving uncoordinated federal, state, and bureaucratic issue-specific, ad hoc approaches), there are large areas where there is no data privacy regulation. Such lack of regulation cannot be described as "legalistic," even though the lobbying efforts of business and privacy advocates are certainly "adversarial." *Cf.* Fred Cate, *Privacy and Telecommunications*, 33 WAKE FOREST L. REV. 1, 34 (1998) (referring to discussion of American "distrust of powerful central government").

83. 5 U.S.C. § 552a (1994). In addition, the Freedom of Information Act provides important safeguards to third-party access to federal records. Although the primary focus of the Act is to provide public access to federal government records, it contains exceptions to the release of information about private individuals contained in such records. *See* 5 U.S.C. § 552 (1994).

84. *See* 5 U.S.C. § 552a. However, the Privacy Act contains a significant exception in the form of the "routine use exception" that permits federal agencies to transfer information between themselves for what they justify as a "routine use." 5 U.S.C. § 552a(b)(3). Paul Schwartz and Joel Reidenberg critique the "routine use" exception to the 1974 Privacy Act as a loophole that permits

federal agencies to designate a "Privacy Act official" to oversee their compliance with the Act's requirements, as well as "Data Integrity Boards" to review inter-agency data matching activities.[85]

Because of the U.S. federal system, the Privacy Act does not apply to the states. The vast majority of states lack omnibus privacy acts,[86] and instead offer scattered statutes applying to specific sectors or concerns, such as the regulation of "access to educational records and child abuse data banks."[87] Except for certain issue-specific legislation that is federally mandated,[88] there is little uniformity of state law, resulting in fifty different jurisdictions with distinct regimes. While provisions of the U.S. Constitution have been held to offer some privacy guarantees against actions of state and federal government officials, the coverage is quite limited and once more only applies to government action, not private action.[89]

B. *U.S. Protections Against Data Processing by the Private Sector*

Unlike the European Union, the United States provides no generalized protection to individuals from the processing of personal information by the private sector. Congress has limited federal privacy protection to discrete sectors and concerns, as depicted in the following statutory titles: the Driver's

---

almost "any use" of personal data by any federal agency once obtained. *See* PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW: A STUDY OF UNITED STATES DATA PROTECTION 94–100 (1996).

85. *See* 5 U.S.C. §§ 552a(r), (u)(3). Commentators, however, find that the oversight practices of the Privacy Act officials and Data Integrity Boards are of limited effectiveness. *See* SCHWARTZ & REIDENBERG, *supra* note 84, at 120.

86. In 1996, Schwartz and Reidenberg reported that "only thirteen states have general statutes that establish fair information practices for the government's processing of personal information." *Id.* at 131. These states were Alaska, California, Connecticut, Hawaii, Indiana, Massachusetts, Minnesota, New Hampshire, New York, Ohio, Utah, Virginia, and Wisconsin. *See id.*

87. *Id.* at 130.

88. For an example of a federal mandate, a federal statute now requires states to permit drivers to opt out of having their motor vehicle registration information sold to third parties, such as direct marketers. *See* 18 U.S.C. § 2721 (1994). The State of Michigan raised over a half-million dollars through such sales in 1993. *See* Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 612 (1995).

89. Only the Thirteenth Amendment's prohibition of slavery applies directly to private parties. All other constitutional rights apply only to actions by governmental officials. The Fourteenth Amendment forbids states from "depriv[ing] any person of life, liberty or property, without due process of law," and has been held by the U.S. Supreme Court to render most of the Bill of Rights binding on the states. However, it does not apply to actions of private persons. In consequence, only the federal and state governments are bound by constitutional provisions implicating privacy interests, such as First Amendment rights to freedom of expression and association, the right to vote, and the Fourth Amendment's protection against unreasonable searches and seizures, as well as the Supreme Court's recognition of a limited right to informational privacy under the due process clauses in the Fifth and Fourteenth Amendments. The central case on informational privacy is *Whalen v. Roe*, 429 U.S. 589 (1977). *Whalen* concerned a New York law that created a central file of persons who obtained prescription drugs. While the U.S. Supreme Court recognized an "individual interest in avoiding disclosure of personal matters" and an "interest in independence in making certain kinds of important decisions," it applied a lower level of scrutiny to the state law and found that the New York statute did not "pose a sufficiently grievous threat to either interest to establish a constitutional violation." *See Whalen*, 429 U.S. at 599–600; *see also* SCHWARTZ & REIDENBERG, *supra* note 84, at 76 (discussing *Whalen* and subsequent lower court decisions).

Privacy Protection Act of 1994,[90] the Videotape Privacy Protection Act of 1988,[91] the Electronic Communications Privacy Act of 1986,[92] the Cable Communications Policy Act of 1984,[93] and the Fair Credit Reporting Act of 1971.[94] Rather than engage in a concerted effort to protect individual privacy, in most cases, Congress has simply reacted to public scandals. In passing the Fair Credit Reporting Act, Congress responded "to consumer horror stories of dealings with credit reporting agencies."[95] The Driver's Privacy Protection Act "was inspired by the murder of an actress . . . who was tailed by a stalker who obtained her address . . . from state driver's license records."[96] Congress enacted the Video Privacy Protection Act after the video rental records of Judge Robert Bork were obtained and published by a news reporter in the course of a campaign against his Supreme Court nomination.[97] As a result, in the United States, "video rentals are afforded more federal protection than are medical records."[98]

---

90. 18 U.S.C. § 2721 (1994) (regulating the dissemination of personal information held by departments of motor vehicles).

91. 18 U.S.C. § 2710 (1994) (prohibiting the disclosure of film titles rented by specific customers and requiring the destruction of personally identifiable information within a year of collection). This Act is under challenge before the U.S. Supreme Court. *See The Supreme Court on Privacy*, N.Y. TIMES at 14 (Nov. 14, 1999) (concerning the Supreme Court's review of *Condon v. Reno*, 155 F.3d 453 (4th Cir. 1998), *cert. granted*, 67 U.S.L.W. 3588 (U.S. May 17, 1999) (No. 98-1464) (appeal of the Fourth Circuit's ruling that the Driver's Privacy Protection Act is unconstitutional)).

92. Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.). The Electronic Communications Privacy Act of 1986, among other matters, prohibits unauthorized third-party eavesdropping and recording of telephone conversations. Its prohibition of the disclosure by telecommunication service providers of the contents of communications over their networks is subject to a significant exception. Disclosure may occur upon the consent of any one of the parties to that communication. *See* 18 U.S.C. § 2511 (1994).

93. 47 U.S.C. § 551 (1994) (requiring subscribers' cable television records to be kept confidential).

94. 15 U.S.C. § 1681 (1994). The Fair Credit Reporting Act (FCRA) governs the disclosure of credit information by credit bureaus. Under the FCRA, credit information may only be provided to those businesses with a legitimate need for it. The individual must have access to the information and be able to have it corrected. If ever credit is denied to a person on the basis of a credit report, the person must be informed of the reason for denial and the identity of the credit report in question. *See id.*

95. CENTER FOR PUBLIC INTEGRITY, NOTHING SACRED: THE POLITICS OF PRIVACY 14 (1998) [hereinafter NOTHING SACRED] (noting, for instance, that a newspaper reporter's insurance was canceled because a private investigator fabricated a report that he was a "hippie type" who was "suspected of being a drug user by neighbors," it being subsequently determined that the report was fabricated).

96. *The Supreme Court on Privacy*, *supra* note 91.

97. *See* Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 506 n.48 (1995) (noting the "public outrage" when Judge Bork's "video rental records . . . were publicized").

98. SHERI ALBERT, SMART CARDS, SMARTER POLICY: MEDICAL RECORDS, PRIVACY AND HEALTH CARE REFORM 13 (1993). While the Video Privacy Protection Act prohibits the disclosure of video rental records, there is no comparable federal legislation regulating the handling of medical records. State laws and industry "self-regulation" are limited at best. *See id.* As Mark Hudson, a former insurance company employee, states, "I can tell you unequivocally that patient confidentiality is not eroding. It can't erode because it's simply nonexistent." Bob Herbert, *What Privacy Rights?*, N.Y. TIMES, Sept. 27, 1998, at 15 (quoting Hudson). The Clinton Administration has, however, proposed new regulations to protect the privacy of medical records. The proposed regulations are now subject to notice and comment with a finalized version intended to be adopted as law by Feb. 21, 2000. *See* Robert Pear, *Rules of Privacy on Patient Data Stir Hot Debate*, N.Y. TIMES, Oct. 30, 1999, at A1. The proposed rules are nonetheless critiqued for failing to require patient consent for health plans and insurance companies to use such information. *See id.*

While U.S. data privacy protection may be adequate under EU standards in some sectors, it was thought inadequate in most.[99] Individuals have little or no privacy protection in unregulated sectors. From an ex ante perspective, the United States does not require an individual's consent to the processing, marketing, and sale to third parties of personal information. From an ex post perspective, individuals have no access to processed information and cannot challenge its accuracy or use before a court or administrative body. Congress has, in particular, kept its hands off the powerful direct marketing industry. As a result, enterprises can freely compile, mix, match, buy, sell, and trade profiles and dossiers covering an individual's purchasing proclivities; physical, emotional, and mental conditions; ethnic identity; political opinions; and moral views.[100] As one direct marketer boasts, its profiles "make it easy to keep up with the Joneses, as well as the Johnsons, the Francos, the Garcias, the Wongs and all the others."[101] The attitude of many U.S. businesses is encapsulated in the remarks of the chairman and chief executive of Sun Microsystems: "You already have zero privacy—get over it."[102]

Even where information is covered by U.S. legislation, no central administrative agency monitors compliance. In the United States, a hodgepodge of federal agencies oversee privacy issues relating to disparate sectoral and issue-specific concerns. Responsible agencies include the Federal Trade Commission, the Office of Consumer Affairs, the Office of Management and Budget, the Office of the Comptroller of the Currency, the Social Security Administration, the Department of Health and Human Services, the Internal Revenue Service, the Federal Reserve Board, and the National Telecommunications and Information Administration.[103] To date, these agencies do not coordinate their data privacy oversight.[104]

---

99. A sector-by-sector analysis of U.S. data privacy protection is contained in SCHWARTZ & REIDENBERG, *supra* note 84. The book was prepared for the European Commission by two American professors working in the area of data protection law. Schwartz and Reidenberg suggest that U.S. data protection of health records and of records transferred by data marketing industries is particularly suspect. *See id.* at 155–66, 308; *see also* PETER SWIRE & ROBERT LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE 170–72 (1998). Swire and Litan note that U.S. data privacy protection in the areas of human resources/employment information, health information, data marketing, and insurance is relatively lax and is of concern to EU authorities, whereas U.S. data privacy protection in the areas of credit histories, student records, and cable and video rental records should be of less concern to EU authorities. *See id.*

100. Direct marketing companies may compile profiles of an individual's ethnicity, political perspectives, sexual preferences, sexual potency, purchasing habits of undergarments, views on abortion, and health problems. To do this, they gather information from diverse sources, including registration records, business files, credit card purchases, warranty applications, and other places. *See* Reidenberg, *supra* note 97, at 518–23.

101. *Id.* (quoting an advertisement of a Claritas profiling product, DM NEWS, May 23, 1994, at 26). Schwartz and Reidenberg note the large market for the secondary use of health information. They affirm that one of the primary reasons for the acquisition by Merck & Co., "the world's largest pharmaceutical company," of Medco Containment Services, the U.S.'s "largest mail order pharmacy," was to obtain access to Medco's collection of personal medical data for marketing purposes. SCHWARTZ & REIDENBERG, *supra* note 84, at 168.

102. John Markoff, *Growing Compatibility Issue: Computers and User Privacy*, N.Y. TIMES, Mar. 3. 1999, at A1 (quoting Sun Microsystems chairman and chief executive Scott McNealy).

103. *See generally* Barbara S. Wellbery, *"For Your Eyes Only" . . . Means What in the Cyber Age? The Gap Between What "Privacy" Means in the U.S. Versus the European Union Must Be*

Advocates of the use of market mechanisms often maintain that the private sector operates most efficiently when government regulation does not constrain entrepreneurial activity. At first glance, this maxim seems to apply to the gathering and compilation of information, as attested by the success of the data marketing industry in the United States compared to Europe. In the United States, even the FBI seeks information for its investigations from private companies.[105] However, whether a lack of regulation increases the "efficiency" of business data protection practices depends on the crucial condition of whether businesses take adequate account of the costs of privacy infringements. To be efficient, businesses must internalize the costs of privacy infringements in the pricing of their products.

Because of the government's ad hoc approach to data privacy, U.S. regulation of the private sector largely depends on industry norms and individual company policies that are developed in reaction to market pressures. Yet until recently, industry norms and policies were rare. While they have suddenly proliferated in the context of U.S.-EU negotiations over the adequacy of U.S. data privacy protections,[106] these "self-regulatory" schemes remain voluntary, unenforceable, and, it appears, often ignored by the very companies advocating their use.[107] Privacy labeling programs are being created for companies to market their data privacy practices to attract customers, but there is presently little to no external monitoring of labeling practices.[108] While privacy advocates assert that these "self-regulatory" measures are smoke-screens to impede government regulation,[109] they nonetheless hope to use the EU Directive's regulatory mechanisms (and U.S.-

Addressed, ABA BANKING J., Dec. 1, 1997 at 30, 34–38 (concerning the U.S. sectoral approach).

104. However, in March 1999, largely in reaction to the EU Directive, the Clinton Administration created a new post of "chief counsel for privacy" in the Office of Management and Budget to "coordinate policy for public and private sector use of information and serve as a point of contact on international privacy issues." *Clinton Administration To Name Swire as OMB's Privacy Policy Coordinator*, 16 Int'l Trade Rep. (BNA) 396 (Mar. 10, 1999).

105. *See* Reidenberg, *supra* note 97, at 536 n.216 (citing Ray Schultz, *FBI Said To Seek Compiled Lists for Use in Its Field Investigations*, DM NEWS, Apr. 20, 1992, at 1).

106. *See infra* Section V.C.

107. *See* SCHWARTZ & REIDENBERG, *supra* note 84, at 309 (noting that while the DMA issued "Guidelines for Personal Information Protection" and established a "Privacy Task Force," even the Task Force's "founding members ignore them"). Similarly, TRUSTe (formerly eTRUST) claims that 88% of all web users visit a TRUSTe-licensed website each month. According to TRUSTe, these websites exhibit a TRUSTe seal in order to build trust among customers that the site's privacy policies are genuine. *See* TRUSTe website (visited on Nov. 29, 1999) <http://www.truste.org/about/about_ranking>. Yet the FTC brought a suit against GeoCities, which claimed to abide by the TRUSTe data privacy principles. The FTC found that GeoCities sold personal information in violation of the privacy safeguards set forth in its on-line notice to consumers. *See Comments of Mark Silbergeld on the Department of Commerce Draft Safe Harbor Principles* (visited Jan. 13, 1999) <http://www.ita.doc.gov/ecom/com1abc.htm#silbergeld>. Silbergeld spoke on behalf of the Center for Media Education, Consumer Federation of America, Consumers Union, Electronic Privacy Information Center, Junkbusters, The NAMED, Privacy International, Privacy Journal, Privacy Rights Clearinghouse, Privacy Times, and the U.S. Public Interest Research Group.

108. For example, TRUSTe monitors the very companies that fund it, leading to criticism that it is not independent. *See* Jeri Clausing, *On-Line Privacy Group Decides Not To Pursue Microsoft Case*, N.Y. TIMES, Mar. 23, 1999, at C5 (noting that Microsoft had contributed $100,000 to the TRUSTe group).

109. *See infra* note 267 and accompanying text.

EU negotiations over their application) to change regulatory policies and market practices in the United States.

C. *Problems with the Public-Private Distinction*

Given the increasing importance of large private actors in decisions affecting individuals' lives—offering employment, health care, personal injury insurance, home financing, and most transportation, communication, and entertainment services—it may seem odd that the private sector is subject to less regulation over the use of personal information than the public sector. As the management theorist Peter Drucker wrote over a half century ago, in American society, the large corporation has become the "institution which sets the standard for the way of life and the mode of living of our citizens; which leads, molds and directs; which determines our perspectives on our own society; around which crystallize our social problems and to which we look for their solution."[110]

The traditional distinction in the American legal system between the public and the private has long been critiqued.[111] The distinction's basis lies in liberal political theory, according to which individuals need to be protected from collective control over their behavior.[112] Critics maintain that private entities' activities need to be subject to similar controls because they too can coerce or otherwise significantly influence individual behavior.[113] For example, numerous constitutional law scholars critique the Supreme Court's well-entrenched "state action" doctrine, which limits the application of the

110. PETER FERDINAND DRUCKER, THE CONCEPT OF THE CORPORATION 6–7 (1946).

111. *See generally* GERALD TURKEL, DIVIDING PUBLIC AND PRIVATE: LAW, POLITICS, AND SOCIAL THEORY (1992) (exploring critiques of the distinction by major social theorists); Morton J. Horwitz, *The History of the Public/Private Distinction*, 130 U. PA. L. REV. 1423 (1982) (maintaining that the public/private distinction arose in order to define an area free from the influence of the state, and that the distinction has eroded as private entities have assumed more power); Duncan Kennedy, *The Stages of the Decline of the Public/Private Distinction*, 130 U. PA. L. REV. 1349 (1982) (describing a theoretical progression whereby the public/private distinction has blurred such that the characteristics of each are found in the other).

112. *See, e.g.*, Horwitz, *supra* note 111, at 1423 ("[I]n reaction to the claims [of leaders] to the unrestrained power to make law, there developed a countervailing effort to stake out distinctively private spheres free from the encroaching power of the state."); Robert H. Mnookin, *The Public/Private Dichotomy: Political Disagreement and Academic Repudiation*, 130 U. PA. L. REV. 1429, 1440 (1982) (posing questions about how much control over behavior a state should have, and which activities should be protected by categorizing them as private).

113. Many of the critics of the public-private distinction are also critics of liberalism itself. *See, e.g.*, CHALLENGING THE PUBLIC/PRIVATE DIVIDE: FEMINISM, LAW, AND PUBLIC POLICY (Susan B. Boyd ed., 1997); ROBERTO MANGABEIRA UNGER, LAW IN MODERN SOCIETY 192–93 (1976) (describing the incoherence of the public-private distinction); Ruth Gavison, *Feminism and the Public/Private Distinction*, 45 STAN. L. REV. 1, 44–45 (1992) (critiquing the distinction from a feminist perspective as perpetuating social power structures). However, strands of liberal theory support regulating corporate use of personal information. Under liberal theory, individuals also must be protected from the collective control or dominance of large economic interests. *See* ANDREW ALTMAN, CRITICAL LEGAL STUDIES: A LIBERAL CRITIQUE 10–13 (1990). Altman cites L.T. Hobhouse's "reconstruction of liberal theory," which argued that the state should adopt economic policies calculated to reduce the vast inequalities generated by the operation of the market. *See id.* at 10–11. Altman also refers to the law's power, under liberal thought, "to constrain, confine, and regulate the exercise of social and political power," whether exercised "by other individuals" or "by institutions." *Id.* at 13.

Fourteenth Amendment's due process and equal protection requirements to federal governmental actions.[114] Legal realists have long cast doubt on the workability of the public-private distinction, given that so many "private" entities provide "public" functions or are deemed to act in the "public interest."[115] Law and society scholars such as Stuart Macaulay note that in many cases, private firms perform public government's three primary functions—the creation and interpretation of rules, adjudication over compliance, and application of sanctions for non-compliance.[116]

Private sector proposals for "self-regulation" of data privacy protections are an excellent example of private rulemaking, adjudication, and enforcement. Under self-regulatory programs, private associations enumerate privacy principles, award privacy seals to complying corporations, hear individual complaints, and determine the consequences of violations. Yet as regards problems of data privacy protection, privacy advocates doubt whether individuals can look to corporations and associations funded by them—to return to Drucker's words—"for their solution."[117] They lobby for legislative intervention providing for state enforcement of individual privacy rights.

---

114. *See* WILLIAM P. KREML, THE CONSTITUTIONAL DIVIDE: THE PRIVATE AND PUBLIC SECTORS IN AMERICAN LAW (1997) (charting the history of the Supreme Court's use of the public/private distinction); Charles L. Black, Jr., *Foreword: "State Action," Equal Protection, and California's Proposition 14*, 81 HARV. L. REV. 69, 91–95 (1967) (summarizing numerous critiques about the doctrine's inability to define meaningful categories); Paul Brest, *State Action and Liberal Theory: A Casenote on* Flagg Brothers v. Brooks, 130 U. PA. L. REV. 1296 (1982) (analyzing the state action doctrine in the context of the Supreme Court's finding that there was no due process violation when a private company disposed of goods under a warehouseman's lien without any governmental hearing); Erwin Chemerinsky, *Rethinking State Action*, 80 NW. U. L. REV. 503 (1985) (examining the incoherence of the state action doctrine under various theories of rights and justifications of the doctrine).

115. *See, e.g.*, Morris R. Cohen, *Property and Sovereignty*, 13 CORNELL L.Q. 8 (1927) (arguing that state enforcement of property rights is best conceptualized as delegated public power); Robert Lee Hale, *Coercion and Distribution in a Supposedly Non-Coercive State*, 38 POL. SCI. Q. 470, 470 (1923) (noting the coercion inherent in a protection of property rights under a laissez-faire system).

As regards private entities providing public functions, the early U.S. corporate law scholar Adolf Berle examines the power of the public corporation and refers to it as a social organization fulfilling public functions and having social responsibilities. *See* ADOLF A. BERLE, JR., THE 20TH CENTURY CAPITALIST REVOLUTION 104–05 (1954) ("The corporation is, in theory at least, a creature of the state which charters it, and its operations are sanctioned and in measure aided by any state in which it is authorized to do business . . . . If it has power to use, and does use its supply or employment functions to effect political policies as well as to produce and distribute electricity or gasoline, motor cars or washing machines, it has, *de facto* at least, invaded the political sphere and has become in fact, if not in theory, a quasi-governing agency."). In this respect, see also CORPORATIONS AND SOCIETY: POWER AND RESPONSIBILITY (Warren J. Samuels & Arthur S. Miller eds., 1987).

In the contemporary context, Colin Bennett notes how "Canada's small network of privacy and information commissioners" has been increasingly concerned by "the gradual erosion of the boundaries between the 'public' and the 'private' sectors . . . [on account of] efforts to privatize or 'outsource' government functions." Colin J. Bennett, *The EU Data Protection Directive: The North American Response* (visited Nov. 11, 1999) <www.cous.uvic.ca/poli/bennett/research/plb98.htm>.

116. *See* Stewart Macaulay, *Private Government*, *in* LAW AND THE SOCIAL SCIENCES 445, 447–49 (Leon Lipson & Stanton Wheeler eds., 1986) (citing examples such as "company towns," trade associations, and internal corporate mechanisms for arbitration and protection against industrial espionage).

117. DRUCKER, *supra* note 110, at 6–7.

D. *Alternative Institutions: The Interaction of U.S. Markets, Legislatures, and Courts in Regulating Private Sector Use of Personal Data*

Alternative institutions can regulate the commercial exploitation of personal information. Government regulation—whether federal, state, or local—is only one means to regulate firm behavior. Even in unregulated sectors, and even where courts do not recognize common law or constitutional rights of action, market forces can still constrain company behavior. While the institutional alternatives posed by U.S. and EU negotiations have focused on legislative intervention and market-influenced business "self-regulation," the United States offers a third institutional mechanism to constrain privacy infringements. Common law courts can intervene to protect individual privacy interests from tortious acts. The Supreme Court could, in theory, also read constitutional provisions broadly to better protect individual informational privacy. This section examines the interaction of these institutions at the national level in order to set up a subsequent assessment of how this institutional interaction is affected by the actions of institutions in powerful foreign states.

1. *Role of Markets*

Markets can be powerful regulators. Companies value their reputations. Tradenames and trademarks not only facilitate product promotions; they facilitate boycotts. A company's reputation in the market can thereby constrain its use and transfer of information about its clients.[118] Major U.S. companies have implemented data protection policies in response to negative publicity or to reduce their risk. Pacific Bell and America Online, two huge communications companies, abandoned plans to sell information on their subscribers in response to widespread customer complaints,[119] and developed new company data privacy policies.[120] Bowing to consumer protests, Lotus Development Corporation, the large software company, and Equifax, the large credit bureau, abandoned plans to create a CD-ROM containing household information that would be valuable for marketing.[121] Equifax reputedly ceased marketing consumer names and addresses altogether, even though it had earned $11 million in revenue from such sales the previous year.[122] Intel likewise reversed its decision to activate an identifying code number in its

118. For this constraint to be effective, however, a significant number of consumers must be aware of both the entity with which they are transacting and that company's deserved reputation. These conditions are not always met, especially in transactions over the Internet.

119. *See* Rajiv Chandraskoran, *AOL Cancels Plan for Telemarketing: Disclosure of Members Protested*, WASH. POST, July 25, 1997, at G1; *see also* Bruce Keppel, *Bell Drops Plan To Sell Phone Customer Lists*, L.A. TIMES, Apr. 16, 1986, at 3.

120. *See Profile of Pacific Bell and Its 1992 Customer Privacy Policy*, PRIVACY & AM. BUSINESS, Sept./Oct. 1993, at 11, 15; *Comments of America Online on the Department of Commerce Draft Safe Harbor Principles* (visited Jan. 13, 1999) <http://www.ita.doc.gov/ecom/com4abc.htm>.

121. *See* Lawrence M. Fisher, *New Data Base Ended by Lotus and Equifax*, N.Y. TIMES, Jan. 24, 1991, at D6.

122. *See* Shelby Gilje, *Credit Bureau Won't Sell Names*, SEATTLE TIMES, Aug. 9, 1991, at D6.

next generation of computer chips that would enable companies to gather profiles of individual users of websites. It did so just hours after a consumer rights group—the Electronic Privacy Information Center—called for a boycott of the chip.[123] These companies did not react to lawsuits or government threats; they merely attempted to preserve their market image.

By enhancing their privacy protection policies, companies can, in theory, potentially improve their market position vis-à-vis competitors. In particular, they can potentially increase electronic sales through marketing their privacy protection policies.[124] Surveys have found that consumers identify concerns about the privacy of their personal information as the main reason they have stayed off the Internet.[125] Federal Trade Commissioner Mozelle Thompson observes: "Companies' economic future depends on making people feel good on the Internet. People are not going to buy on the Internet if they don't feel safe."[126]

A number of U.S. commentators and policymakers advocate a "contractual approach to data privacy."[127] The National Telecommunications and Information Administration of the U.S. Department of Commerce, for example, promotes "a modified contractual model that allows businesses and consumers to reach agreements concerning the collection, use, and

123. *See* Jeri Clausing, *The Privacy Group that Took on Intel*, N.Y. TIMES, Feb. 1, 1999, at C4. The identifying code numbers nevertheless remain a concern. Shortly after Intel announced its decision a computer hacker demonstrated that he could reactivate the identifying code number without an individual's knowledge. *See* Markoff, *supra* note 69, at 3.

124. The implementation of data privacy protection to enhance electronic commerce, however, raises another collective action problem. While all companies may collectively benefit if they all implement data privacy controls, individual companies may not implement them in order to profit from using and selling personal information. To the extent that all companies do not collectively enhance data privacy protections, consumers may be wary of engaging in any e-commerce, even with companies implementing protections. Accordingly, the purpose of the Canadian data privacy protection bill now being considered before the Canadian parliament is not solely to "protect" privacy, but rather "to support and promote electronic commerce by protecting personal information that is collected, used or disclosed." Act to Support and Promote Electronic Commerce by Protecting Personal Information, Bill C-54, The House of Commons of Canada (1999) (visited Apr. 4, 1999) <http://www.parl.gc.ca/36/1/parlbus/chambus/house/bills/government/C-54/C-54_1/C-54_cover-E.html>. The Canadians wish to overcome companies' collective action problem by mandating greater privacy protection so that all companies will benefit from increased consumer confidence in electronic commerce transactions. *See id.*

125. *See* Louis Harris & Alan F. Westin, *Commerce, Communication and Privacy Online* (visited Oct. 7, 1999) <http://www.privacyexchange.org/iss/surveys/computersurvey97.html> (finding that in 1997 large numbers of non-users of the Internet would be more likely to go online if their personal information were protected); Alan F. Westin, *Netizens Want Better Privacy Rules and Practices for E-Commerce* (visited June 3, 1999) <http://www.pandab.org/pabsurve.htm> (reporting that 79% of those who do not use the Internet state they would find privacy issues important if they went online); *1996 Equifax/Harris Consumer Privacy Survey: Executive Summary* (visited Oct. 5, 1999) <http://www.equifax.com/consumer/parchive/svry96/docs/summary.html> (stating that 64% of the public disagrees that on-line service providers should be able to track their activities on the Internet).

126. Jamie Beckett & Dan Fost, *FTC Sets Deadline on Internet Privacy Rules*, S.F. CHRON., Oct. 14, 1998, at B1 (quoting Thompson).

127. Steven A. Bibas, *A Contractual Approach to Data Privacy*, 17 HARV. J.L. & PUB. POL'Y 591 (1994); *see also* Scott Shorr, *Personal Information Contracts: How To Protect Privacy Without Violating the First Amendment*, 80 CORNELL L. REV. 1756, 1850 (1995) (advocating the use "of contracts for buying, selling, renting and utilizing [personal] information").

dissemination of TRPI [telecommunications-related personal information]."[128] Proponents of contractual models claim that such models are economically more efficient than government regulation. As Scott Bibas contends, "[a] contractual approach, by pricing information . . . , more efficiently allocate[s] data than would a centrally planned solution," such as that established by the EU Directive.[129] Under a contractual model, individuals can simply pay for privacy protection or threaten to take their business elsewhere.[130] Consumers may not be able to bargain individually with companies over their data privacy policies, but they can, according to this model, influence those policies by threatening to exit from transactions.[131]

Commentators advocating a contractual model also support greater consumer education to enhance consumers' bargaining position. One advocate of a market-based approach proclaims: "The answer to the whole privacy question is more knowledge. More knowledge about who's watching you. More knowledge about the information that flows between us—particularly the meta information about who knows what and where it's going."[132] The National Consumers League and others have designed projects to educate consumers in these matters.[133] As Professor Fred Cate notes, consumers can learn to check help screens and instruction manuals, and generally develop a greater awareness of privacy issues, including their right to "opt out" of having their personal information used for other purposes.[134] In this way, market advocates argue, consumers may enforce privacy rights through contract, explicit or implicit, and through threatened exit from contract.[135]

Like efforts to regulate privacy through legislation and court intervention, however, private contract and market models proffer no panacea.

---

128. NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION, U.S. DEPARTMENT OF COMMERCE, PRIVACY AND THE NII: SAFEGUARDING TELECOMMUNICATIONS-RELATED PERSONAL INFORMATION (1995), *cited in* CATE, *supra* note 59, at 96. TRPI is personal information that is created in the course of an individual's subscription to a telecommunications or information service or as a result of his or her uses of that service.

129. Bibas, *supra* note 127, at 605 (maintaining that the EU Directive establishes such a centrally planned solution). For support, Bibas cites the work of the free market economist Friedrich von Hayek, who advocates limited government involvement in the economy. *See id.*

130. As Professor Fred Cate writes, "if enough consumers demand better privacy protection and back up that demand, if necessary, by withdrawing their patronage, companies are certain to respond." CATE, *supra* note 59, at 104. The power of market constraints is demonstrated by the pressures placed on Pacific Bell, Lotus, Equifax, and Intel. *See supra* notes 118–123 and accompanying text.

131. For a discussion of the roles of *exit* and *voice* in transacting, see ALBERT O. HIRSCHMAN, EXIT, VOICE, AND LOYALTY: RESPONSES TO DECLINE IN FIRMS, ORGANIZATIONS, AND STATES (1970).

132. Joshua Quittner, *Invasion of Privacy*, TIME, Aug. 25, 1997, at 35. *Invasion of Privacy* was the feature article of this issue of *Time*. Quittner was news director of Pathfinder, Time, Inc.'s "mega info mall." He concludes: "The only guys who insist on perfect privacy are hermits like the Unabomber." *Id.*

133. *See* FEDERAL TRADE COMMISSION, PUBLIC WORKSHOP ON CONSUMER PRIVACY ON THE GLOBAL INFORMATION INFRASTRUCTURE, § III.B (visited Jan. 13, 1999) <http://www.ftc.gov/reports/privacy/privacy1.htm>. Businesses, through the Online Privacy Alliance (a consortium now consisting of more than 80 large companies and business associations), also advocate educating consumers about privacy issues. *See* Online Privacy Alliance website at <http://www.privacyalliance.org/who/> (visited Nov. 28, 1999).

134. *See* CATE, *supra* note 59, at 103.

135. *See id.*

Markets, not surprisingly, are imperfect: Knowledge is expensive and parties have unequal access to information. The market for data privacy protection is characterized by widely dispersed individuals, with low stakes,[136] entering into ad hoc transactions with large enterprises. Enterprises know how they will exploit personal information; individuals do not. Enterprises repeatedly use individual information; individuals are only intermittently aware of privacy intrusions. Individuals have highly imperfect information upon which they can improve only at considerable cost. For each individual, the aggregate of these costs exceeds the value of the individual's privacy interest. To investigate the privacy practices of every business with which one contracts for a product or service costs time and, in market terms, time is money. Individuals thus forego investigating enterprise behavior and forget contracting.

The Clinton Administration's inter-agency Information Infrastructure Task Force, while supporting a contractual approach to privacy, recognizes the problem of unequal "bargaining conditions" that interfere with "mutually agreeable privacy protections."[137] The Task Force unfortunately fails to define these bargaining conditions. Yet for almost all consumers, almost all of the time, high information costs, low average stakes, and unequal bargaining power prevail. Technologically informed and wealthy persons may be able to overcome some of these hurdles. They may, for example, be able to buy greater privacy protection through contract, the use of software technology,[138] encryption devices, or "Smart Cards."[139] Poorer and less educated persons remain at greater risk.

2. *Role of Legislation*

The market is not solely an alternative to legislation and judicial intervention. It is also a complement. Legislation creates default rules around which bargaining can take place. While Bibas, a proponent of a

136. Individuals have lower per capita stakes, and thus have less incentive to participate in the market for personal information. In most cases, third-party use of personal information is harmless. Yet in some instances the harm is immense. On average, the individual has less stake in protecting her privacy than the enterprise that profits from violating it. Examples of significant harm are cited in ROTHFEDER, *supra* note 1, at 15 (mentioning the murder of a sitcom star by an emotionally crazed admirer who found her through computer database information). *See also supra* notes 95–97 (reporting on scandals leading to new privacy legislation).

137. Privacy Working Group, Information Policy Committee, Information Infrastructure Task Force, *Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information* (visited Jan. 13, 1999) <http://www.iitf.nist.gov/ipc/ipc/ipc-pubs/niiprivprin_final.html>.

138. Novell has developed software that permits Internet users to control how much information may be collected from them by an Internet website. The software "might also make it possible for users to sell or barter their personal information for rebates, discounts or other special considerations." John Markoff, *Novell To Offer Data-Privacy Technology for Internet*, N.Y. TIMES, Mar. 22, 1999, at C1; *see also* Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553, 558 (1998) (discussing the Platform for Internet Content Selection (PICS), designed to "facilitate the selective blocking of access to information on the Internet and to provide an alternative to legal restrictions").

139. The FTC defines a Smart Card as "a stored value card bearing an implanted microprocessor. It permits its owner to enter in to transactions anonymously and to transmit encrypted information via the Internet." FEDERAL TRADE COMMISSION, *supra* note 133, § II n.68.

contractual/market approach to privacy protection, recognizes that "opt out" and "opt in" rights create default rules, he fails to acknowledge the importance of choosing between them.[140] In critiquing the EU Directive for being "centrally planned" and thus inefficiently allocating privacy rights, Bibas fails to note that, in almost all cases under the EU Directive, consumers can "opt into" or "out of" the free dissemination of personal information about them.[141] The "opt in" right creates a different default rule around which market negotiations can take place than an "opt out" right or no right whatsoever.[142] Companies are more likely to have to pay a price for individual consent under an "opt in" regime, thereby employing the very pricing mechanism Bibas advocates. Were U.S. law to require an individual's affirmative consent for personal information to be gathered for one purpose and marketed for another, private contracting could still occur. Companies would have to provide individuals with adequate notice and obtain their affirmative consent. The market would still function. The law, by requiring companies to provide more information to individuals, would place individuals in a stronger negotiating position. In fact, because companies would be less able to exploit information and transaction cost asymmetries, the pricing of privacy protection would more likely take place.

There are, however, powerful reasons that U.S. legislation has yet to change. These reasons parallel the problems encountered with market mechanisms. Businesses are more likely to lobby legislative representatives

140. *See* Bibas, *supra* note 127. Richard Posner, on the other hand, is clear in assigning the default rule, maintaining that "there is a prima facie case for assigning the property right away from the individual where secrecy would reduce the social product by misleading the people with whom he deals." Posner, *supra* note 63, at 403–04 (arguing that a legal right of privacy should be "based on economic efficiency" and that, on account of transaction costs and the interest in obtaining creditable information, property rights in privacy should be assigned "away from the individual"); *see also* RICHARD A. POSNER, OVERCOMING LAW 531–51 (1995) (containing a subsequent confirmation of these views and a response to Kim Lane Scheppele, a critic of his analysis of the law and economics of U.S. courts' treatment of privacy issues). For a challenge to Posner from a law-and-economics approach, see Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381 (1996). Murphy sets forth the economic rationale for a default rule assigning the property right to the individual and argues that "[a] privacy rule . . . forces the merchant to bring his unique knowledge out into the open. The consumer becomes better informed and therefore the transaction is more likely to achieve the most efficient allocation." *Id.* at 2414; *see also* Paul M. Schwartz, *Privacy and the Economics of Personal Health Care Information*, 76 TEX. L. REV. 1, 9–10 (1997) (providing more general criticisms of Posner's data privacy analysis). Similarly, Ian Ayres and Robert Gertner point out that "[s]etting a default rule that least favors the better informed parties creates an incentive for the informed party to bring up the relevant contingency in negotiations." Ian Ayres & Robert Gertner, *Strategic Contractual Inefficiency and the Optimal Choice of Legal Rules*, 101 YALE L.J. 729, 761 (1992).

141. Bibas, *supra* note 127. On "opt in" and "opt out" rights under the EU Directive and their relation to the sensitive nature of the information, see *supra* note 44 and accompanying text. The EU Directive leaves it to the EU Member States to decide whether to prohibit or permit (subject to express informed consent) a data subject from consenting to the "processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life." EU Directive, *supra* note 2, art. 8(1). This is in turn subject to certain exemptions. *See id.*

142. "Opt in" rights provide significantly greater protection than "opt out" rights. With only an "opt out" choice, any time a consumer forgets to check a box, she is deemed to have consented to the use, compilation, and onward transfer of personal information about her. The hundreds of times she previously remembered to check an "opt out" box would be of no avail.

over data privacy issues because they have greater per capita stakes.[143] Moreover, many Americans are somewhat ambivalent about privacy. While privacy advocates cite polls showing that eighty percent of Americans believe they have "lost all control over how companies collect and use their personal information,"[144] a majority of Americans nonetheless appear to accept being targeted for marketing by mail based on consumer profiles.[145] In addition, the popular daytime shows hosted by Jerry Springer, Oprah Winfrey, Sally, Ricky, and others feed off self-exposure and voyeurism.[146] Even individuals who desire to protect their own privacy may covet intruding on the privacy of others.

The market for regulation encounters the same characteristics of well-financed groups with clearly defined, high per capita stakes being more active and effective players than dispersed consumers with less clearly defined, low per capita stakes.[147] Businesses better promote their interests before Congress

---

143. Businesses pour millions of dollars into Congressional campaigns. *See* NOTHING SACRED, *supra* note 95, at 5 (noting that "the nation's hospitals, insurance companies, and members of trade associations" that oppose legislation requiring greater protection of health-care records "have poured more than $45.6 million into congressional campaigns" from 1987 to 1996); *id.* at 55–61 (breaking these figures down into tables). For a general analysis of the "privileged" position of business in U.S. politics, see CHARLES E. LINDBLOM, POLITICS AND MARKETS: THE WORLD'S POLITICAL-ECONOMIC SYSTEMS 170–200 (1977).

144. Alan F. Westin, *The Era of Consensual Marketing Is Coming* (visited Nov. 11, 1999) <http://www.privacyexchange.org/iss/surveys/1298essay.html> (also finding that nine out of ten Americans are concerned about threats to privacy). In general, survey evidence indicates that a large majority of the public is concerned about privacy. *See, e.g.*, Lorrie Faith Cranor et al., *Beyond Concern: Understanding Net Users' Attitudes About Online Privacy*, AT&T LABS-RESEARCH TECHNICAL REPORT TR 99.4.3 (visited Apr. 14, 1999) <http://www.research.att.com/library/trs/TRs/99/99.4/99.4.3/report.htm> (finding that only 13% of Internet users are unconcerned with privacy and noting that the level of Internet users' concern varies widely according to the type of information collected and the uses to which it is put). These and other privacy surveys are available at the Privacy Exchange website. *See* Opinion Surveys (visited Nov. 29, 1999) <http://www.privacyexchange.org/iss/surveys/surveys.html>. Polls show that individual concern over threats to privacy has consistently risen since the 1970s. *See Citations to Harris-Equifax Consumer Privacy Surveys Since 1970*, *in* Murphy, *supra* note 140, at 2404–05.

145. *See* Westin, *supra* note 144 (stating that 61% of U.S. consumers in 1998 found it "acceptable for businesses they patronize . . . to look at their profile of activities and inform them about products and services that might be of interest to them"). A significant minority nonetheless do not accept such marketing. Moreover, the issue is positively framed in terms of "business[es] they patronize" and "products . . . that might be of interest," which should influence the data. *Id.*

146. This ambivalence toward privacy issues is captured on the cover of *Newsweek* published during the week the House of Representatives was to vote on President Clinton's impeachment. The cover read "HOT TICKET: Nicole Kidman bares all—about her daring Broadway debut, marriage to Tom Cruise and their fight for privacy." NEWSWEEK, Dec. 14, 1998. Kidman's fight for privacy obviously had a price, a price *Newsweek* was willing to pay so Americans could peep into her private life. The timing, paralleling the trial of the President over his concealment of a sexual affair, was apropos.

147. This raises the question why business interests have been more successful in forestalling greater data privacy regulation in the United States than in Europe. This Article, which examines the impact of EU institutions on U.S. policies and practices, does not focus on this issue. Possible explanations nonetheless include the following: (i) European historical and cultural circumstances: In the aftermath of Nazism, Germans desired greater protection of their personal privacy against the state. Privacy regulation ironically also protected former members of the Nazi party and regime collaborators; (ii) European tastes: From my eight years of living in Paris, France, it was clear that the French are much more discreet in discussing personal matters than Americans. In the Clinton-Lewinsky affair, for example, the French could not understand why a personal matter received such publicity. On the

and administrative bodies than do individual consumers facing considerable collective action problems.[148] When the Department of Commerce asks for comments on draft privacy guidelines, comments stream in from large multinational corporations and business associations.[149] As a result of successful industry lobbying, industry remains the dominant regulator of information privacy standards in the United States, resulting in fewer constraints on the collection, use, and commodification of personal information.

3. *Role of Courts*

Privacy advocates also stress the need for courts to protect an individual's privacy rights to personal data. Some advocates demand that Congress create new rights of action by passing an omnibus data privacy statute (analogous to the EU Directive) under which courts and administrative bodies would recognize individual rights in personal information and could enjoin company use of it, issue civil and criminal fines, and award personal damages for rights violations.[150] Others call for courts independently to expand tort law and recognize a cause of action for "tortious commercial dissemination of private facts."[151] Still others call for "legal recognition of

---

contrary, in France, the press knew but did not publicize the fact that President Mitterrand had an illegitimate daughter; (iii) Greater deference to state bureaucracies: Bureaucracies play a much more important role in continental European traditions than in the United States; (iv) Different modes of capitalism: The United States arguably imposes fewer controls over the private sector. While this is contestable in some areas (such as environmental regulation), it is clearly the case with respect to labor regulation.

148. A significant part of the battle lies in the framing of the debate. Industry has so far succeeded in framing the debate in terms of enterprises' right as *private* owners of information to be free from *public* (government) interference. Any ban on their use of data files would in many cases be claimed a "taking" in violation of the Fifth Amendment's prohibition against the government's taking of private property without due process or just compensation. To be successful, privacy advocates must re-frame the issue into one of protecting fundamental human *privacy* rights from the *publication* of personal information by private commercial enterprises without the individual's consent. Alternatively, advocates must invoke a balancing of privacy interests and economic interests that differentiates the need to protect the free flow of information in a democracy from the exploitation of personal information for marketing purposes, as well as from potentially manipulative anti-democratic aims.

149. *See infra* Part V. In addition, even where legislation is passed, regulatory agencies whose formal role is to apply it may be "captured" by special interests. *See, e.g.*, Roger Noll, *Economic Perspectives on the Politics of Regulation, in* HANDBOOK OF INDUSTRIAL ORGANIZATION (R. Schmalensee & R.D. Willig eds., 1989); Sam Peltzman, *Toward a More General Theory of Regulation*, 19 J.L. & ECON. 211 (1976).

150. *See, e.g., Financial Institutions and Consumer Credit Unions: Financial Privacy Before the House Committee on Banking*, 106th Cong. (July 20, 1999) (statement of Edmund Mierzwinski, Consumer Program Director, U.S. Public Interest Research Group, that the United States needs to "move beyond the sectoral approach").

151. Jonathan P. Graham, Note, *Privacy, Computers, and the Commercial Dissemination of Personal Information*, 65 TEX. L. REV. 1395, 1428 (1987). United States courts already recognize a common-law privacy tort. Yet this tort is limited to the following types of acts: unauthorized wiretapping and other forms of intrusion, publicizing offensive private facts, publicizing false information, and misappropriation of identity. *See* RESTATEMENT (SECOND) OF TORTS § 652 (1977); WILLIAM PROSSER, HANDBOOK OF THE LAW OF TORTS, 829–51 (3rd ed., 1964). The notion of a common-law right to privacy was early espoused in the famous article by Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890) which maintained that the privacy right "to be left alone" is based on the principle "of an inviolate personality." *See also* Shorr, *supra* note 127, at

property rights in personal information" that are enforceable before courts.[152] Personal information is valuable property and thus the business of trafficking it is rapidly expanding.[153] Without a recognition of property rights in personal information, by statute or independent judicial action, personal information is an object in the public domain free for capture.[154] In such a case, it is only transformed into property once obtained by a business that stores and processes it as part of a database for its own or a third-party's exploitation.

Yet there are limits to relying on courts.[155] Application of a balancing test in a tort or property case—with judges balancing, on a case-by-case basis, privacy concerns against the benefits of free data flows—would be time-consuming and expensive. It would use up limited judicial resources and reallocate them away from legal claims in other areas. Moreover, even with relatively clear legislative guidelines, given the virtually infinite number of transactions in which data privacy concerns arise, courts could not possibly handle all conflicts. Judicial budgets and staffs are finite.[156] And, in any case, most individuals would not have the time and financial means to pursue them.

Nonetheless, judicial and administrative remedies can complement market and legislative measures. The mere threat of judicial or administrative intervention can significantly contribute to changes in business practice. Even where this threat is limited in practice, human resources departments and in-house and external counsel will make businesses aware of its potential and, generally, foster business compliance with formal law. This can lead to changed business practice.[157] The EU Directive alters the institutional balance in the United States, spurring such changes.

E. *The Limits of Single Jurisdictional Analysis: The Need To Account for Transnational Institutional Interdependence*

Comparative institutional analysis correctly identifies the key question "who decides who decides." Should decision-making be delegated to the markets and their pricing mechanisms, to legislatures and regulators that can create fairer and more efficient default rules around which bargaining takes place, or to courts that can balance competing concerns on a case-by-case

---

1776–84.

152. Shorr, *supra* note 127, at 1818; *see also* Patricia Mell, *Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness*, 11 BERKELEY TECH. L.J. 1, 10 (1996) (naming the individual's right to privacy "a type of property right in his electronic persona"). Mell, in her conclusion, calls for recognition of this property right by statute. *See id.* at 78–81; *see also* Murphy, *supra* note 140, at 2410, 2416-17.

153. *See supra* notes 64–65 and accompanying text.

154. Although personal data is not a limited natural resource, its free taking in a system of non-recognition of property rights can be viewed as analogous to a "tragedy of the commons" problem, in that personal information will be over-exploited without any recognition of the personal and collective costs of privacy infringements. On the tragedy of the commons, see, for example, Garrett Hardin, *The Tragedy of the Commons*, 162 SCI. 1243 (1968) (stating that "freedom in a commons brings ruin to all").

155. *See* KOMESAR, *supra* note 24, at 123–50.

156. The budgets and staffs of the data privacy supervisory authorities that are to oversee processing operations in each of the EU Member States are similarly limited.

157. *See infra* Subsection V.B.2.

basis? Which institutional mechanisms should predominate in which policy areas?[158]

Yet just as single institutional analysis is inherently problematic because it does not compare the relative strengths and weaknesses of competing institutions in addressing specific policy issues, so too single jurisdictional analysis fails to account for the dynamics of regulatory change in a globalizing economy. What happens in one jurisdiction can affect not only the playing field in other jurisdictions, but also the players' perceptions of their stakes. Data privacy regulations in Europe not only inform the tenor and context of debates in the United States, but also shape interest groups' appreciation of their options.[159] Under the EU Directive, U.S. businesses face potential litigation before European courts and administrative bodies. United States regulators press U.S. businesses to enhance internal data privacy protections in order to avert a trade war implicating other U.S. interests. Playing off the U.S.-EU regulatory conflict and its media coverage, privacy advocates jack up pressure on U.S. regulatory authorities and business. Thus, U.S. businesses are pressed to modify their data privacy practices from multiple directions. As a result of the confluence of these pressures, the EU Directive can help shape a new default rule in the United States—that of prior informed consent—around which bargaining in the U.S. market can take place.

We live in a world where it is less and less accurate to think solely in terms of national regulation and national institutions. In one sense, the EU Directive is an exogenous force in internal U.S. conflicts over the regulation of privacy protection, shifting the stakes of U.S. political and economic actors. On the other hand, it is misleading simply to segregate the foreign from the domestic, the external from the internal. In importing and exporting goods and services, countries can also import standards and procedures. In a globalizing economy characterized by high numbers of transactions, widely dispersed stakes, and competing national, regional, and transnational jurisdictional authorities, the allocation of decision-making among alternative institutions (be they markets, legislatures, or courts) at alternative levels of social organization (be they sub-states, states, regions, or international regimes) becomes even more complex. In a world of interdependent institutions, the difficult, but essential task of comparative institutional analysis becomes even more challenging.

158. As noted above, however, we do not live in an ideal world of clearly differentiated alternative institutions. Institutions are typically complements to one another, not clear alternatives. Government regulations both shape market negotiations and facilitate their operation. *See* VOGEL, *supra* note 81, at 3 (maintaining that in the context of globalizing markets, governments have not deregulated but rather re-regulated in response to a common set of pressures). Regulations "set the terms of market competition." *Id.* at 261. The same holds for the recognition of justiciable rights. As Posner has long noted, courts have taken the market into account in their decision-making. *See* RICHARD POSNER, ECONOMIC ANALYSIS OF LAW 229–38 (3d ed. 1986).

159. *See infra* Part V.

III. THE TRANSATLANTIC CONTEXT: MANAGING THE CONFLICT OVER PRIVACY

This part first examines the roles of transatlantic economic liberalization and EU market power in U.S.-EU negotiations over data privacy standards (Section A). It then assesses the multiple public and private means through which Europe can restrict data transfers to the United States (Section B) and the attempts by U.S.-EU authorities to manage the resulting regulatory conflict (Section C).

A. *Pooling Sovereignty To Bolster Market Power: The Role of the EU Market*

The U.S.-EU dispute over the adequacy of U.S. data privacy protection affects U.S. privacy policies and practices because the European Union exercises market power.[160] Simply put, the EU market matters to U.S. business. The European Union is the U.S.'s largest trading partner and the site of most U.S. foreign investment.[161] In 1997, the United States exported $253.6 billion of goods and services to the European Union and imported $270.3 billion of goods and services from the European Union.[162] Though massive in itself, transatlantic trade is dwarfed by sales of U.S.-controlled affiliates based in Europe. "In 1995, the last year for which complete U.S. and foreign affiliate data are available, U.S. affiliates in Europe produced $1.2 trillion" of goods and services.[163] This constituted "over half of all the foreign production of U.S. companies."[164] These companies depend on information flows, not only with third-party suppliers, customers, consultants, marketers, and other service providers, but also internally, within their complex networks of affiliates, joint ventures, and partnerships. A potential restriction on transatlantic data flows matters.

European Union market power provides EU officials with considerable bargaining leverage over data privacy issues. Were a country that attracted little U.S. trade and investment to restrict data transfers to the United States, a ban would pose little harm to overall U.S. commercial interests because of the small size of the country's market. More importantly, that country's exports

---

160. For an assessment of market power, see HIRSCHMAN, *supra* note 33.

161. *See* KEVIN FEATHERSTONE & ROY H. GINSBERG, THE UNITED STATES AND THE EUROPEAN UNION IN THE 1990S: PARTNERS IN TRANSITION 137, 149 (2d ed. 1996); *see also Bureau of Economic Analysis, International Accounts Data: Balance of Payments: Transactions by Area* (visited Jan. 12, 1998) <http://www.bea.doc.gov/bea/di/bparea-d.htm>.

162. This was out of a total of $690 billion of U.S. exports. *See Issues in U.S.-European Union Trade: European Privacy Legislation and Biotechnology/Food Safety Policy Before the House Committee on International Relations*, Federal News Services (May 7, 1998) (testimony of Franklin Vargo, Assistant Secretary of Commerce).

163. *Id.* The Department of Commerce estimates that "in 1998, such production [of U.S. companies in the European Union] will amount to around $1.5 trillion." *Id.*

164. *Id.* Vargo notes that "[t]ogether the United States and Europe account for $16 trillion of GDP, nearly half of the value of all the goods and services produced globally." *Id.*

would be disproportionately vulnerable to access restrictions to the much larger U.S. market. United States retaliation against the European Union, on the other hand, could give rise to counter-retaliation seriously harming U.S. commercial interests. Affected U.S. companies would, in turn, press the U.S. government to accommodate EU demands in order to regain access to the EU market.

The United States increasingly negotiates with the European Union as an independent political institution apart from the fifteen EU Member States. As Assistant Secretary of Commerce Franklin Vargo states, the New Transatlantic Agenda signed between the United States and the European Union in December 1995 "marks the first time that we are dealing with the EU as a political institution on a large scale."[165] A central purpose of the New Transatlantic Agenda is to coordinate and spur further trade and investment liberalization, both transatlantic and global.[166] By delegating trade negotiating authority to EU institutions, the EU Member States have been able to speak with a single, more powerful voice. This has facilitated the negotiation of tariff reductions and other trade liberalization measures and enhanced the EU role in these negotiations.[167] Businesses on both sides of the Atlantic do not want officials sidetracked by disputes over data privacy protection.

---

165. *Id.* For an overview of the history of U.S.-EU economic relations since World War II, together with recent institutional developments in the transatlantic relationship, see generally Mark Pollack & Gregory Shaffer, *Transatlantic Governance in a Global Economy* (visited Nov. 2, 1999) <http://www.polisci.wisc.edu/~pollack> (introduction to working manuscript delivered as a paper at the Annual Meeting of the Political Science Association, Sept. 2, 1999).

166. One of the four major goals of the Agenda is "to create a New Transatlantic Marketplace, which will expand trade and investment opportunities and multiply jobs on both sides of the Atlantic" and contribute "to the expansion of world trade and closer economic relations." *The New Transatlantic Agenda* (visited Nov. 1, 1999) <http://europa.eu.int/en/agenda/tr05.html>.

167. During the 1990s, transatlantic liberalization efforts gained momentum. Large U.S.- and EU-based enterprises responded favorably to the New Transatlantic Agenda and worked with government representatives to advance negotiations. In November 1995, U.S.- and EU-based multinational enterprises formed the Transatlantic Business Dialogue (TABD) to provide input and help shape transatlantic trade negotiations and policy coordination. *See TABD Background* (visited Nov. 1, 1999) <http://www.TABd.org/about/background.html>.

In June 1997, under TABD-sponsored negotiations, the United States and the European Union concluded negotiations on a series of mutual recognition agreements (MRAs) pursuant to which they recognized each other's standards for a wide range of products. The 1997 Transatlantic MRA was estimated to save affected industries more than $1 billion per year. *See EU/US/Canada: Mutual Recognition Agreements Concluded*, EUR. REP., June 14, 1997, *available in* 1997 WL 8517569. An earlier "breakthrough" was reached "after a group of top European and American business executives managed to forge a compromise between the policy makers." *See EU-US: Businessmen Forge Breakthrough on Testing*, EUR. REP., Nov. 13, 1996, *available in* 1996 WL 11074861. Within Europe, MRAs were earlier a major impetus to the completion of the European Union's single internal market. *See* Karen J. Alter & Sophie Meunier-Aitsahalia, *Judicial Politics in the European Community and the Pathbreaking* Cassis de Dijon *Decision*, 26 COMP. POL. STUD. 535 (1994) (discussing the *Cassis de Dijon* decision and the European Commission's mutual recognition policy).

Also in 1997, the United States and the European Union led an effort to eliminate tariffs on information technology products, which businesses cite as "a high point for U.S.-EU cooperation." *The New Transatlantic Agenda: Hearings Before the Subcommittee on Trade of the U.S. House of Representatives Ways and Means Committee* (July 23, 1997), *available in* 1997 WL 11235217 (testimony of Patrick Yanahan on behalf of the American Electronics Association). Charlene Barshefsky, the United States Trade Representative, testified to Congress that this "amounts to a global tax cut of $5 billion." *Consumer Trade Issues: Hearings Before the Senate Commerce Committee* (Apr. 30, 1997), *available in* 1997 WL 10570508 (testimony of Charlene Barshefsky).

In transferring negotiating authority to the European Commission over transnational data protection matters,[168] individual European countries enhanced their autonomy and influence vis-à-vis the United States. EU centralization has made the EU threat to restrict transatlantic data transfers more credible. Before the EU Directive, a number of EU Member States had data privacy legislation that, on the books, permitted them to restrict data transfers to the United States. Yet the threat of across-the-board data transfer restrictions was deemed unlikely. It was not until the EU Directive became effective that U.S. authorities reacted seriously, attempting to negotiate a solution with EU officials while simultaneously inciting U.S. businesses to enhance their internal data privacy protections to avoid a regulatory conflict.[169]

Pooling their sovereignty and acting collectively, EU Member States increased their bargaining power by magnifying the impact of a data transfer ban and by magnifying the consequences were the United States to retaliate against such a ban. Without this coordination, the United States might otherwise have exercised overwhelming economic and political clout against individual EU Member States by threatening to retaliate against them. The United States is now more restrained. The threat of counter-retaliation by the European Union is a powerful countervailing force.[170] The EU Member States have not simply "lost" sovereignty in working through centralized EU authorities. They have reallocated it in a manner that effectively enhances their negotiating authority—and, thus, their autonomy—vis-à-vis the United States.[171]

---

168. Not all enforcement authority was transferred. Under article 25(4) of the EU Directive, the Commission is to investigate and determine the adequacy of third-country data privacy protections and "enter into negotiations with a view to remedying the situation" where it feels protections are inadequate. EU Directive, *supra* note 2, art. 25(4)–(5). Commission decisions to restrict data transfers are to be approved by Member State representatives by a qualified majority vote. *See id.* art. 31(2). "Member States shall [then] take the measures necessary to comply with the Commission's decision." *Id.* art. 25(6).

169. *See infra* Section V.A.

170. An example of this phenomenon is the constraint on U.S. use of unilateral retaliation against the European Community pursuant to section 301 of the 1974 U.S. Trade Act. *See* PATRICK LOW, TRADING FREE: THE GATT AND U.S. TRADE POLICY 91 (1993). While the United States was relatively successful in using section 301 against Japan and the newly industrialized countries of Asia during the 1980s, this approach was considerably less useful against the European Community because of the constraining impact of potential EC counter-retaliation on U.S. exports. *See id.*

171. As Joel Trachtman states, "[s]overeignty, viewed as an allocation of power and responsibility, is never lost, but only reallocated." Trachtman, *Reflections*, *supra* note 19, at 400. A "loss" of sovereignty "may be viewed as a question of what is received, and by whom, in exchange for a reduction in the state's sovereignty, rather than simply a question of whether sovereignty is reduced." *Id.* Nonetheless, ongoing Member State differences can still undercut a common EU position and weaken the Commission's negotiating stance. To the extent that a qualified majority of EU Member States do not support an aggressive Commission position on challenging third-country data privacy standards, the pooling of sovereignty will have less impact. There remain clear Member State differences in the article 31 Committee that oversees and provides instructions to the Commission regarding the EU-U.S. negotiations over data privacy protection. *See* Interviews with U.K. and Danish permanent representatives and officials from DGXV, in Brussels (June 23–24, 1999). Despite these internal disagreements, however, the point remains that the Directive has brought the United States to the table to negotiate enhanced U.S. data protection protections.

As in the case of the internal EU market liberalization, the U.S.-EU goal in the New Transatlantic Agenda of promoting trade and investment liberalization facilitates the upward leveraging of data privacy protection. The European context itself demonstrated how efforts to ensure trade liberalization can strengthen social protection within a larger geographic area.[172] In the European Union, data privacy regulation itself was not a barrier to trade. Rather, it was the lack of adequate harmonization of this protection that raised a potential barrier. By harmonizing data privacy protection, the European Union helped ensure the free flow of information within it. Similarly, it is because U.S. and EU data privacy laws are not sufficiently harmonized that the European Union can potentially block data transfers to the United States. It is because the European Union is a powerful political entity with a large market that transfer restrictions matter to the United States. It is the effort to preserve and enhance trade liberalization between the world's largest trading blocs that now facilitates the upward leveraging of data privacy protection throughout the world. Where data privacy protection is a salient interest in a powerful state, ensuring data privacy protection and enhancing trade liberalization become twin goals.

B. *Public and Private: The Multiple Means To Restrict Data Transfers to the United States*

European Union data privacy regulation poses multiple threats to U.S. companies. As described in Part II, article 25 of the EU Directive instructs the EU Member States "to comply with Commission decisions" to ban all data transfers to countries that fail to ensure adequate data privacy protection. Even if, as appears likely for political reasons, the Commission refrains from finding that the United States, as a whole, inadequately ensures data privacy protection, it can limit its determination to certain economic sectors, types of information, or operations. For example, the European Union could ban transfers of health information or transfers for direct marketing purposes.[173] In either case, affected firms would have to process information separately in

172. *See supra* Section I.A. Members with lower levels of protection also no longer have a veto power in international negotiations regarding the maintenance of the status quo. *See* Josephine Jupille, *The European Union and International Outcomes*, 53 INT'L ORG. 408, 423 (1999) (noting how collective decision-making on environmental matters by qualified majority vote has enabled the European Union to take a more proactive role in international environmental negotiations, driving standards upward in bargaining over international ozone layer protection and hazardous waste trade). Decisions in the European Union over data privacy protection are similarly taken by a qualified majority, rather than a unanimous, vote.

173. In 1998, the European Commission appointed consultants from several countries, including Robert Gellman, former Chief Counsel and Staff Director of the Subcommittee on Information, Justice, Transportation, and Agriculture of the House Committee on Government Operations, to review the adequacy of privacy protections in several areas, including human resources and medical research and epidemiology, in the United States and a number of other countries. Swire and Litan point out that this suggested that the European Commission could target enforcement in these areas. *See* SWIRE & LITAN, *supra* note 99, at 171–72.

governmental authorities can attempt to manage the ensuing transatlantic conflicts, devising new mechanisms to accommodate each other's larger interests. These mechanisms, however, can give rise to new domestic tools for promoting data privacy protection.

C. *Conflict Management: U.S.-EU Negotiations over Adequacy*

The United States and the European Union are attempting to negotiate a solution to the data privacy controversy. Pressure from U.S. firms makes this a high profile issue for the U.S. administration. In line with business views, the Clinton Administration maintains, as its negotiating position, that industry should be "self-regulating" in its use of personal data.[181] United States Commerce officials defend U.S. practices, critiquing the European Union for its "top-down approach" of "privacy czars and bureaucrats" as antithetical to U.S. traditions of limited governmental intrusion into the private sector.[182] Yet to avoid a regulatory conflict, U.S. officials simultaneously prompt businesses to create "self-regulatory" procedures more protective of individual privacy.[183] Entering the fray, U.S. privacy advocates, skeptical of "self-regulation," press for further legislation.[184]

The European Union has delayed enforcing the EU Directive's provisions on third-country transfers while negotiations take place.[185] The United States remains a formidable negotiating opponent because the U.S. market is also the largest foreign market for EU firms, buttressing U.S. negotiating clout.[186] European Union commercial interests press their Member

---

181. *See* David Banisar, *The Privacy Threat to Electronic Commerce*, COMM. WK. INT'L, June 1, 1998, at 8. However, there are divisions within the administration on privacy issues as presented in Section V.A., *infra*.

182. Andrews, *supra* note 81, at A1 (quoting David Aaron, Under Secretary of Commerce); *see also* U.S. GOVERNMENT WORKING GROUP ON ELECTRONIC COMMERCE, FIRST ANNUAL REPORT 18 (1998) (critiquing the EU's "broad, centralized, top-down approach to privacy protection" that could disrupt "the free flow of information") [hereinafter WORKING GROUP FIRST ANNUAL REPORT].

183. *See infra* note 248 and accompanying text.

184. Privacy advocate Marc Rotenberg of EPIC has criticized the policy of U.S. officials: "[A]t the end of the day, it can be fairly asked whether the administration's policy was based on self-regulation or on promoting business interests." Jeri Clausing, *U.S. Report on Net Commerce Set for Release*, N.Y. TIMES, Nov. 30, 1998, at C1 (quoting Rotenberg). One problem with the self-regulatory approach advocated by the U.S. Department of Commerce is that, even if one is granted the formal right to retain confidentiality of one's personal data, that right is meaningless if not accompanied by the power to do something about its disclosure. The Department of Commerce critiques the EU approach as "top-down," yet the EU approach gives individuals the right to act as private attorneys general to ensure that businesses adopt the principles advertised in self-regulatory systems. The focus of enforcement depends on "bottom-up" citizen activism in the tradition of much of American law. It is this American tradition that may in fact most concern U.S. businesses. *See infra* notes 325–326 and accompanying text.

185. *See EU States Endorse Standstill with U.S. on Transfers of Data During Privacy Talks*, 15 Int'l Trade Rep. (BNA) 1789 (Oct. 28, 1998).

186. This raises the questions of why the U.S. exercise of market power will not cause the EU data privacy protections to be lowered, and why U.S. pressures do not affect the playing field in Europe by providing leverage for EU businesses to demand that data privacy requirements be eased. While this Article does not focus on the internal EU situation, the following points are noted. First, there are powerful internal reasons why the European Union has enacted data privacy protections and why EU businesses have not been able to thwart this, though they clearly tried when the contents of the EU Directive were initially negotiated. *See supra* note 147. In addition, now that EU businesses are subject

Europe or apply for an exemption from Member State supervisory authorities. Firms are not allured.[174]

Member State authorities can also independently fine individual companies and enjoin them from transferring data, including data to their U.S. affiliates.[175] Company officials can even be imprisoned. Though imprisonment is unlikely, company officials will not wish to test its likelihood. Privacy rights associations can trigger these proceedings by filing claims with supervisory authorities. They have put companies on notice that they will do so.[176]

Individuals and, depending on a Member State's standing rules, privacy rights associations can also sue companies for damages before Member State courts or through referral to administrative bodies. In the Internet era, U.S. companies whose only presence in Europe is the availability of their websites can be subject to claims before European courts.[177] American companies are already subject to EU-based claims. The United Kingdom fined the U.S. Robotics Corporation "for failing to register under the UK's Data Protection Act and for obtaining personal information about individual visitors to its Web site and then using that information to market other products."[178] American Airlines is appealing a Swedish court ruling that bars it from transferring data from Sweden to its U.S. electronic reservation system without first obtaining customer consent.[179] Other data transfers to the United States have been barred by British, French, and German courts and administrative authorities.[180]

In liberal regimes, law is not the monopoly of the state and its representatives. The EU Directive is now in force. It takes on a life of its own. Private parties can use it before courts and administrative bodies in ways that the original drafters did not predict. In an institutionally interdependent world,

174. Operating a new processing facility would cost tens of millions of dollars per year. A Harvard Business School study found that a data processing center costs between $15 and $50 million a year in hardware and maintenance, depending on the size of the center. *See id.* at 54 (citing David B. Yoffie & Tarun Khanna, *Microsoft Goes Online: MSN 1996*, Harvard Business School reprint N9-797-088 (1997)).

175. The EU Directive arguably covers ad hoc transfers of information, such as by e-mail, concerning company employees, customers, or suppliers. The EU Directive could affect a company's ability to transfer human resources records where companies centralize compensation and benefits information, skills databases, and related records; or information about customers and employees to business consultants and auditors. *See* Peter Swire, *The Great Wall of Europe*, CIO ENTERPRISE MAG., Feb. 15, 1998, at 26.

176. Just before the EU Directive went into effect, Privacy International, a London-based privacy organization, warned that it would oversee the EU Directive's application to ensure its enforcement. It threatened to file claims against American Express and EDS for failing to provide adequate data privacy protection. *See Will Amex and EDS Privacy Lawsuits in Europe?*, COMPUTERGRAM INT'L, July 2, 1998, *available in* 1998 WL 13761936.

177. Member States could claim jurisdiction over U.S. companies on the basis of (i) their actions in the Member State in question; or (ii) the "effects" on individuals in the Member State on account of actions taken in the United States. On the issue of jurisdiction, see *supra* note 6.

178. Gidari & Aglion, *supra* note 80, at B7.

179. *See The EU's Privacy Law*, CHRISTIAN SCI. MONITOR, Nov. 12, 1998, at 12.

180. *See* Cate, *supra* note 27, at 438 (citing prohibitions on data transfers to the United States from Britain (involving sales to a direct mail organization) and France (involving patient records)). As for Germany, see *infra* text accompanying note 354.

State representatives and EU officials to avoid a transatlantic trade war over data privacy issues. A ban would not only impede data transfers, it would hamper further tariff negotiations and mutual recognition agreements in areas important to both large U.S. and EU commercial interests.[187]

In addition, only a minority of the fifteen EU Member States have so far enacted legislation implementing the EU Directive, even though they were all to have done so by October 25, 1998.[188] Even though this Member State failure is due primarily to legislative inertia and not to opposition to data privacy controls per se, their failure undermines the Commission's negotiating position. Were the European Union to ban data transfers to the United States before all Member States themselves implemented the EU Directive's protections, the ban could be more vulnerable to a U.S. claim that it violates international trading rules.[189] European Union authorities act in the shadow of a supranational institution, the World Trade Organization, and are subject to constraints imposed by its rules.

The United States proposes that the European Union and the United States agree to a set of core data privacy protection principles pursuant to which U.S. company "self-regulation" would be deemed adequate so long as it complies with these principles.[190] The United States maintains that compliance must provide companies with a "safe harbor" against any challenge by EU authorities to their data processing practices. The European Union, however, rejected the U.S.'s initial proposals as inadequate. Although

---

to EU and Member State controls, they would like these controls to be applied by the United States to their U.S. competitors as well. For a discussion of the protectionist aspects of the EU Directive, see *infra* note 193. Nonetheless, the EU Directive grants Member States flexibility in its implementation. As Bainbridge notes, there remain some pressures on Member States to implement the EU Directive in a business-friendly manner, where permissible, so as to attract data processing operations to their jurisdiction. *See* Bainbridge, *Legal Analysis*, *supra* note 45, at 73.

187. *See supra* note 167 and accompanying text. To give just one example, the European Union has indicated that unless there is an agreement by the WTO ministerial meeting in Seattle, Washington, in November 1999, it will block U.S. efforts to make permanent a moratorium on imposing customs duties on electronic transmissions. *See EU Says It Will Not Support WTO E-Commerce Moratorium*, 16 Int'l Trade Rep. (BNA) 1162 (July 14, 1999).

188. The Commission initiated proceedings that could eventually go before the European Court of Justice against nine (of the fifteen) Member States on July 29, 1999, challenging their failure to implement the EU Directive. *See* Joe Kirwin, *Privacy: Eyeing Talks with U.S., EC Moves To Spur Members To Implement Data Privacy Rules*, Int'l Bus. & Fin. Daily (BNA) D14 (July 30, 1999). Nonetheless, under the EU "direct effect" doctrine, individuals may invoke the provisions of the data privacy Directive in national courts even where the Member State has yet to implement the EU Directive through national legislation. Individuals injured as a result of a state's failure to pass such implementing legislation may still seek reparation before national courts. *See Directive on Personal Data Enters into Effect* (visited Jan. 13, 1999) <http://europa.eu.int/comm/dg15/en/media/dataprot/news/925.htm>; *see also U.S., EU Narrow Differences in Talks on EU Privacy Directive, Officials Say*, 15 Int'l Trade Rep. (BNA) 1695 (Oct. 14, 1998) (quoting John Mogg, Director General of the European Commission for the Internal Market, who said that "even without implementation by every member state . . . the directive will take effect under the EU's 'direct effect' doctrine").

189. *See infra* Part IV. As one EU representative confirmed, "considering that only four or five member states have implemented the data privacy directive, taking such a measure [a ban on transfers] would be inconsistent." *EU Rejects U.S. Data Privacy Plan*, 15 Int'l Trade Rep. (BNA) 1963 (Nov. 25, 1998).

190. *See infra* notes 249–259 and accompanying text.

U.S.-EU discussions may soon result in a negotiated compromise,[191] the European Union has confirmed that it will enforce the EU Directive's provisions banning data transfers to third countries if a satisfactory solution is not reached. EU authorities note that were the European Union to agree to "safe harbor" provisions to remove the threat of a ban, EU residents would retain their right to file private complaints before EU Member State courts and administrative bodies against companies that transfer personal information to the United States "without adequate protecting privacy."[192] In an institutionally interdependent world, U.S. officials negotiate safe harbor requirements under the pressure of these threats.

IV. THE SUPRANATIONAL CONTEXT: THE CONSTRAINTS OF INTERNATIONAL TRADE RULES

The EU Directive's extra-jurisdictional impacts could be beneficial—if the United States currently under-regulates data privacy protection—or detrimental if the European Union over-regulates. The extra-jurisdictional effects of EU regulatory dictates can be constrained, and U.S. national autonomy preserved, by supranational trade rules. Yet in the case of EU data privacy protection, supranational trade rules offer the United States only limited recourse. This part commences by presenting the grounds for a U.S. claim that the EU Directive violates the supranational rules of the world trading system, which constrain countries' abilities to restrict trade (Section A). It then evaluates why the United States would likely not prevail under WTO rules (Section B), in particular in light of the procedural concerns articulated in recent WTO jurisprudence (Section C). The Part concludes that WTO rules provide little protection to the United States from external pressures to raise privacy standards. On the contrary, WTO rules help shield the European Union from U.S. retaliation against application of the EU Directive. Ironically, contrary to popular conceptions, by constraining the U.S. ability to retaliate against the EU Directive's application, WTO rules reinforce the EU Directive's extra-jurisdictional effects (Section D). They thereby enable a trading up of U.S. standards.

A. *WTO Constraints on the European Union: Claims That the EU Directive Violates WTO Rules*

There are arguably some protectionist motives behind the EU Directive. United States businesses are more advanced in the use of information technology than are EU businesses. European Union businesses, unable to forestall EU regulation, would like to level the playing field so that U.S.

191. *See, e.g., EU Official Encouraged by "Greater Clarity" in U.S. Stance on Data Privacy Enforcement*, Int'l Trade Rep. (BNA) (Sept. 22, 1999); Robert MacMillan, *EU, U.S. Predict Data Accord by End of '99*, NEWSBYTES, Sept. 24, 1999, *available in* 1999 WL 20020294.

192. *EU Rejects U.S. Data Privacy Plan*, *supra* note 189, at 196 (noting remarks of Gerrit de Graaf, First Secretary of the European Union).

businesses must operate under similar constraints.[193] In an attempt to ward off EU action, U.S. officials implicitly threatened to challenge any ban imposed by the European Union before the Dispute Settlement Body of the World Trade Organization (WTO).[194] The threshold issue under WTO rules is whether the transfer of data constitutes a sale of goods or of services: If it is a sale of goods, the transfer is covered by the 1994 General Agreement on Tariffs and Trade (GATT 1994);[195] if it is a service, the transfer is covered by the General Agreement on Trade in Services (GATS).[196]

Data is typically transferred across the Atlantic electronically, as part of an electronic message. In March 1998, the WTO Secretariat issued a report entitled *Electronic Commerce and the Role of the WTO* that addresses, among other matters, the coverage of electronic transactions under present WTO agreements.[197] As noted by the report, "[e]lectronic commerce could be

193. The potential protectionist impacts of the EU Directive are discussed in SWIRE & LITAN, *supra* note 99, at 145, 189. A primary protectionist concern is that, through causing the United States to raise its data privacy requirements, the European Union would level the playing field by increasing data privacy protection costs for U.S. firms, since U.S.-based firms would henceforth be subject to similar constraints in the use of information. Swire and Litan also note that the EU Directive could favor EU data processors to the extent that firms decide to use separate data processing facilities in Europe. Similarly, they maintain that the EU Directive could favor EU service providers to the extent that firms decide to do business with EU-based firms to whom they can freely transfer data, and not with U.S.-based firms. *See id.* However, these impacts are difficult to measure and, as discussed below, are not the result of de jure discrimination because all firms would still be subject to the EU Directive's requirements.

194. For example, Ira Magaziner, the senior Clinton Administration official overseeing electronic commerce issues at the time, including privacy issues, stated: "In general, we [in the United States] don't recognize an extra-territorial attempt to shut down the electronic flow of data between countries . . . . According to principles of international trade, I think that's a violation of WTO rules." Kenneth Cukier, *U.S. Under Fire over 'Aggressive' Net Tax Stance*, COMM. WK. INT'L, Mar. 2, 1998, at 17 (quoting Magaziner).

195. General Agreement on Tariffs and Trade, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1A, 33 I.L.M. 1154 (1994) [hereinafter GATT 1994]. GATT 1994 incorporates the General Agreement on Tariffs and Trade, Oct. 30, 1947, 55 U.N.T.S. 194 [hereinafter GATT], as amended. *See* GATT 1994, art. 1(a).

196. General Agreement on Trade in Services, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1B, LEGAL INSTRUMENTS—RESULTS OF THE URUGUAY ROUND, vol. 31, 33 I.L.M. 1167 (1994). Another possibility is that both GATT and GATS would apply. The WTO Appellate Body has held that both agreements may apply to the same set of facts. *See, e.g.*, World Trade Organization, *Report of the Appellate Body on the European Communities Regime for the Importation, Sale and Distribution of Bananas*, WT/DS27/AB/R (Aug. 22, 1997), *reprinted in* 37 I.L.M. 243, 244 (1998).

The use of the term supranational "rules" is delicate according to some U.S. trade officials. They fear that the term "supranational rule" conjures up an image of a supranational legislative body drafting secondary legislation, which that body independently enforces against infringing governments and even those governments' constituents. *See* Telephone Interview with Donald Abelson, Chief Negotiator for Communications and Information, Office of the U.S. Trade Representative (USTR) (Apr. 19, 1999). However, in other contexts, USTR officials praise the WTO for being a "rule-based" institution. The different positions depend on whether the USTR is defending the need for WTO rules to protect U.S. export interests before Congress, or defending the autonomy of U.S. policy-making despite WTO rules. This Article refers to the constraints of supranational rules. It does so because the infringement of WTO provisions can lead to litigation before WTO dispute settlement panels, with a right of appeal to the WTO Appellate Body. This can ultimately result in WTO-authorized sanctions against the infringing WTO member, and can constrain government action.

197. *See* WORLD TRADE ORGANIZATION, ELECTRONIC COMMERCE AND THE ROLE OF THE WTO (1998). The report represents views of its specific authors, not the WTO or WTO Secretariat as a whole.

characterized as trade in goods, trade in services, or as something different from either of these."[198] The report considers that a book sold over the Internet in digital form is a good since it is a "standardized product," but that "customized data . . . would be treated as non-standardized products and classified as services."[199] To the extent that personal data is a non-standardized product, its transfer should thus be covered under GATS, and not GATT 1994.[200]

WTO members' obligations under GATS are substantially less than under GATT 1994. Most GATS obligations only apply if the service in question is specifically included in a schedule of market access commitments. The EU schedule of commitments is complicated, set forth in charts comprising over one hundred pages, containing numerous exceptions and qualifications, and amended by four subsequent "supplements," which in turn have been revised.[201] The European Union has made market access commitments for "Telecommunications Services" (including "basic" and "value-added telecommunications"), which could cover data transfers.[202] It has also made commitments for numerous other service sectors and activities that could be affected by data transfer restrictions, including medical, retailing, advertising, computer reservations, executive searches and placements, data processing, consulting, insurance, banking, and various financial services.[203]

198. *Id.* at 50.

199. *Id.* at 51. The report concludes that "many products which can be delivered between jurisdictions as digitalized information flows are classified as services" under the existing GATS framework. *Id.* at 52.

200. *See Electronic Commerce Is Covered by Services Accord, WTO Report Says*, 15 Int'l Trade Rep. (BNA) 1261 (July 22, 1998). On September 25, 1998, WTO members created a work program to review further electronic commerce issues under the relevant WTO Agreements, including under GATT 1994 and GATS. *See* WTO General Council, Work Programme on Electronic Commerce WT/L/274 (Sept. 30, 1998). In the WTO Work Programme, the issue of "protection of privacy" is to be treated under "the GATS legal framework." *WTO Members Outline Views for Future Talks on Electronic Commerce*, 15 Int'l Trade Rep. (BNA) 1627 (Sept. 30, 1998). The work program issued a report submitted in the summer of 1999 showing that WTO members have been unable to overcome their longstanding disagreement on whether all electronic deliveries are services or whether some transfers should be classified as goods. *See WTO Services Body Submits E-Commerce Report Showing Major Gaps*, INSIDE U.S. TRADE 4 (Aug. 6, 1999). The European Union maintains that all electronic transactions should be classified as trade in services while the United States maintains that some should be classified as trade in goods. The work program report is to be modified and combined with others for purposes of the November 30, 1999 WTO Ministerial meeting in Seattle, Washington. *See, e.g., WTO Delegates Debate Draft Declaration Issued by General Council for Next Round*, 16 Int'l Trade Rep. 1642 (BNA) (Oct. 13, 1999). One outside possibility is that data privacy protections could themselves be incorporated into WTO rules just as intellectual property protections have been incorporated under the WTO TRIPS Agreement (Agreement on Trade-Related Aspects of Intellectually Property Rights). However, while business organizations intensively pressured U.S. and EU authorities to incorporate intellectual property protection into WTO rules, businesses will likely oppose the incorporation of stringent data privacy protections. Business opposition to privacy regulation is discussed generally in Section V.C, *infra*.

201. *See* European Communities and their Member States, Schedule of Specific Commitments GATS/SC31 (Apr. 15, 1994), *supplemented by* GATS/SC31/Suppl.1 (July 28, 1995); GATS/SC/31/Suppl.1/Rev.1 (Oct. 4, 1995); GATS/SC/31/Suppl.2 (July 28, 1995); GATS/SC31/Suppl.3 (Apr. 11, 1997); GATS/SC/31/Suppl.4 (Feb. 26, 1998) [hereinafter EU Schedules].

202. *See id.*; Telephone Interview with Donald Abelson, Chief Negotiator for Communications and Information, Office of the U.S. Trade Representative (Dec. 7, 1998).

203. *See* EU Schedules, *supra* note 201.

Because the telecommunications commitments only cover the "transport of electromagnetic signals" and not the "content" of those signals, arguably only obligations under sector-specific commitments would apply.[204]

If a data transfer is covered under one of the EU commitments, then the European Union is obliged to treat U.S. service providers no less favorably than EU service providers[205] and to apply its domestic regulation in a "reasonable" manner.[206] It is the claim of reasonableness that could lie at the core of a U.S. action. In addition, were the European Union to ban data transfers only to the United States, but not to other WTO members that inadequately protect data privacy under the EU criteria, the European Union could violate the GATS most-favored-nations clause under article II.[207]

B. *Why the United States Should Not Prevail*

The United States would likely not prevail in an action before the WTO Dispute Settlement Body for three primary reasons. First, on its face, the EU Directive applies equally to transfers to all countries and thus should not

---

204. *See* Supplement 3 (Sector 2.C Telecommunications Services) in EU Schedules, *supra* note 201. Any EU data transfer restriction would be based on the data's content, such as an individual's health, employment, or purchase records, and not on the act of telecommunication transmission itself. The EU schedule for commitments in telecommunications services provides, "Telecommunications services are the transport of electro-magnetic signals—sound, data image and any combinations thereof, excluding broadcasting [which is separately defined]. Therefore, commitments in this schedule do not cover the economic activity consisting of content provision which require telecommunications services for its transport. The provision of that content, transported via a telecommunications service, is subject to the specific commitments undertaken by the European Communities and their member states in other relevant sectors." *Id.*

205. *See* GATS, art. XVII.

206. GATS, art. VI. There are other technical legal defenses that the European Union might invoke were a case brought before a WTO panel. For example, the transfer of personal data to a third country may constitute an *export* of services to which GATS does not apply (unlike GATT, which applies to imports and exports). Article XVII of GATS, the national treatment clause, provides that "each member shall accord to services and service suppliers of any other member, in respect of all measures affecting the supply of services, treatment no less favorable than that it accords to its own like services and service suppliers." GATS, art. XVII. The wording suggests that the provision could apply only to EU internal requirements for the provision of services, and not to the export of services. *See* E-mail Message from Eric White, Legal Services Division of the European Commission (May 24, 1999) (on file with author). In this respect, see the GATS definition of "service of another Member" in GATS, art. XXVIII(F).

It is also questionable whether intra-corporate group data transfers constitute a commercial service operation covered by GATS, especially where there is no contract or consideration for the transfer. The United States (as claimant) might contend, on the one hand, that an export ban generally prejudices the supply of services by U.S.-owned service providers in the European Union, because they are more likely to be affected than EU-owned service providers. The European Union might respond that such an indirect effect on the provision of services in the European Union could not be covered under GATS because ultimately all measures have indirect effects. The United States might, in turn, counter that a ban on data transfers to the United States clearly has foreseeable effects on the provision of services by U.S.-owned service providers in the EU market, in which case they are discriminatory and thus prohibited under GATS.

207. *See* GATS, art. II. Under the most-favored-nations clause, the European Union cannot accord less favorable treatment to U.S. services and service suppliers than to those of any other WTO members. *See id.* This latter obligation is not limited to those commitments made in the EU Schedules to GATS, but rather applies to EU treatment of all U.S. services and service providers.

violate the GATS most-favored-nations clause.[208] It applies equally to EU-owned and -registered companies and foreign-owned and -registered companies and thus should not violate the GATS national treatment clause.[209] So long as the European Union does not clearly discriminate against the United States or U.S. service providers in its application of the EU Directive, the United States would likely not prevail.

Second, the European Union has a legitimate public policy objective—to protect the privacy of EU residents who are the subjects of data transferred to the United States. The GATS general exception clause in article XIV explicitly authorizes WTO members to restrict commerce in order to protect "the privacy of individuals."[210] This provision significantly bolsters the EU defense. While GATS's thrust is to liberalize trade in services, under article XIV, WTO members may adopt and enforce measures relating to services that are "*necessary* to secure compliance with laws or regulations not inconsistent with the provisions of this Agreement, including those relating to: . . . the *protection of the privacy* of individuals in relation to the processing dissemination of personal data and the protection of confidentiality of individual records and accounts" so long as they "are not applied in a manner which would constitute a means of arbitrary or *unjustifiable discrimination* between countries where like conditions prevail, or a *disguised restriction on trade* in services."[211] Given the express language and given that the privacy interests of EU residents are directly at stake, it is unlikely that a WTO panel would find the EU Directive's content to be "unreasonable."[212]

---

208. *See id.*

209. *See id.* art. XVII. The United States has recognized this non-discriminatory aspect of the EU Directive. As Assistant Secretary of Commerce Franklin Vargo reported to the U.S. Congress, "[t]he effect [of a ban on data transfers] would not be one-sided, and European firms would suffer as badly or even worse than U.S. firms if they were suddenly unable to process and send across the Atlantic financial information, personnel records, and many other forms of information vital to business." *Issues in U.S.-European Union Trade: European Privacy Legislation and Biotechnology/Food Safety Policy, supra* note 162.

210. GATS, art. XIV.

211. *Id.* (emphasis added). Whereas the former GATT exception clause contains only broad language referring to securing "compliance with laws or regulations," the new GATS exception includes "the protection of privacy" as a specific example of laws and regulations to which deference is to be granted. GATS, art. XIV. Compare the GATT exception clause in GATT, art. XX.

As noted above, it is unlikely that a transfer of personal data will be deemed a good covered under GATT 1994. If it were, the United States would claim that the EU ban violates the prohibition of quantitative restrictions, including bans, on "the exportation or sale for export of any product" to another WTO member. *See* GATT, art. XI. Even if the data transfer is found to involve a trade in goods, the EU ban should still be permitted under the GATT exception clause, provided the European Union does not apply the ban in a clearly discriminatory manner. *See id.* art. XX. GATT article XX provides that WTO members may adopt and enforce measures that do not constitute "arbitrary or unjustifiable discrimination," which are either "necessary to protect human . . . life or health" or "necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement." *Id.* The relevant generic language ("necessary to secure laws or obligations") in the GATS exception clause (article XIV) is taken from the GATT exception clause (article XX). In the end, the characterization of transferred data as a good or a service should be irrelevant.

212. Lax foreign regulations have externalities that can undermine the EU Directive's goal of protecting the privacy of EU residents. *See supra* note 20 and accompanying text; *infra* text accompanying note 370.

Faced with this defense, the United States would focus on the conditions for article XIV's invocation, in particular that a trade restriction be "necessary to secure compliance with laws."[213] In support, the United States would note that prior trade panels have interpreted the term "necessary" to require a measure to be the "least trade-restrictive" available,[214] and that, in general, exceptions to GATS obligations are to be applied restrictively. The United States would contend that its policies are adequate under international norms, and EU restrictions are thus neither reasonable nor necessary.[215] In all events, the United States would affirm that a case-by-case ban on transfers is clearly less trade restrictive than a country-wide ban, and thus that any ban is excessive under WTO criteria.[216]

Third, although the United States has some arguments in its favor, a WTO panel will be wary of engaging in a delicate balancing of trade and privacy interests, particularly since the privacy of residents within the European Union—as opposed to outside the European Union—is directly at stake. Under media scrutiny, WTO dispute settlement panels would prefer to refrain from engaging in a close balancing of competing trade and privacy interests, and rather review the process by which the European Union takes account of foreign privacy protections. This is the approach recently taken by the WTO Appellate Body in an analogous case.

---

213. GATS, art. XIV.

214. *See* Thailand: Import Restrictions on Importation of and Internal Taxes on Cigarettes, Nov. 7, 1990, B.I.S.D. 37S/200, para. 75.

215. The United States might argue, for example, that the European Union and other developed countries have negotiated and agreed to a set of privacy principles that reflect a multilateral consensus of what is "reasonable." These principles, agreed to on September 23, 1980 by the members of the Organization for Economic Development (OECD), are set forth in *Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, 20 I.L.M. 422 (1981). However, the OECD principles are merely hortatory and not enforceable, nor do they bind the European Union in its determination of what is "reasonable" to protect its citizens and residents. Moreover, it is questionable whether the United States actually complies with the OECD guidelines.

The United States might also argue that the EU Directive is unreasonable given the nature of developments in telecommunications. For example, electronic mail is now commonly used but was less of an issue when the EU Directive was first enacted. To the extent that the EU Directive applies to most electronic mail communications, the United States might argue that this is excessive. *See* SWIRE & LITAN, *supra* note 99, at 189–93. The European Union may respond, however, that these technological developments render the need for privacy protection even more important.

216. The United States would also note that the introductory clause to article XIV sets forth an additional condition—that EU restrictions must not constitute "arbitrary or unjustifiable discrimination." GATS, art. XIV. If the European Union were, in practice, to apply the EU Directive in a discriminatory manner vis-à-vis the United States or U.S.-controlled companies, it would fail to comply with this core condition. The European Commission thus needs to assure that it treats other WTO members similarly before implementing a ban on data transfers to any single country. It must likewise refrain from specifically targeting U.S.-owned companies. As Scott Blackmer, an attorney from the Washington D.C. firm of Wilmer, Cutler & Pickering, observes, "[i]f all the enforcement heat falls on a handful of U.S. multinationals, the U.S. can bring a complaint to the World Trade Organization's new dispute resolution body." *Will Amex and EDS Privacy Lawsuits in Europe?*, *supra* note 176.

C. *A Focus on Process: The EU Directive Under the WTO's New Criteria*

The EU regulation of data privacy protection is "extra-jurisdictional" in its focus in that it is concerned with the adequacy of data privacy protection outside EU jurisdiction. The recent WTO Appellate Body Report in the *Shrimp-Turtle Case*,[217] which concerned a U.S. ban of foreign shrimp imports on account of a U.S. finding of inadequate sea turtle conservation policies in South and Southeast Asia, confirms the EU's strong position from a procedural standpoint. Even though, in the shrimp-turtle case, the WTO Appellate Body held that the U.S. application of its law violated GATT rules and was not protected by the GATT general exception clause,[218] the Appellate Body enumerated a number of relevant criteria that support an EU defense. The Appellate Body held that U.S. law fell within the scope of the article XX exception clause but that the law's application by the U.S. Department of State was arbitrary and discriminatory.[219] The United States thus failed to comply with article XX's conditions on the following procedural grounds:

(i) The United States required all exporting WTO members to adopt "essentially the same [conservation] policy," and not merely "comparable" ones;

(ii) The United States failed to take "into consideration the different conditions which may occur in the territories . . . of different members";

(iii) The United States did not seriously attempt to reach a multilateral solution;

(iv) Under its country-wide ban, the United States prohibited shrimp imports even where vessels caught them using U.S.-prescribed methods; and

217. Report of The Appellate Body, United States—Import Prohibition of Certain Shrimp and Shrimp Products, WT/DS58/AB/R (Oct. 12, 1998), *available in* 1998 WL 716669 (W.T.O. Oct. 12, 1998) [hereinafter AB Shrimp-Turtle Report]. For an overview and analysis of the Appellate Body shrimp-turtle decision, see Gregory Shaffer, *United States—Import Prohibition of Certain Shrimp and Shrimp Products*, 93 AM. J. INT'L L. 507 (1999) [hereinafter Shaffer, *Import Prohibition*]; and Gregory Shaffer, *The U.S. Shrimp-Turtle Appellate Body Report: Setting Guidelines Toward Moderating the Trade-Environment Conflict*, BRIDGES, Oct. 1998, at 9 [hereinafter Shaffer, *Shrimp-Turtle*]. The shrimp-turtle case applied article XX of GATT 1994 (the general exception provisions) to the United States. The United States prescribed a particular method, the use of devices known as turtle excluder devices (TEDs), which enable sea turtles to escape from shrimp nets to avoid drowning. Significantly, the Appellate Body held that the underlying U.S. conservation law did not violate WTO rules. *See* Shaffer, *Import Prohibition*, *supra*.

218. *See* GATT, art. XX. For further information on article XX, the model for the GATS exception clause, see *supra* note 211.

219. *See* AB Shrimp-Turtle Report, *supra* note 217, at 83.

(v) The U.S. certification process was not transparent or predictable.[220]

The EU application of the EU Directive should meet these Appellate Body criteria for permissible extra-jurisdictional measures. First, unlike the U.S. guidelines applied to foreign shrimping practices, the EU Directive only requires that states ensure "adequate" privacy protection, not that they adopt "essentially the same" protection. Second, whereas the United States did not examine differentiating conditions in individual countries, the European Union has created a Working Group to report on individual country practices and conditions that affect the privacy of EU residents.[221] The European Union specifically commissioned a detailed report on U.S. practices from Professors Paul Schwartz and Joel Reidenberg, which is now published as a book of over 490 pages entitled *Data Privacy Law: A Study of United States Data Protection*.[222]

Third, the European Union has engaged in prolonged, detailed discussions with U.S. representatives to examine data privacy safeguards that could be applied.[223] If the U.S.-EU discussions do not result in a negotiated solution and restrictions are ultimately imposed, the European Union will have strong grounds to claim that the restrictions were "necessary" on account of the parties' failure to reach a solution that adequately protected EU residents. In the shrimp-turtle case, on the other hand, the United States did not offer to enter into negotiations with the concerned countries in South and Southeast Asia until after its ban went into effect.[224]

Fourth, the EU Directive specifically provides that individual companies meeting EU requirements may still transfer data to the United States despite the imposition of a country-wide ban.[225] Even if the European Union finds U.S. data protection laws inadequate, individual companies could obtain exemptions by demonstrating that they employ adequate internal policies. The EU Directive also creates express exceptions to a general ban, including where the individual data subject "unambiguously" consents to the transfer

---

220. *See* AB Shrimp-Turtle Report, *supra* note 209, at 69–83 (paras. 161–186). The U.S. implementation of the ban was also faulted for applying different "phase-in" periods for different countries and for expending greater efforts to transfer the required TED technology to certain developing countries than others. *See* Shaffer, *Import Prohibition*, *supra* note 217, at 512. Only if the EU ban goes into effect will the issue of "phase-in" periods arise. However, the technology transfer issue is inapposite to the United States.

221. *See supra* note 77 and accompanying text.

222. SCHWARTZ & REIDENBERG, *supra* note 84.

223. *See supra* Section III.C.

224. *See* AB Shrimp-Turtle Report, *supra* note 217, at 71–73 (para. 166).

225. Article 26(2) of the EU Directive provides that:

> [A] Member State may authorize a transfer or set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25(2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.

EU Directive, *supra* note 2, art. 26(2).

and is informed as to how the data will be used, and where "the transfer is necessary for the . . . performance of a contract concluded in the interest of the data subject."[226] The U.S. shrimping guidelines, on the other hand, did not permit any exceptions to its country-wide ban, even where individual companies implemented the very measures mandated by the United States.[227]

Fifth, unlike South and Southeast Asian authorities in the U.S. shrimp-turtle case, U.S. authorities and companies have had access to EU officials to comment on the EU Directive and its applications. This access has been both direct and in coordination with EU companies through the Transatlantic Business Dialogue.[228] In addition, procedures for companies to receive authorization for data transfers will likely be transparent and provide for administrative or judicial review of supervisory authority decisions. The U.S. Department of State provided for no such review in its initial guidelines applying to foreign shrimp imports.

Most importantly, the privacy provisions will receive more deference because in the shrimp-turtle case, the U.S. statute was aimed at protecting marine animals located outside of U.S. territorial waters. From a WTO perspective, the EU Directive is more defensible because it regulates product-related standards that affect EU residents, and not non-product-related production processes that affect only foreign residents. In the case of the EU Directive, its aim is to protect the privacy of persons residing within the European Union, not outside of it.[229]

D. *Reinforcing a Trading Up: WTO Rules as an EU Shield*

WTO supranational trade rules offer U.S. authorities only a limited check on the EU Directive's application, primarily by constraining the EU's ability to discriminate against U.S.-based companies. WTO rules thus do not relieve the pressure on the United States to raise its data privacy standards. Rather, WTO rules constrain the U.S.'s ability to retaliate unilaterally against the European Union for harming U.S. commercial interests. Were the United

---

226. *Id.* art. 26. As an example of the operation of the latter exception, a data transfer pursuant to which the name and address of a customer were transmitted to the United States solely for purposes of shipping goods to that customer pursuant to an order would be permissible. Any additional information concerning the customer, however, would likely be deemed unnecessary and thus could not be processed without the customer's consent.

227. *See* AB Shrimp-Turtle Report, *supra* note 217, at 71 (para. 165).

228. *See* discussion of TABD, *supra* note 167, *infra* note 315 and accompanying text.

229. WTO trade rules treat trade restrictions based solely on non-product-related production processes less favorably because they can be used to coerce foreign jurisdictions to change regulatory practices on competitiveness grounds in a context where the health and safety of domestic residents is not at issue. Product characteristics and product-related production processes, on the other hand, can directly affect the residents of the regulating country. *See* ERNST-ULRICH PETERSMANN, INTERNATIONAL AND EUROPEAN TRADE AND ENVIRONMENTAL LAW AFTER THE URUGUAY ROUND 18, 29–35 (1995). The EU regulation of the way data is processed directly affects the data's content (i.e., whether personal information is included with an EU resident's consent). The processing is an integral part of the product, which ultimately affects EU residents. On the other hand, the U.S. regulation in the shrimp-turtle case concerned a foreign production method (shrimp harvesting), which did not affect the product's content or characteristics.

States to so retaliate, it would itself violate WTO rules and be subject to an EU complaint before the WTO's Dispute Settlement Body.[230]

WTO supranational trade rules are often criticized for limiting the ability of countries to enact socially-oriented legislation because WTO rules are primarily "negative" in their orientation. That is, they limit the grounds under which states can restrict trade. In particular, they obligate states not to restrict imports on account of non-product-related foreign production methods, such as "unfair" environmental or labor practices that result in foreign environmental harm or foreign labor repression.[231] Paradoxically, in the case of data privacy, rather than protecting the United States from coercion to raise U.S. privacy standards, WTO rules shield the European Union from a countervailing retaliatory threat. WTO rules thereby reinforce pressure on the United States to negotiate with the European Union a set of "positive," more stringent, data privacy requirements. WTO rules thereby contribute to a trading up of U.S. standards.

V. THE EU DIRECTIVE'S EXTRA-JURISDICTIONAL EFFECTS IN THE UNITED STATES: CHANGING THE STAKES OF DOMESTIC PLAYERS

Because the EU Directive applies to data transfers worldwide, it has extra-jurisdictional effects. United States businesses feel the greatest impact because they engage in more European transactions than other foreigners and because they make the most sophisticated use of information on account of their technological edge.[232] The EU Directive has drawn attention to data privacy issues in the United States. It has pressed U.S. governmental authorities to address the adequacy of current U.S. data privacy regulation in order to fend off a regulatory conflict with the European Union (Section A). It has armed U.S. privacy advocates in their efforts to promote stronger U.S. protections through lobbying legislatures and agencies, intervening before courts, and using media to keep business data privacy practices in the spotlight (Section B). It has pressed U.S. businesses to enhance self-regulatory efforts to forestall EU restrictions on data transfers to the United States, divert

230. The WTO does not permit unilateral retaliatory measures, as exemplified by the U.S.-EU dispute that has lasted over ten years regarding the EU ban on meat from cows fed with certain hormones. After consultations did not resolve the conflict, the United States unilaterally retaliated in 1989 with duties imposed on various EU imports. After the creation of the WTO, the European Union requested (in 1996) that the WTO establish a panel challenging the U.S. retaliatory tariffs, and the United States, a month later, removed them in the shadow of a likely adverse panel decision. Instead, the United States brought its own WTO claim challenging the EU ban on U.S. meat. Only after WTO dispute settlement panels ruled in favor of the United States and the European Union failed to comply with the ruling was the United States permitted to take retaliatory measures. The WTO rulings are available at *WTO Dispute Settlement* (visited Oct. 5, 1999) <http://www.wto.org/wto/dispute/distab.htm>. *See also* Kevin C. Kennedy, *The Illegality of Unilateral Trade Measures To Resolve Trade-Environment Disputes*, 22 WM. & MARY ENVTL. L. & POL'Y REV. 375, 449–50 (1998) (describing the procedural history of the meat hormone dispute).

231. *See supra* note 229. Critics also claim that trade liberalization subjects domestic producers to greater competitive pressures, so that they demand that domestic standards be lowered—be they environmental, labor, or other standards—in order to enhance their competitiveness. *See generally* DANIEL ESTY, GREENING THE GATT 162–63 (1994).

232. *See supra* Section III.A.

demands for stricter U.S. regulation, and counter negative publicity (Section C). The context in which U.S. domestic debates over data privacy protection take place has been altered.[233] United States businesses are now on the defensive about their practices. So are officials in the U.S. Department of Commerce who represent U.S. business interests abroad.

A. *Enhanced U.S. Regulatory Efforts*

The U.S. administration is divided over data privacy issues. These pre-existing fissures facilitate the EU Directive's influence in U.S. domestic debates. The U.S. Department of Commerce has advocated a more market-based approach, focusing on the role of business "self-regulation." It has taken a hard line against the EU Directive as an over-reliance on "big government" and in itself an "invasion of privacy."[234] On the other hand, members of the Clinton Administration, some members of Congress, and the Federal Trade Commission (FTC) have taken a more aggressive approach, promoting legislation to expand data privacy protection. Vice President Gore, for example, has urged Congress to pass an "electronic bill of rights" guaranteeing on-line privacy, in particular as regards medical and financial records.[235] Although the United States formally presents a united front in negotiations with the European Union, many in positions of power within the U.S. Administration simultaneously press for legislative protections mandated by the EU Directive.

The FTC, the independent federal agency that oversees consumer interests, has taken the lead among federal agencies in advocating greater data privacy protection in the United States. In the fall of 1998, the FTC successfully lobbied for greater on-line data privacy protection for children,[236]

---

233. This is in line with "constructivist" theory, which focuses on the way knowledge, agenda, and norms are shaped through communicative processes, including interactions among policy makers and private parties. *See, e.g.*, MARGARET KECK & KATHERINE SIKKINK, ACTIVISTS BEYOND BORDERS 1–8 (1998). Keck and Sikkink note how transnational advocacy groups "contribute to changing perceptions that both state and societal actors may have of their identities, interest, and preferences, to transforming their discursive positions, and ultimately to changing procedures, policies, and behavior." *Id.* at 3. In the case of data privacy, however, issues are being shaped in the United States largely by the impact of foreign regulatory pressure on the stakes of U.S. domestic actors.

234. *See* Andrews, *supra* note 81 (quoting David Aaron, Undersecretary of Commerce). Aaron appears to be referring to the privacy interests of large private commercial interests to be left alone by government, as in a "laissez-faire" ideal world.

235. *See U.S. Vice President Issues Proposals To Protect On-Line Privacy*, Agence-France Presse, July 31, 1998. Gore's electronic bill of rights include the following: "(1) The right to choose whether one's personal information is disclosed; (2) The right to know how, when and how much of that information is being used; (3) The right to see that information themselves; (4) The right to know if information is accurate and corrected if it is not." WORKING GROUP FIRST ANNUAL REPORT, *supra* note 182, at 18. President Clinton subsequently called for greater privacy protection of medical records in his 1999 State of the Union address. *See My Fellow Americans . . . State of Our Union Is Strong*, WASH. POST, Jan. 20, 1999, at A12 (transcript of President Clinton's State of the Union Address); *Remarks by the President on Financial Privacy and Consumer Protection* (visited Sept. 8, 1999) <http://www.whitehouse.gov/WH/New/html/19990504-1925.html> (financial records discussed in May 4, 1999 address). The Clinton Administration proposed new regulations to protect the privacy of medical records in late October 1999. *See* Pear, *supra* note 98, at A1.

236. This culminated in Congress's passing the Children's Online Privacy Protection Act in

and generally criticized the on-line data collection practices of U.S. businesses for failing to provide adequate privacy protection.[237] Although privacy advocates were critical of the FTC's ensuing July 1999 report to Congress entitled *Self-Regulation and Privacy Online* because the report did not recommend new legislation,[238] the FTC Chairman nonetheless maintained, in presenting the report, that "Congress and the Administration should not foreclose the possibility of legislative and regulatory action if we cannot make swift and significant additional progress."[239] The FTC continues to monitor

---

October 1998, which now requires websites to provide actual notice and to obtain prior parental consent before companies collect information about children under the age of 13. *See Children's Online Privacy Protection Act of 1998* ("COPPA"), Pub. L. No. 105-277, 112 Stat. 2681, tit. XIII (1998). In his Congressional testimony in support of the Act, FTC Chairman Robert Pitofsky noted that in its survey of commercial World Wide Web sites, the FTC found that while almost 90% of the children's websites collect personal information from and about children, only 1% of those sites obtain parental permission before collecting such information. *See Protection of Children's Privacy on the World Wide Web: Hearing Before the Subcommittee on Communications of the Senate Committee on Commerce, Science & Transportation* (1998) (prepared statement of the Federal Trade Commission, presented by Chairman Robert Pitofsky). Pursuant to COPPA, the FTC proposed new implementing regulations to protect children's privacy interests on the Internet in April 1999. *See* Stephen Labaton, *U.S. Urges New Rules To Guard Privacy of Children on Internet*, N.Y. TIMES, Apr. 21, 1999, at A20.

237. *See* FEDERAL TRADE COMMISSION, PRIVACY ONLINE: A REPORT TO CONGRESS (June 1998), *available at* <http://www.ftc.gov/reports/privacy3/index.htm> [hereinafter FTC JUNE 1998 REPORT ON PRIVACY ONLINE]. The FTC concluded in this report that, "despite the Commission's three year privacy initiative supporting a self-regulatory response to consumers' privacy concerns, the vast majority of online businesses have yet to adopt even the most fundamental fair information practice," much less any enforcement mechanism whatsoever. FTC JUNE 1998 REPORT ON PRIVACY ONLINE, *supra*, at 41. After completing a three-year study, the FTC concluded that "industry's efforts to encourage voluntary adoption of the most basic fair information practices have fallen short of what is needed to protect consumers." Federal Trade Commission, *FTC Releases Report on Consumers' Online Privacy* (visited June 4, 1998) <http://www.ftc.gov/opa/1998/9806/privacy2.htm>. In a survey of websites conducted by FTC investigators in the spring of 1998, the FTC found that "more than 90% of the roughly 1,400 [web]sites examined collected personal information from visitors, but only 14% of them disclosed how that information could be used." FTC JUNE 1998 REPORT ON PRIVACY ONLINE, *supra*, at 23; *see also* Joel Brinkly, *FTC Surfs the Web and Gears Up to Demand Privacy Protection*, N.Y. TIMES, Sept. 21, 1998, at C1.

In December 1998, FTC Commissioner Mozelle Thompson went so far as to state to EU authorities that "industry's progress toward self-regulation" is "practically non-existent." Mozelle W. Thompson, *Solutions for Data Protection and Global Trade, Remarks Before the EU Committee of AMCHAM* (visited Dec. 3, 1998) <http://www.ftc.gov/speeches/thompson/speech123.htm>. Such statements weaken the U.S. position in its negotiations with the European Union over the "adequacy" of U.S. business self-regulation.

238. *See Hearing on Privacy on the Internet Before the Subcommittee on Communications of the Senate Commerce Commission*, 106th Cong. (July 27, 1999) (statement of Marc Rotenberg, Director, Electronic Privacy Information Center).

239. Statement of Robert Pitofsky, FTC Chairman, on *Self Regulation and Privacy Online*, Before the Subcommittee on Communications of the Committee on Commerce, Science and Transportation at Telecommunications, Trade, and Consumer Protection of the Committee on Commerce, United States House of Representatives, at 12 (July 13, 1999) <http://www.ftc.gov/os/1999/9907/pt071399.htm> (Prepared Statement of the Federal Trade Commission, presented by Chairman Robert Pitofsky). In its July 1999 report, the FTC concluded by a 3-1 vote that "legislation to address on line privacy is not appropriate at this time in view of ongoing process in industry self-regulation efforts." FEDERAL TRADE COMMISSION, SELF-REGULATION AND PRIVACY ONLINE, *available at* <http://www.ftc.gov/os/1999/9907/privacy99.pdf> (visited Nov. 15, 1999) [hereinafter FTC JULY 1999 REPORT ON SELF-REGULATION]. Although the FTC found significant progress in business self-regulation to protect consumers' privacy over the past year, it nonetheless noted that, depending on the study, only around 10 to 20% of the most active websites offer all of the four basic "substantive fair information practices": "Notice/Awareness, Choice/Consent, Access/Participation, and Security/

self-regulatory developments and support other privacy legislation. In addition to recently drafting the implementing regulations protecting children's online privacy,[240] the FTC testified in support of greater privacy protection in the financial sector at the same time that it issued its report on Self-Regulation.[241]

The FTC and Congress remain under pressure to act, as do state legislatures and regulatory agencies. Numerous bills to enhance data privacy are pending.[242] The FTC maintains that it is studying "what additional incentives are required in order to encourage effective self-regulatory efforts by industry" to protect consumers generally.[243] Media reports on the "adequacy" of U.S. protections under the EU Directive keep these data privacy issues in the spotlight.[244]

The EU Directive, together with the potential for further U.S. legislation, also enhances the FTC's leverage in working with businesses to change their market practices. The FTC conducts periodic public workshops on data privacy issues that bring together federal regulators, technology experts, businesses, and privacy advocates.[245] The EU Directive, on account of its definition of fair information practices, provides a yardstick against which business practices may be measured. Through the workshops, the FTC informs businesses of the need to raise internal privacy standards both to forestall further U.S. legislation and to avoid lawsuits brought in the European Union.[246] As the FTC's most conservative member on privacy regulation states, "[i]n the event our joint efforts [toward industry adoption of fair information practices] do not produce results, I would caution industry that there are many eager and willing to regulate."[247]

Integrity."

240. *See supra* note 236.

241. *See FTC Chairman Testifies Before House Subcommittee on the Privacy Provision of H.R. 10* (visited July 21, 1999) <http://www.ftc.gov/opa/1999/9907/hr10.htm>.

242. *See, e.g.*, Consumer Internet Privacy Protection Act of 1999, H.R. 313, 106th Cong.; Freedom and Privacy Restoration Act of 1999, H.R. 220, 106th Cong.; Children's Privacy Protection and Parental Empowerment Act of 1999, H.R. 369, 106th Cong. Bills before state legislatures also proliferate. *See* Denise Caruso, *Personal Information Is Like Gold in the Internet Economy, and the Rush Is on To Both Exploit It and Protect It*, N.Y. TIMES, Mar. 1, 1999, at C4. Caruso notes that the California legislature "is considering more that a dozen privacy laws, including one that would restrict the collection and disclosure of personal information by government, business or nonprofit organizations. It specifically includes information gathered via Internet sites." *Id.*

243. *See* FTC JUNE 1998 REPORT ON PRIVACY ONLINE, *supra* note 237, at 41; *see also* FTC JULY 1999 REPORT ON SELF-REGULATION, *supra* note 239, at 14 ("A second task force will address how incentives can be created to encourage the development of privacy enhancing technologies.").

244. *See infra* note 262 and accompanying text.

245. The FTC initiated these workshops in April 1995. *See Internet Privacy Hearing Before the Subcommittee on Courts and Intellectual Property of the House Committee on the Judiciary* (1998) (visited Nov. 29, 1999) <http://www.ftc.gov/os/1998/9803/privacy.htm>.

246. *See, e.g., Staff Report: Public Workshop on the Global Information Infrastructure* (1996) (visited Nov. 29, 1999) <http://www.ftc.gov/reports/privacy/privacy1.htm> (examining privacy online).

247. *Separate Statement of Commissioner Orson Swindle*, Annex to FTC JULY 1999 REPORT ON SELF-REGULATION, *supra* note 239. In July 1998, the FTC proposed a "legislative model [that] would set forth a basic level of privacy protection for all consumers visiting U.S. consumer-oriented commercial Web sites . . . unless industry can demonstrate that it has developed and implemented broad-based and effective self-regulatory programs by the end of this year." *"Consumer Privacy on the World Wide Web": Hearing Before the Subcommittee on Telecommunications, Trade, and Consumer Protection of the House Committee on Commerce* (visited July 21, 1998) <http://www.ftc.gov/os/1998/

While defending U.S. commercial interests in data privacy negotiations with the European Union, the Department of Commerce has similarly urged businesses to develop enhanced self-regulatory procedures. Otherwise, Commerce's advocacy of a "self-regulatory" approach to privacy protection has little credibility. Commerce Secretary William M. Daley has asserted that, while he supports a self-regulatory approach, it must include "meaningful consequences to companies that don't comply" or the government will have to step in with new regulations.[248] Not surprisingly, the lack of enforcement mechanisms in the United States has been a contentious issue in U.S.-EU negotiations.

In an effort to demonstrate to the European Union that privacy protection can be assured through business self-regulation and, in the process, shield U.S. businesses engaged in self-regulation from data transfer restrictions, Commerce issued a draft of "Safe Harbor Principles" in November 1998, within a month of the EU Directive's becoming effective.[249] Commerce's draft guidelines were made subject to comment for a fifteen-day period, although they were not published in the Federal Register.[250] Following internal consultations with industry and intensive external negotiations with EU authorities over the substance of the principles, Commerce issued a revised set of Safe Harbor Principles on April 19, 1999.[251] The April 1999 Safe Harbor Principles are:

(i) "Notice": An organization must provide "clear and conspicuous" notice to individuals "about the purposes for which it collects information about them, how to contact the organization with . . . complaints, the types of third

---

9807/privac98.htm> (prepared statement of the Federal Trade Commission, presented by Chairman Robert Pitofsky).

248. *Business Leaders to Propose Charter To Address Problems of Internet Regulation*, 15 Int'l Trade Rep. (BNA) 1179 (July 8, 1998).

249. Commerce's initial draft Safe Harbor Principles are available on the Department of Commerce website (visited Jan. 12, 1999) <http://www.ita.doc.gov/ecom/aaron114.html#Safe> [hereinafter November 1998 Safe Harbor Privacy Principles]. *See also Information Technology: EU States Endorse Standstill with U.S. on Transfers of Data During Privacy Talks*, 15 Int'l Trade Rep. (BNA) 1780 (Oct. 28, 1998).

250. Commerce's cover letter was not addressed to the general public, but rather specifically to "Industry Representatives." In total, Commerce received 65 comments, largely from multinational corporations and large business associations. Nonetheless, some public advocacy groups responded, expressing concerns clearly opposed to industry's. They accused Commerce of not only an industry bias, but also of having worked surreptitiously with certain industry representatives in preparing the principles before opened for comment. *See Comments of Mark Silbergeld, supra* note 107. Silbergeld spoke on behalf of the Center for Media Education, Consumer Federation of America, Consumers Union, Electronic Privacy Information Center, Junkbusters, The NAMED, Privacy International, Privacy Journal, Privacy Rights Clearinghouse, Privacy Times, and the U.S. Public Interest Research Group. This group claimed that Commerce "developed this proposal in private consultation with industry representatives," and that "once again, the train has left the station unannounced and the industry, as represented by the Transatlantic Business Dialogue, is the engineer in the cab." *Id.*; *see also Comments of the ACLU on the Department of Commerce Draft Safe Harbor Principles* (visited Jan. 13, 1999) <http://www.ita.doc.gov/ecom/com2abc.htm#aclu>.

251. *International Safe Harbor Privacy Principles* (visited Apr. 19, 1999) <http://www.ita.doc.gov/ecom/shprin.html> [hereinafter April 1999 Safe Harbor Privacy Principles].

parties to which it discloses the information, and the . . . means . . . for limiting its use and disclosure";

(ii) "Choice": Organizations must provide individuals with a clear and conspicuous choice to "opt out" of how their personal information is used and to whom it may be disclosed; for certain "sensitive information, such as medical and health information, information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information concerning the sex life of the individual they must be given affirmative or explicit (opt in) choice";

(iii) "Onward Transfer": When transferring personal information to a third party, organizations must require the third party to provide at least the same level of privacy protection as required by the relevant Safe Harbor Principles, including consistency "with the principles of notice and choice";

(iv) "Security": Organizations must take reasonable measures to assure the reliability of information and protect it from disclosure or loss;

(v) "Data Integrity": Organizations must retain only information relevant to the purpose for which it was collected, and "take reasonable steps to ensure that it is accurate, complete and current";

(vi) "Access": Organizations must grant individuals "[reasonable] access to personal information held about them and the opportunity to have it corrected"; and

(vii) "Enforcement": There must be "mechanisms for assuring compliance" with the principles and "consequences" for non-compliance, which must include "readily available and affordable independent recourse mechanisms" and "sanctions that must be sufficiently rigorous to ensure compliance." These obligations can be satisfied through compliance with private sector developed privacy programs.[252]

The drafting, reception of public comments, and revisions of these "principles" are analogous to negotiated rulemaking under U.S. administrative

252. *Id.*

law.[253] Yet, it is a negotiated rulemaking of a peculiar variety. The principles are not intended, on their face, to affect U.S. law, but rather to provide a "safe harbor" to companies in respect of a foreign law, the EU Directive. Domestic parties, however, are aware of the spill-over effects these principles will have on data privacy policy and practice in the United States. While U.S. companies would not—technically—be forced to adopt them, most large businesses may do so in order to avoid EU restrictions on data transfers.[254]

Yet, if a company adopts the Safe Harbor Principles and fails to comply with them, it subjects itself to challenge by the FTC for "using unfair or deceptive acts or practices in or affecting commerce."[255] The FTC has, in fact, already brought two enforcement actions in the last year.[256] Were there no EU

---

253. For discussions of negotiated rulemaking, see Philip J. Harter, *Negotiating Regulations: A Cure for Malaise*, 71 GEO. L.J. 1 (1982); Henry H. Perritt, Jr., *Negotiated Rulemaking Before Federal Agencies: Evaluation of Recommendations by the Administrative Conference of the United States*, 74 GEO. L.J. 1625 (1986); and Lawrence Susskind & Gerard McMahon, *The Theory and Practice of Negotiated Rulemaking*, 3 YALE J. ON REG. 133 (1985). For a critique of negotiated rulemaking, see William Funk, *When Smoke Gets in Your Eyes: Regulatory Negotiation and the Public Interest—EPA's Woodstove Standards*, 18 ENVTL. L. 55 (1987).

254. Commerce's privacy principles, once adopted by corporations, can also be seen as a code of conduct. In this way, they are similar to many transnational developments aimed at protecting social concerns. Labor and human rights activists pressure companies to adopt internal codes applying fair labor standards, including the elimination of child labor and the right of workers to bargain collectively. *See, e.g.*, Lance A. Compa & Tashia Hinchliffe Darricarrere, *Private Labor Rights Enforcement Through Corporate Codes of Conduct*, *in* HUMAN RIGHTS, LABOR RIGHTS, AND INTERNATIONAL TRADE 181 (Lance A. Compa & Stephen F. Diamond eds., 1996). Environmental activists work with companies and regulatory authorities to develop "voluntary" eco-label programs whereby companies agree to reduce the adverse environmental impact of a product throughout its life cycle. *See, e.g.*, George Richards, *Environmental Labeling of Consumer Products: The Need for International Harmonization of Standards Governing Third-Party Certification Programs*, 7 GEO. INT'L ENVTL. L. REV. 235, 244 (1994). Shareholder activists pressure corporate groups to adapt and implement labor rights and environmental protection principles for their domestic and foreign production. *See, e.g.*, General Electric Company Proxy Statement, provided with 1998 Annual Report (on file with author). International organizations, such as the International Organization for Standardization (ISO), develop principles pursuant to which companies agree to implement environmental management systems. If companies meet ISO standards, they may place an ISO seal on their products. *See, e.g.*, Paula C. Murray, *The International Environmental Management Standard, ISO 14000: A Non-Tariff Barrier or a Step to an Emerging Global Environmental Policy?*, 18 U. PA. J. INT'L ECON. L. 577 (1997).

Skeptics properly question whether these "self-regulatory" programs are sufficient, maintaining that they must be backed by independent audit and enforcement procedures. These issues similarly lie at the core of negotiations over the substance of Commerce's privacy principles. The case of data privacy demonstrates that enforcement potentially can come from multiple directions—both through EU- and U.S.-based authorities. In addition, there is potential for privacy advocates and concerned individuals to oversee the overseers, monitoring their enforcement of agreed principles.

255. Federal Trade Commission Act § 5, 15 U.S.C. § 45(a)(6) (1994).

256. In 1998, the FTC brought an enforcement action against GeoCities, which has "one of the most popular sites on the Web." FTC JULY 1999 REPORT ON SELF-REGULATION, *supra* note 239, at 16 n.16. The FTC alleged that GeoCities was representing that it was collecting personal information for its use when the information was going directly to third parties. GeoCities agreed to settle this dispute pursuant to a consent order finalized in February 1999. *See* GeoCities, Docket No. C-3850 (F.T.C. Feb. 5, 1999) (containing a Final Decision and Order), *available at* <http://www.ftc.gov/os/1999/9902/9823015d&o.htm>. In 1999, the FTC announced its second enforcement action, this time against Liberty Financial Companies, Inc., operator of the Young Investor Web site, for falsely representing that information collected would be maintained anonymously. This again resulted in a negotiated consent order. *See* Liberty Financial Companies, File No. 982 3522 (May 6, 1999) (proposed consent agreement), *available at* <http://www.ftc.gov/os/1999/9905/lbtyord.htm>. A description of these two cases is set forth in the FTC JULY 1999 REPORT ON SELF-REGULATION, *supra* note 239, at 16 & n.16.

Directive or Safe Harbor Principles, companies would be less inclined to notify consumers of company privacy policies. Were companies not induced to adopt privacy policies, the FTC would have no jurisdiction to intervene. In this backhanded way, the EU Directive effectively fashions enhanced U.S. data privacy requirements, potentially becoming the baseline standard within the United States.

European authorities help determine the content of this quasi-legislation. Ultimately, the effectiveness of Commerce's "safe harbor" against data transfer restrictions depends on whether EU authorities recognize the Principles as legally binding. The European Union, however, has so far rejected the U.S. proposals as inadequate.[257] While the outcome of U.S.-EU negotiations may not satisfy U.S. data privacy advocates, at a minimum, the EU Directive has provided leverage to press large U.S. businesses to adopt fair information practices that they otherwise would ignore.

The EU Directive has not only shaped U.S. baseline rules, it has spurred new institutional developments. The Department of Commerce has consistently criticized the European scheme of empowering national supervisory authorities as an anachronistic reliance on big government, as opposed to the decentralized U.S. approach.[258] Yet, under pressure from the EU Directive, the United States finally took a first step toward coordinating U.S. data privacy policy at the federal level by creating a new position of "Chief Counselor for Privacy" within the Office of Management and Budget.[259] While the creation of a single position is far from the creation of a functioning agency, the counselor's initial job portfolio is two-fold: to coordinate U.S. domestic policy on "public and private sector" data processing practices and to "serve as a point of contact on international privacy issues," such as the negotiations with EU authorities.[260] It was EU

257. *See, e.g., EU, U.S. Will Not Sign Data Privacy Pact at Upcoming Bonn Summit, Officials Say*, Int'l Bus. & Fin. Daily (BNA) D4 (June 2, 1999). European Union authorities initially focused on inadequate provisions concerning individual access to records, prior notification of transfers of personal information to third parties, and effective enforcement. *See* Interview with Scott Blackmer, *supra* note 44. The negotiators also argued over the length of the implementation period by which U.S. businesses must comply. *See EU Rejects U.S. Data Privacy Plan*, *supra* note 189, at 1963.

In consequence, U.S. and EU representatives continue to negotiate over the final content of regulations (governmental or self-regulatory) necessary to comply with EU adequacy requirements, affirming that "only a limited number of points are still at issue." *See Joint Report on Data Protection Dialogue to the EU/US Summit* (visited June 21, 1999) <http://www.europa.eu.int/comm/dg15/en/media/dataprot/news/summit.htm>.

258. *See supra* note 182 and accompanying text.

259. The first counselor for privacy will be Peter Swire, a law professor at Ohio State University. *See Clinton Administration to Name Swire as OMB's Privacy Policy Coordinator*, *supra* note 104. As Joel Reidenberg predicted earlier, "if European regulators take the transborder data flow provisions seriously," this could stimulate "a consolidation of the dispersed functions in a single executive branch office" or "the creation of an executive branch data protection office." Joel Reidenberg, *The Movement Toward Obligatory Standards for Fair Information Practice in the United States*, *in* VISIONS FOR PRIVACY IN THE 21ST CENTURY (Colin Bennett & Rebecca Grant eds., forthcoming 1999). For a description of earlier calls for the creation of a federal data protection commission, see Laura Pincus & Clayton Trotter, *The Disparity of Privacy Rights for Private Sector Workers*, 33 AM. BUS. L.J. 51, 76–80, 83 (1995).

260. *Clinton Administration to Name Swire as OMB's Privacy Policy Coordinator*, *supra* note 104.

pressure that incited the creation of the new U.S. position to have both an international "point of contact" and a domestic policy coordinator.

States are not unitary actors. Different regulatory bodies within states respond differently to external pressures. While the outcome of inter-agency and legislative debates depends, in large part, on the extent of public pressure for stronger data privacy protection and the development of effective private self-regulatory schemes, the EU Directive has altered the domestic context. It has bolstered public pressure for regulatory reform. It has spurred state and federal officials (from the more consumer-friendly FTC to the more business-friendly Commerce Department) to press businesses to develop enhanced private data protection schemes. It has created opportunities for FTC enforcement of new data privacy standards. These efforts of U.S. regulatory authorities, from lobbying Congress to promoting more stringent self-regulation to judicial enforcement, are conducted in the shadow of foreign regulators—the European Commission and EU Member State authorities.[261]

B. *An Opportunity for Public Advocacy Groups and Privacy Service Providers*

Data privacy advocates have attempted to use the EU Directive to challenge lax business practices in the United States. Beginning in the fall of 1998 when the EU Directive first went into effect, it was featured, together with U.S.-EU negotiations over the "adequacy" of U.S. data privacy protection, in *The New York Times*, *USA Today*, *The Washington Post*, *The Wall Street Journal*, and *The Financial Times*,[262] among other newspapers read by business representatives and policymakers. Numerous symposia have been held that addressed the "adequacy" of U.S. data protection practices in light of the EU Directive.[263] The EU Directive and the publicity it received drew attention to data privacy advocates and provided leverage for their efforts.[264] It has also provided free advertising for developing service

261. Similarly, the European Commission acts within the shadow of other bodies. The Commission is accountable both to EU Member State representatives and the World Trade Organization. For a general overview of interactions between U.S. and EU regulatory authorities, whether through programmatic cooperation or to manage regulatory conflicts, see George Berman, *Regulatory Cooperation Between the European Commission and U.S. Administrative Agencies*, 9 ADMIN. L.J. AM. U. 933 (1996).

262. *See* Andrews, *supra* note 81, at A1; *EU and US Seek Solution*, FIN. TIMES, Oct. 27, 1998, at 4; Robert O'Harrow, Jr., *Privacy Rules Send U.S. Firms Scrambling; European Union Will Curb Transmissions to Nations Considered Lax*, WASH. POST, Oct. 20, 1998, at C1; Jennifer L. Schenker & Julie Wolf, *Data Privacy Is Issue as EU Law Takes Effect*, WALL ST. J., Oct. 21, 1998; Elizabeth Weise, *EU Privacy Paradigm May Lock U.S. Firms Out*, USA TODAY, Oct. 21, 1998, at 6D.

263. The EU Directive was discussed at symposia such as *One Planet, One Net*, sponsored by the Computer Professionals for Social Responsibility, held on October 10, 1998, at MIT; The Privacy in American Business 5th Annual National Conference—*Managing the Privacy Revolution in 1998*, held on December 1–2, 1998, in Arlington, Virginia; and *Legal Aspects of the Internet*, held on November 5–6, in San Francisco, and November 16–17, 1998, in New York City, sponsored by *The American Lawyer*, *The National Law Journal*, *The Recorder*, and *New York Law Journal*. I was part of one such symposium held in Madison, Wisconsin, on November 14, 1998, portions of which were later broadcast on Wisconsin Public Radio.

264. Even congressional representatives have met with European officials over data privacy

industries, including legal counsel, which profit from assisting firms to comply with EU requirements.

1. *The Role of Privacy Advocates*

Privacy advocates play an important role because they are "repeat players" in ongoing negotiations over U.S. data privacy rules.[265] They are, in this way, different from individuals who transact with companies on an ad hoc basis and who may commence "one-shot" disputes when they feel their privacy interests are impinged. As repeat players, privacy advocates have longer time horizons in which to implement strategies to maximize gain. They have an incentive to expend resources to influence the development of relevant data privacy standards, whether through threatened company boycotts, legislative lobbying, or judicial challenge.

Privacy advocates jumped on the opportunity to pressure the Department of Commerce to make its Safe Harbor Principles more stringent. They responded to Commerce's call for comments on its Safe Harbor Principles even though Commerce directed its invitation only to "Industry Representatives." Privacy advocates criticized Commerce for focusing on protecting U.S. businesses from EU privacy requirements instead of protecting U.S. consumers from business exploitation of private information.[266] They objected to Commerce's advocacy of self-regulatory mechanisms, responding that "self-regulation has been a lot of smoke and mirrors."[267] In line with the EU Directive, they maintained that the United States also needs "a comprehensive approach to privacy protection,"[268] not a fragmented, scandal-specific one.

Privacy advocates believe that individuals must be able to control the commercial use of personal information about them. The advocates criticized the Safe Harbor Principles for their loopholes and recommended ways these could be closed. On the issue of "Choice," for example, privacy advocates argued that Commerce's support of an "opt out" right was insufficient because it requires consumers to check an "opt out" box every time they enter a transaction. Privacy advocates demand instead an "opt in" right so that personal data may not be used or transferred unless the individual

---

legislation. *See Goodlatte Calls on Administration To Begin Talks with Congress on Data Privacy Issues*, 16 Int'l Trade Rep. (BNA) 502 (Mar. 24, 1999) (noting remarks of Robert Goodlatte, co-chair of Congress's "Internet Caucus," concerning his meeting with John Mogg, Director General of the European Commission for the Internal Market, who leads the EU delegation on data privacy discussions, as well as other meetings involving congressional delegates and EU officials, in both Washington and Brussels).

265. The terms "repeat players" and "one-shot" disputes are taken from Marc Galanter's classic piece, *Why the "Haves" Come Out Ahead: Speculations on the Limits of Legal Change*, 9 L. & SOC'Y REV. 95 (1974).

266. *See, e.g., Comments of Mark Silbergeld, supra* note 107 (comments submitted on behalf of a number of privacy advocate groups).

267. Clausing, *supra* note 184, at C1 (quoting Marc Rotenberg of EPIC).

268. *Comments of Mark Silbergeld, supra* note 107.

affirmatively consents.[269] On the issue of "Access," advocates asserted that an individual's right must cover all information collected about her, not just "sensitive" information (which initially was left undefined).[270] On "Enforcement," they contended that business data processing practices must be "independently" monitored, and that so-called "self-certification" by business is a travesty.[271] Some advocates called for the creation of a new U.S. privacy protection agency, analogous to the supervisory authorities mandated by the European Union.[272]

Yet even though privacy advocates critique the Department of Commerce's principles, if the principles are adopted privacy advocates will use them, where possible, as part of their larger strategies. It is privacy advocates who will test new "access" rights. It is privacy advocates who will work, as private attorneys general, with the FTC and other agencies to force companies to adhere to the policies they announce.[273] The EU Directive induces the creation of new legal tools within the United States that U.S. privacy advocates can exploit.

In light of the international nature of U.S.-EU data privacy negotiations, as well as those within the OECD (and potentially within the WTO), privacy advocates are more effective where they coordinate their activities transnationally. The Electronic Privacy Information Center (EPIC), one of the leading privacy advocates in the United States (though consisting of only three attorneys),[274] works in association with Privacy International, a group based in London.[275] EPIC has lobbied Congress for greater privacy protection, commented on proposed Commerce guidelines, and generally tried to track U.S. business practices. Privacy International has announced that it will monitor data transmissions of major U.S. multinational companies and ensure

---

269. *See id.* Privacy activists also advocate limiting the collection of information only to that which is *necessary* for purposes consented to by the individual. *See id.*

270. In Commerce's revised draft guidelines of April 1999, the earlier draft's implication that access only applied to sensitive information was removed. *See* April 1999 Safe Harbor Principles, *supra* note 251.

271. *See Comments of Mark Silbergeld*, *supra* note 107. Privacy advocates also recommend that each company be required to designate an individual or individuals to oversee the company's compliance with governmental and self-regulatory requirements. *See id.*

272. *See id.* Others advocates acknowledged that this may be unrealistic given current attitudes in Congress. *See* Telephone Interview with Deirdre Mulligan, Staff Counsel, Center for Democracy and Technology (Dec. 8, 1998). Given that Congress currently is considering closing existing agencies, it is unlikely to authorize funds for a new one. On the other hand, a division within the FTC, Commerce, or another agency could be made responsible for overseeing and providing consumer support on all data privacy issues. *See also supra* note 259 and accompanying text (concerning the creation of a new position in the executive branch to coordinate U.S. domestic policy on privacy protection).

273. For example, the Electronic Privacy Information Center (EPIC) conducted and published its own review of website data processing practices a year before the FTC conducted and published its own critique. *See Surfer Beware: Personal Privacy and the Internet* (visited Nov. 11, 1999) <http://www.epic.org/reports/surfer-beware.html>.

274. *See Epic.org* (visited Jan. 11, 1999) <http://www.epic.org/>.

275. *See Privacy International* (visited Jan. 11, 1999) <http://www.privacy.org/pi/>. EPIC and Privacy International have organized national conferences on data privacy issues since 1994. *See* Comments from Marc Rotenberg, *supra* note 31.

that the EU Directive is enforced.[276] Through their coordination, privacy advocates enhance the EU Directive's impact on U.S. business practices.

The United States and European Union recently facilitated the formation of a Transatlantic Consumer Dialogue (TACD), consisting of consumer advocates on both sides of the Atlantic.[277] The TACD held its first meeting on electronic commerce in Brussels in April 1999, in the midst of U.S.-EU negotiations over the content of the Safe Harbor proposals. The grouping of transatlantic consumer advocates passed a resolution urging "the European Commission and the Member States to reject the [U.S.] Safe Harbor Proposal."[278] United States consumer advocates knew that EU Member States and EC officials were implicitly their allies, and provided them with support to demand tougher U.S. privacy protection standards.

2. *The Role of Privacy Service Providers*

By calling attention to data privacy issues, the EU Directive not only permits privacy advocates to challenge lax business practices more effectively, but it also increases the demand for the advocates' services, as well as the services of for-profit enterprises. The Center for Social and Legal Research, "a privacy think tank" founded by Alan Westin, has created a series of initiatives under its "Privacy and American Business" program, through which it advises businesses on developments in privacy regulation domestically and abroad. For example, the group arranges periodic conferences for companies and industry associations on privacy protection issues, publishes a journal titled *Privacy and American Business*, and works with multinational companies in drafting codes of conduct to meet the EU Directive's requirements.[279] The Center's Global Business Privacy Project focuses, in particular, on the impact of the EU Directive in the United States and other countries where U.S. companies operate.[280] The Electronic Frontier Foundation, a San Francisco-based public interest organization, has associated with information technology companies to launch a program named TRUSTe to rate the privacy protection of Internet sites.[281] Similarly, Alan Westin

276. *See Will Amex and EDS Privacy Lawsuits in Europe?*, *supra* note 176. Privacy International specifically mentioned its monitoring of Electronic Data Systems, Ford, Hilton International, Microsoft, and United Airlines. It is reported that "the target companies say they are hurrying to meet Europe's new privacy requirements." Noah Shachtman, *EU Privacy Law is Awkward for US*, WIRED, Oct. 23, 1998, *available at* < http://www.wired.com/wired/> (visited Nov. 29, 1999); *see also* Baker, *supra* note 62, at 20.

277. *See TACD* (visited Nov. 15, 1999) <http://www.tacd.org>. The Transatlantic Consumer Dialogue will most likely be funded by OECD member governments and certain of the Dialogue's more financially secure members. *See* Interview with Deirdre Mulligan, *supra* note 272.

278. TACD, *Safe Harbor Proposal and International Convention on Privacy Protection* (visited Oct. 13, 1999) <http://www.tacd.org/meeting2/electronic.html#safe>.

279. *See Privacy and American Business* (visited Nov. 15, 1999) <http://www.pandab.org>; *see also* SWIRE & LITAN, *supra* note 99, at 170.

280. *See* Privacy and American Business, *Global Business Privacy Project* (visited Nov. 15, 1999) <http://www.pandab.org/corpo.htm>.

281. *See Electronic Frontier Foundation* (visited Oct. 13, 1999) <http://www.eff.org>; *TRUSTe* (visited Oct. 13, 1999) <http://www.truste.org>. The latter organization was initially named

provides consulting services to the Better Business Bureau OnLine on its new privacy seal program.[282] The EU Directive has provided an opening for privacy advocates not only to goad and shame businesses, but also to collaborate with them in raising internal company standards.

The EU Directive fosters the creation of a new service industry for the certification and monitoring of self-regulatory programs. The U.S. Council of Better Business Bureaus markets itself as a provider of timely, reliable certification services under its new program BBB OnLine.[283] It maintains that it "investigates over 170 different aspects of an applicant's information practices, including privacy notice, content and placement, corporate structure, security measures, transfer and merger of information, access, [and] correction," and conducts "surprise audits on program participants."[284] TRUSTe similarly works with major accounting firms, such as PricewaterhouseCoopers and KPMG, that are paid to review information processing practices of firms displaying the TRUSTe seal.[285] To drum up business, TRUSTe consistently refers to the EU Directive, noting how TRUSTe looks "for ways to incorporate 'adequacy' as defined in the EU Directive into our program"[286] and "bridge the Internet privacy gap for companies who do business in Europe or are thinking of forging an

---

eTRUST. For critiques of the TRUSTe program, see *supra* notes 107–108 and accompanying text.

282. *See* Telephone Interview with Gary Laden, Director, BBB OnLine Privacy Program (Apr. 21, 1999); *see also BBB OnLine Privacy Program Created To Enhance User Trust on the Internet* (visited Oct. 13, 1999) <http:/www.bbb.org/alerts/BOLprivacy.html>.

283. In its comments on the draft Safe Harbor Principles, contrary to other businesses, the Council for Better Business Bureaus declared that "[n]either 'self-certification' of compliance by a business, nor routine, mandatory CPA firm audits are appropriate or workable requirements." *Comments of the Council of Better Business Bureaus on the Department of Commerce Draft Safe Harbor Principles* (visited Jan. 13, 1998) <http://www.ita.doc.gov/ecom/com1abc.htm#bbb>. The Council contended that only reviews by independent organizations, such as itself, are dependable. *See id.* The Council is the umbrella organization for 135 U.S. Better Business Bureaus. Though funded by major corporations, the Council operates with a degree of independence. Its goal is to foster goodwill between businesses and consumers and thereby to promote the public image of its members. The Better Business Bureaus serve as an outlet for consumer grievances, and thus are a more favorable alternative to litigation for businesses. Nonetheless, BBB OnLine's auditing of company practices and its receipt and investigation of customer complaints can change business behavior. Moreover, complaints before Better Business Bureaus need not be an exclusive remedy; they are merely a less costly alternative to litigation both for businesses and consumers. BBB OnLine's dispute settlement process will "not be binding on the consumer, so consumers will be free to exercise available judicial remedies in addition to the remedies offered by BBB OnLine." Prepared Testimony of BBB OnLine Senior Vice President and COO, Russell T. Bodoff, before the Senate Judiciary Committee, Apr. 21, 1999, *available at* <http://www/BBBOnLine.arg/about/senate_testimony> (visited Apr. 21, 1999).

284. *Id.*

285. *See TRUSTe Program Principles* (visited Jan. 12, 1999) <http://www.truste.org/webpublishers/pub_principles.html>; *see also eTrust Launches Pilot Program* (visited Dec. 20, 1996) <http://www.eff.org/effector/effect09.15>. The TRUSTe Website provides a list of official auditors at <http://www.truste.org/about/about_sponsors/html>.

286. Anne Jennings, *The European Union Data Directive: What Does It Really Mean for Your Business?, TRUSTe Newsletter (Fall 1998)* (visited Nov. 11, 1999) <http://www.truste.org/newsletter/fall98.html> (describing the effects the EU Directive will have on U.S. policy).

international presence."[287] United States businesses join these programs with an eye on EU (not just U.S.) regulators.[288]

Accountants, through their national organization the American Institute of Certified Public Accountants (AICPA), have created an analogous program entitled CPA WebTrust, under which they propose to evaluate websites, conduct audits of firms' privacy practices, and recertify participating firms every three months.[289] The EU Directive helps define the data protection practices that businesses must meet if they wish to receive privacy seals from the AICPA or one of its competitor programs. The initial WebTrust guidelines, formulated in September 1997, focused more on the security of payment mechanisms to promote e-commerce than on privacy protection.[290] The initial guidelines would have merely confirmed that a certified company publishes a privacy policy, whatever that policy may be.[291] Since then, however, privacy protection has become a more central part of the WebTrust scheme.

Private seal programs are problematic because they are funded by business. In order to attract business participants, seal programs do not demand more than what "business is willing to sign onto."[292] However, through the threat of data transfer restrictions and foreign litigation under the EU Directive, the European Union helps raise the bar of what U.S. business is willing to sign. Legislation, in this case foreign legislation, both stimulates business demand for independent certification and raises the standards for certification.

The EU Directive has also spurred the creation of a new corporate position—the director of privacy issues in companies' human resources divisions. These company employees attend conferences on the EU Directive and U.S. privacy legislation,[293] write internal memoranda on privacy issues, and generally increase firm awareness of privacy issues. In formulating and overseeing the implementation of company policies, they affect internal

287. *EU Directive—Bridging the Privacy Gap with Europe, TRUSTe Newsletter (Summer 1997)* (visited Nov. 15, 1999) <http://www.truste.org/newsletter/summer97.html>.

288. For example, it was reported that the American Electronics Association agreed to promote use of the BBB OnLine privacy seal among its 3000 high-tech member companies "in a move likely to ease tensions in the current dispute between the United States and the European Union over data privacy." Gary Yerkey, *AEA Will Promote Corporate Use of BBB Online To Ensure Privacy on the Internet*, 16 Int'l Trade Rep. (BNA) 627 (Apr. 14, 1999). John Mogg, Director General of the European Commission for the Internal Market, had stated a month earlier in Washington that an effective BBB Online system could "'greatly contribute to the resolution of a number of our concerns.'" *Id.*

289. *See The* CPA WebTrust *Seal Means Greater Security* (visited Apr. 21, 1999) <http://www.cpawebtrust.org/shared/eval/eval.html>.

290. See E-mail Communication from Anthony Pugliese, Director of Assurance Services, who is responsible for privacy issues at AICPA (Aug. 8, 1999) (on file with author).

291. *See* Telephone Interview with Linda Dunbar, Public Relations Director of AICPA (May 4, 1999).

292. Telephone Interview with Paola Benassi, Product Operations Manager, TRUSTe (Apr. 21, 1999).

293. A symposium in the fall of 1998 on data privacy organized by Westin's group, the Center for Social and Legal Research, was attended by over 170 people, primarily from corporate human resource departments. *See* Interview with Peter Swire, White House Chief Counsel for Privacy (Mar. 26, 1999).

business culture, fostering company compliance with existing legal requirements and norms, including foreign ones.[294]

Business lawyers who defend their clients against privacy advocates' claims also aid privacy advocates' ends. Even if the risk of EU restrictions is minute, lawyers benefit if their clients take the law seriously.[295] In-house counsel has an interest in being heard within the firm's hierarchy. When consulted by the firm's business personnel, in-house counsel—together with employees from the firm's human resources division—may overstate the risks to an enterprise from non-compliance by focusing on a legal reading of the EU Directive, with its substantive requirements and potentially draconian sanctions, including the risks of a ban on data transfers and imprisonment of company executives. Outside law firms distribute to clients and prospective clients manuals, memoranda, and business law articles on the EU Directive's legal provisions.[296] Their memoranda highlight why U.S. businesses must pay close attention to the EU Directive's requirements.[297] At symposia, lawyers market contractual precautions which can be drafted and implemented to reduce the risk of European intervention.[298] Ironically, in providing legal counsel to their clients on the EU Directive's provisions and risks, business lawyers and human resource employees become unconscious abettors of the aims of otherwise underfunded and disparate data privacy advocates.

For lawyers to benefit, disputes must arise, requiring two sides. For example, private lawyers rarely practice environmental law in continental Europe because environmental litigation remains rare, unlike in the United States.[299] The EU Directive, through its threat of restrictions on transatlantic

---

294. *See* Lauren B. Edelman et al., *Professional Construction of Law: The Inflated Threat of Wrongful Discharge*, 26 L. & SOC'Y REV. 47 (1992). In their study of wrongful discharge law, the authors conclude that "[t]he personnel profession, with some help from the legal profession, has constructed the law in a way that significantly overstates the threat it poses to employers." *Id.* at 53. This has resulted in more labor-friendly company discharge policies. Companies' internal human resources personnel can similarly affect companies' appreciation of data privacy regulations that may, in fact, lack adequate enforcement mechanisms.

295. In the field of wrongful discharge law, it has been noted how "[e]mployer's in-house counsel may benefit from increased demands for their services within the firm and, like personnel professionals, may attain power by helping to curb the perceived threat of wrongful discharge lawsuits. . . . The threat of wrongful discharge, then, may [also] help practicing lawyers [of outside firms] in the field of employment law expand the market for their services." *Id.* at 75.

296. For example, Masons Solicitors published a *Handbook on Cost Effective Compliance with Directive 95/46/EC*. *See supra* note 41. I have also received unsolicited copies of law firm manuals on the EU Directive. Examples of articles by lawyers include *EU and U.S. Data Protection Law—and Soon the Twain Shall Meet*, RECORDER (1998); and Simon Zinger, *From Europe with Love? U.S. Companies Face Increasingly Complex Overseas Hurdles in the Wake of the EU's Bold Data Privacy Initiative* (Dec. 1998) (on file with author).

297. As one prominent Washington lawyer affirms, businesses must understand that "data processed outside the EU on European customers and employees is subject to the same procedures, rules and protections as in Europe." *See Write Privacy Protection into Contracts with EU-Based Businesses, Panel Says*, 15 Int'l Trade Rep. (BNA) 2135 (Dec. 23, 1998) (referring to remarks of Scott Blackmer of the law firm Wilmer, Cutler & Pickering in Washington D.C.).

298. *See id.* (noting that "a panel of attorneys recommends that companies use contracts to address security and access to help ensure that data flows continue").

299. This was highlighted to me in a conversation with the French sociologist Yves Dezalay, in Washington, D.C. (Mar. 27, 1999) (confirming my own experience in private legal practice in Paris).

data transfers, creates and reinforces that other side within the United States. The EU Directive, a foreign law, thereby opens up new business for American lawyers—as well as other service providers—advising American clients over their American data processing practices.

The EU Directive also stimulates the development of new technology that protects privacy interests. NCR, the information technology company, offers new database software that facilitates "a consumer's right of access to information,"[300] responding to a major sticking point in U.S.-EU negotiations. Under NCR's new data privacy initiative, NCR markets consulting services to assist companies in complying with EU and U.S. governmental requirements and self-regulatory objectives. The EU Directive's threat to business concerns spurs new business ventures. These ventures capitalize on privacy advocates' exhortations, FTC workshops on fair information practices, and the prospects of future U.S. legislation and EU intervention.[301]

C. *U.S. Business Under the Gun: Business Reactions to EU Pressures for Privacy Protection*

1. *Business Organization, Protest, and Development of Codes*

United States businesses have vehemently objected to EU data privacy demands. These businesses work independently and join sector-specific and cross-sector business associations to lobby governmental representatives to defend their interests against EU intervention and leave data privacy to business self-regulation. They have even hired a former FTC Commissioner, Christine Varney, as a consultant.[302] They spend large sums on lobbying because they calculate that new data privacy legislation will significantly raise business compliance, transaction, operational, and opportunity costs.[303]

Businesses from a wide variety of sectors presented detailed comments to Commerce's Safe Harbor Principles, reflecting the EU Directive's broad impact on U.S. commercial interests.[304] These sectors included the direct marketing,[305] retail,[306] publications,[307] insurance,[308] financial,[309] credit,[310] and

300. *NCR Announces Consumer Data Privacy Initiative; Opt-Out/Opt-In Features To Be Built into Company Software*, PR NEWSWIRE, Oct. 5, 1998. The software permits users to "manage and audit a consumer's choice to opt-in or opt-out of personal data collection." *Id.*

301. A firm named PrivaSeek Inc. recently offered software "that enables users to control the level of information they pass on to websites." *PrivaSeek Unveils Personal 1.1*, NETWORK BRIEFING, Aug. 12, 1999, *available in* 1999 WL 17639674.

302. The Online Privacy Alliance has hired former FTC Commissioner Christine Varney to assist it in developing self-regulatory principles as an alternative to government regulation. *See* Steve Lohr, *Seizing the Initiative on Privacy: On-Line Industry Presses Its Case for Self-Regulation*, N.Y. TIMES, Oct. 11, 1999, at C1.

303. *See supra* Section II.C.

304. These businesses had to react quickly, being granted only 15 days in November 1998 to submit their comments. *See* Letter from David Aaron, Undersecretary of Commerce for International Trade, to Industry Representatives (visited Nov. 4, 1998) <http://www.ita.doc.gov/ecom/aaron114.html#Safe>.

305. Direct marketers were represented by the Direct Marketing Association (DMA). *See Comments of the Direct Marketing Association on the Department of Commerce Draft Safe Harbor Principles* (visited Apr. 4, 1999) <http://www.ita.doc.gov/ecom/com2abc.htm#dma>. The DMA is very

pharmaceutical and health industries.[311] The information technology industry was the most active, both through individual company and collective submissions by industry organizations.[312]

---

active on the safe harbor issue. In a letter submitted to the Department of Commerce, H. Robert Wientzen, the President and CEO of DMA, argued that the market should be the controlling force in global data privacy regulation. *See* Thom Weidlich, *DMA Criticizes Euro Data Directive*, DIRECT, May 15, 1998, at 13.

306. Retailers were represented by groups such as the National Retail Federation and the Toy Manufacturers Association of America. *See Comments of the National Retail Federation on the Department of Commerce Draft Safe Harbor Principles* (visited Apr. 4, 1999) <http://www.ita.doc.gov/ecom/com2abc.htm#nrf>; *Comments of the Toy Manufacturers Association on the Department of Commerce Draft Safe Harbor Principles* (visited Apr. 4, 1999) <http://www.ita.doc.gov/ecom/com4abc.htm#toy>.

307. Submissions were made by the Magazine Publishers of America, the Interactive Digital Software Association, Time Warner, McGraw-Hill Companies, Amazon.com, and LEXIS-NEXIS. *See Comments of the Magazine Publishers of America on the Department of Commerce Draft Safe Harbor Principles* (visited Apr. 4, 1999) <http://www.ita.doc.gov/ecom/com2abc.htm#mpa>; *Comments of the Interactive Digital Software Association (IDSA) on the Department of Commerce Draft Safe Harbor Principles* (visited Apr. 4, 1999) <http://www.ita.doc.gov/ecom/com1abc.htm#idsa>; *Comments of Time Warner on the Department of Commerce Draft Safe Harbor Principles* (visited Apr. 4, 1999) <http://www.ita.doc.gov/ecom/com1abc.htm#time>; *Comments of the McGraw-Hill Companies on the Department of Commerce Draft Safe Harbor Principles* (visited Apr. 4, 1999) <http://www.ita.doc.gov/ecom/com1abc.htm#mcgraw>; *Comments of Amazon.com on the Department of Commerce Draft Safe Harbor Principles* (visited Apr. 4, 1999) <http://www.ita.doc.gov/ecom/com4abc.htm#amazon>; *Comments of LEXIS-NEXIS on the Department of Commerce Draft Safe Harbor Principles* (visited Apr. 4, 1999) <http://www.ita.doc.gov/ecom/com4abc.htm#lexis>.

308. Submissions were made through the Council of Insurance Agents and Brokers, the American Council of Life Insurance, and Allstate Insurance Company. *See Comments of the Council of Insurance Agents and Brokers on the Department of Commerce Draft Safe Harbor Principles* (visited Apr. 4, 1999) <http://www.ita.doc.gov/ecom/com3abc.htm#ciab>; *Comments of the American Council of Life Insurance on the Department of Commerce Draft Safe Harbor Principles* (visited Apr. 4, 1999) <http://www.ita.doc.gov/ecom/com3abc.htm#acli; *Comments of Allstate Insurance Company on the Department of Commerce Draft Safe Harbor Principles* (visited Apr. 4, 1999) <http://www.ita.doc.gov/ecom/com4abc.htm#allstate>.

309. Submissions were made by Citigroup, American Banker's Association, the Securities Industry Association, and Dun & Bradstreet. *See Comments of Citigroup on the Department of Commerce Draft Safe Harbor Principles* (visited Jan. 13, 1999) <http://www.ita.doc.gov/ecom/com4abc.htm#citi>; *Comments of the American Banker's Association on the Department of Commerce Draft Safe Harbor Principles* (visited Apr. 4, 1999) <http://www.ita.doc.gov/ecom/comabc.htm#aba>; *Comments of the Securities Industry Association on the Department of Commerce Draft Safe Harbor Principles* (visited Apr. 4, 1999) <http://www.ita.doc.gov/ecom/com4abc.htm#sia>; *Comments of Dun & Bradstreet on the Department of Commerce Draft Safe Harbor Principles* (visited Apr. 4, 1999) <http://www.ita.doc.gov/ecom/com2abc.htm#d&b>.

310. Submissions were made by Visa U.S.A. and Associated Credit Bureaus. *See Comments of Visa U.S.A. on the Department of Commerce Draft Safe Harbor Principles* (visited Apr. 4, 1999) <http://www.ita.doc.gov/ecom/com2abc.htm#dma>; *Comments of the Associated Credit Bureaus on the Department of Commerce Draft Safe Harbor Principles* (visited Apr. 4, 1999) <http://www.ita.doc.gov/ecom/com2abc.htm#dma>.

311. Pharmaceutical and health industry interests were represented through Pharmaceutical Research and Manufacturers of America, Health Industry Manufacturers Association, Eli Lilly and Company, and Novartis. *See Comments of the Pharmaceutical Research and Manufacturers of America on the Department of Commerce Draft Safe Harbor Principles* (visited Apr. 4, 1999) <http://www.ita.doc.gov/ecom/com4abc.htm#phrma>; *Comments of the Health Industry Manufacturers Association on the Department of Commerce Draft Safe Harbor Principles* (visited Apr. 4, 1999) <http://www.ita.doc.gov/ecom/com1abc.htm#health>; *Comments of Eli Lilly and Company on the Department of Commerce Draft Safe Harbor Principles* (visited Apr. 4, 1999) <http://www.ita.gov/ecom/com4abc.htm#eli>; *Comments of Novartis on the Department of Commerce Draft Safe Harbor Principles* (visited Apr. 4, 1999) <http://www.ita.doc.gov/ecom/com3abc.htm#novartis>.

312. Individual companies submitting comments included America Online, Netscape, Yahoo,

Because businesses have high per capita stakes in opposing data privacy regulation,[313] they dedicate vast resources to sway government officials on data privacy issues. Individual company positions on the Safe Harbor Principles were reinforced by submissions from sector-specific associations, which were in turn supplemented by submissions from cross-sectoral associations.[314] Large multinational businesses also work through transnational networks such as the Transatlantic Business Dialogue, which links over one hundred multinational companies based in the United States and Europe. Department of Commerce representatives confirm that no transatlantic commercial issues are addressed by government regulators without seeking TABD input.[315]

In promoting "self-regulation" as an alternative to EU regulation, however, businesses are simultaneously pressed to raise their internal standards. Suddenly, businesses and business associations are developing a

---

Bell Atlantic, IBM, and Compaq. *See Comments of America Online, supra* note 120; *Comments of Netscape on the Department of Commerce Draft Safe Harbor Principles* (visited Apr. 4, 1999) <http://www.ita.doc.gov/ecom/com1abc.htm#netscape>; *Comments of Yahoo on the Department of Commerce Draft Safe Harbor Principles* (visited Apr. 4, 1999) <http://www.ita.doc.gov/ecom/com1abc.htm#yahoo>; *Comments of Bell Atlantic on the Department of Commerce Draft Safe Harbor Principles* (visited Apr. 4, 1999) <http://www.ita.doc.gov/ecom/com1abc.htm#bell>; *Comments of IBM on the Department of Commerce Draft Safe Harbor Principles* (visited Apr. 4, 1999) <http://www.ita.doc.gov/ecom/com2abc.htm#ibm>; *Comments of Compaq on the Department of Commerce Draft Safe Harbor Principles* (visited Apr. 4, 1999) <http://www.ita.doc.gov/ecom/com2abc.htm#compaq>. Companies also submitted comments collectively through such organizations as the Information Technology Industry Council, the Information Technology Association of America, and the Information Industry Association. *See Comments of the Information Technology Industry Council (ITIC) on the Department of Commerce Draft Safe Harbor Principles* (visited Apr. 4, 1999) <http://www.ita.doc.gov/ecom/com1abc.htm#iti>; *Comments of the Information Technology Association of America (ITAA) on the Department of Commerce Draft Safe Harbor Principles* (visited Apr. 4, 1999) <http://www.ita.doc.gov/ecom/com1abc.htm#itaa>; *Comments of the Information Industry Association (IIA) on the Department of Commerce Draft Safe Harbor Principles* (visited Apr. 4, 1999) <http://www.ita.doc.gov/ecom/com1abc.htm#iia>.

313. *See supra* Section I.C.

314. Cross-sectoral associations that submitted comments included the U.S. Chamber of Commerce, the U.S. Council on International Business (which is a member of the International Chamber of Commerce), the Coalition of Service Industries, and the Online Privacy Alliance. *See Comments of the U.S. Chamber of Commerce on the Department of Commerce Draft Safe Harbor Principles* (visited Apr. 4, 1999) <http://www.ita.doc.gov/ecom/com2abc.htm#uschamber>; *Comments of the U.S. Council on International Business (USCIB) on the Department of Commerce Draft Safe Harbor Principles* (visited Apr. 4, 1999) <http://www.ita.doc.gov/ecom/com1abc.htm#uscib>; *Comments of the Coalition of Service Industries on the Department of Commerce Draft Safe Harbor Principles* (visited Apr. 4, 1999) <http://www.ita.doc.gov/ecom/com3abc.htm#csi>; *Comments of the Online Privacy Alliance on the Department of Commerce Draft Safe Harbor Principles* (visited Apr. 4, 1999) <http://www.ita.doc.gov/ ecom/com2abc.htm#opa>.

315. *See US, EU Business Leaders To Urge Further Easing of Impediments to Trade*, 14 Int'l Trade Rep. (BNA) 1909 (citing statement of Timothy J. Hauser, Acting Undersecretary of Commerce for International Trade, that "'virtually every' market opening initiative undertaken by the United States and the European Union in the past couple of years has been suggested by the TABD"). TABD, like other business organizations, supports self-regulatory mechanisms through the development of model private contractual provisions to address privacy concerns arising from transborder data transfers. The official TABD position on data privacy is that "the TABD is committed to working with EU and US administrations/governments to foster the mutual recognition of culturally different but nevertheless adequate regimes for privacy protection that will meet consumer needs and expectations for privacy protection in the digital environment." *See 1998 EC and US TABD Priorities in Electronic Commerce* (visited Jan. 12, 1999) <http://www.tabd.org/resources/content/apr98.html>.

plethora of data privacy protection "principles," "guidelines," model contracts, and other schemes. The Paris-based International Chamber of Commerce has developed model contract provisions.[316] The Direct Marketing Association (DMA) has created "Guidelines for Personal Information Protection."[317] In June 1998, a group of fifty-one businesses and business associations formed the Online Privacy Alliance, which immediately devised a set of privacy guidelines.[318] Companies such as Intel, Microsoft, and Disney have announced that "they will forgo advertising on sites that do not adhere to fair information practices."[319] Numerous other businesses and associations have adopted or are developing privacy codes, guidelines, and other measures.[320] The timing of these multiple efforts in conjunction with the EU Directive's coming into force in October 1998 is no coincidence. These self-regulatory schemes are the EU Directive's bastard offshoots—the unplanned offspring of the EU Directive's encounter with U.S. business.[321] The EU Directive has pressured U.S. agencies to pressure U.S. businesses to make self-regulatory mechanisms a more meaningful alternative—and complement—to government regulation.[322] U.S.-EU negotiations over Safe Harbor Principles help determine self-regulation's contours.

---

316. *See* International Chamber of Commerce, *ICC Model Clauses for Use in Contracts Involving Transborder Data Flows* (visited Nov. 11, 1999) <http://www.iccwbo.org/home/statements_rules/rules/1998/mode/_clauses.asp>; *see also* Weidlich, *supra* note 305, at 15.

317. The DMA recommends these to its members, which include most direct marketing companies. *See* Reidenberg, *supra* note 97, at 510.

318. The program calls for greater education of consumers and businesses on privacy issues to enhance the efficacy of a private contract-based model. The guidelines recommend independent review of business privacy policies and a uniform seal to indicate compliance with the guidelines. The Alliance's proposed consumer complaint resolution system, nonetheless, remains business friendly. The system would require consumers first to attempt to resolve any conflict over privacy issues directly with the company. Only in the event that a satisfactory resolution is not reached may the consumer employ a private complaint resolution mechanism established under the seal program. Alliance members include America Online, Apple Computer, AT&T, Compaq, Disney, Dun and Bradstreet, Equifax, IBM, LEXIS-NEXIS, Microsoft, Netscape, Time Warner, Viacom, the American Advertising Federation, the Direct Marketing Association, the Internet Alliance, and the Software Publishers Association. For a full list of committed organizations, see the attachment to *Testimony of Ms. Christine Varney on Behalf of the Online Privacy Alliance Before the House Subcommittee on Telecommunications, Trade and Consumer Protection* (visited July 21, 1998) <http://www.privacyalliance.org/resources/Varney_July_21.pdf>. For the Online Privacy Alliance's guidelines on enforcement issues, see *Effective Enforcement of Self Regulation* (visited Jan. 12, 1999) <http://www.privacyalliance.org/resources/enforcement.shtml>.

319. *Testimony of Ms. Christine Varney*, *supra* note 318.

320. For example, the Interactive Digital Software Association, which represents businesses that sell video and computer games, has adopted privacy guidelines. *See Comments of IDSA*, *supra* note 307. IDSA claims that its guidelines closely conform to the draft Safe Harbor Principles. *See id.*; *see also Comments of the ITAA*, *supra* note 312; *"Privacy Principles" of the IBAA, the Bankers Roundtable, the American Bankers Association, and the Consumer Bankers Association* (visited Nov. 11, 1999) <http://www.ftc.gov/reports/privacy3/comments/012b.htm> (referring to private sector guidelines).

321. The term "bastard" is used not in the sense that self-regulatory schemes are necessarily illegitimate or ill-conceived, though many privacy advocates so claim. Rather, the term reflects the fact that these private schemes were not planned by the EU Directive's proponents.

322. As the FTC noted in its July 1999 Report on Self-Regulation and Privacy Online, "online businesses are providing significantly more notice of their information practices than they were last year." FTC JULY 1999 REPORT ON SELF-REGULATION, *supra* note 239, at 6. The FTC cites two studies by Professor Mary Culnan of the McDonough School of Business of Georgetown. *See id.* at n.33 (citing <http://www.msb.edu/faculty/culnanm/gippshome.html>).

2. *Caught in a Bind: Businesses' Support and Wariness of the Department of Commerce's Approach*

Business groups are caught in a bind by the Department of Commerce's Safe Harbor Principles. On the one hand, they strongly support Commerce's efforts to negotiate a "safe harbor" with EU authorities that protects business from EU data transfer restrictions. On the other hand, they fear that the Safe Harbor Principles will lead to more costly data privacy requirements in the United States. Their comments on Commerce's Safe Harbor Principles thus had two primary purposes: (i) to narrow the scope of obligations provided in the Safe Harbor Principles,[323] and (ii) to ensure that EU authorities are bound by the Principles and cannot restrict data transfers on other grounds.[324]

A primary reason U.S. businesses are more wary of the EU Directive's provisions than EU businesses comes down to differences in legal culture. Given the adversarial nature of U.S. legal culture, businesses engaging in the same conduct, subject to the same legal obligations, face much higher litigation risks and costs in the United States than in Europe.[325] Individuals are more likely to bring suit against companies in the United States. The costs of litigation (particularly the costs of discovery) are substantially steeper in the United States, and damage awards are larger, increasing average settlement costs. In addition, activist groups will more likely challenge agencies before courts in the United States for failing to stringently apply regulations. In contrast, in continental Europe non-governmental groups play only a limited role in challenging governmental and corporate actions before courts and regulatory bodies.[326] Thus, U.S. businesses' adverse reactions to the EU

323. As for the scope of obligations, some businesses want entire sectors clearly excluded from the coverage by the Safe Harbor Principles. Some argue journalism should be excluded on First Amendment grounds. *See Comments of McGraw-Hill, supra* note 307. Others argue certain pharmaceutical and medical research should be excluded in order to promote the development of new health products. *See Comments of the Health Industry Manufacturers, supra* note 311; *Comments of the Pharmaceutical Research and Manufacturers of America, supra* note 311.

324. *See infra* notes 343–344 and accompanying text.

325. For a presentation of the costs of U.S. legal culture, what Kagan calls "adversarial legalism," see generally Kagan, *Adversarial Legalism, supra* note 82. A secondary explanation for the difference in reactions of U.S. and EU businesses is that U.S. businesses are much more advanced in the use of information and thus are affected more by regulatory constraints. While it is true that the use of computers and the Internet, the gathering of information from wide sources, and direct marketing enabled by such information are all significantly more widespread in the United States, this is still a much weaker rationale. European businesses are also technologically sophisticated and make increasing use of information and information technology.

326. This is particularly true in continental Europe. In large part, this reflects a systemic difference in U.S. and European systems of governance. The United States is a more pluralist system where private interests organize to press for their goals, both in lobbying legislatures and challenging government agencies and corporate actors before courts. In continental Europe, the bureaucratic state plays a more central role, in particular in the provision of social protections. *See supra* note 147. In addition, the procedural rules of European legal systems provide fewer incentives for private groups to engage in socially activist litigation. Unlike in the United States, European courts do not recognize class actions or contingency fees, or award high attorneys' fees or punitive damages. Non-governmental advocates play a greater role in the United Kingdom, but their actions are still limited by less favorable procedural rules. For a discussion of the uniqueness of American class action suits, see Richard Cappalli & Claudio Consolo, *Class Actions for Continental Europe? A Preliminary Inquiry*, 6 TEMP. INT'L. & COMP. L.J. 217 (1992).

Directive are not solely on account of the EU Directive's contents, but also on account of businesses' experience with U.S. legal culture. Even if not formally stated, a large part of the Department of Commerce's mission is to persuade EU authorities to accept enhanced self-regulatory schemes as adequate on these grounds.

Ideally, businesses would like to eviscerate Commerce's Safe Harbor Principles of substance, so that businesses would retain maximum autonomy to profit from the use of personal data. Businesses thus criticized each of Commerce's seven principles as unreasonable restraints on business operations. Businesses' comments show that, if business had its way, the principles would be words without impact. Yet it appears businesses will be largely unsuccessful. Although privacy advocates may also be unsatisfied, Commerce's revised guidelines, published in April 1999, primarily retained or enhanced the stringency of the initial principles.[327]

On the "Notice" principle, businesses argued that the amount of information Commerce required to be provided in notices was unduly burdensome[328] and that timing requirements for providing notice should be loosened.[329] Although Commerce took some comments into account, the core of the notice principle remains.[330] On the second principle, entitled "Choice," businesses asserted that an "opt-in" choice for "sensitive" data should be eliminated, and that an "opt-out" right should correspondingly only apply to "sensitive" data, narrowly defined.[331] They insisted that "opt-out" rights should not apply to "public" or "proprietary" information, or information needed to combat consumer fraud, even if "sensitive."[332] However, Commerce's revised guidelines instead eliminated the vague qualification that the principles "do not apply to proprietary" information, retained the "opt-in"

---

327. *See* April 1999 Safe Harbor Privacy Principles, *supra* note 251.

328. *See, e.g., Comments of the Magazine Publishers of America, supra* note 307 (proposing that the current U.S. regime should be maintained). The DMA stated that providing consumers with an opt-out right is sufficient, so that there should be no requirement that consumers be notified of the potential recipients (such as direct marketers). *See Comments of the DMA, supra* note 305. Similarly, the ITAA wished to limit the information that must be provided concerning how they collect information (claiming this is proprietary) and to whom they will disclose it. *See Comments of the ITAA, supra* note 312.

329. In particular, businesses maintained that they should be excused from providing prior notice of privacy policies when they first contact consumers by telephone or other non-online means. *See, e.g., Comments of DMA, supra* note 305; *Comments of McGraw-Hill, supra* note 307; *Comments of the National Retail Federation, supra* note 306; *Comments of Time Warner, supra* note 307.

330. *Compare* November 1998 Safe Harbor Privacy Principles, *supra* note 249, *with* April 1999 Safe Harbor Privacy Principles, *supra* note 251.

331. *See, e.g., Comments of ITAA, supra* note 312. The ITAA wished to narrow the definition of sensitive information to "medical and health information as well as information related to children under the age of 13" (the latter being already required under U.S. law). *Id.* Citigroup proposed that the term "informed consent" be substituted for the term "opt in." *See Comments of Citigroup, supra* note 309.

332. *See, e.g., Comments of the American Council of Life Insurance, supra* note 308; *Comments of the National Fraud Center on the Department of Commerce Draft Safe Harbor Principles* (visited Jan. 13, 1999) <http://www.ita.doc.gov/ecom/com1abc.htm#national>; *Comments of Stone Investments on the Department of Commerce Draft Safe Harbor Principles* (visited Jan. 13, 1999) <http://www.ita.doc.gov/ecom/com1abc.htm#stone>.

choice for sensitive information, and defined the term "sensitive" broadly, taking the definition from article 8 of the EU Directive.[333]

Businesses wanted the third principle, entitled "Onward Transfer," deleted and merged into the "Notice" and "Choice" provisions.[334] They did not want to risk liability for the actions of their third-party transferees, contending that this would result in unreasonable secondary liability.[335] Rather, they wished to limit their obligations to providing notice to consumers that information could be transferred to third parties unless the consumer "opted out." While Commerce's revised guidelines tied the Onward Transfer principle more closely to the initial two principles, it expanded the definition of sensitive information for which affirmative "opt-in" consent is required.[336]

On the fourth, fifth, and sixth principles—"Security," "Integrity," and "Access"—businesses wanted to limit their obligations to securing, maintaining, and providing access to only "sensitive" information, in order to limit compliance costs and potential liability. They maintained that responding to consumer requests for access to non-sensitive information would be an "expensive and time consuming process."[337] They likewise asserted that a requirement for them to retain only "current" and "complete" data would result in costs beyond any compensating benefit to consumers.[338] Commerce's revised guidelines concerning "Security," "Integrity," and "Access," however, apply to all information. While under the Access principle, Commerce is attempting to retain a qualification that access need only be "reasonable," the European Union is demanding this limitation be eliminated or more narrowly defined.[339]

As regards the key issue of "Enforcement," businesses demanded that enforcement may be permitted through self-regulatory mechanisms, which alone would decide the appropriate consequences of violations. In particular, businesses wished to exclude any private right of action to sue for damages before courts or administrative tribunals. One organization, the Information Technology Industry Council, went so far as to maintain that no reference

333. *See* April 1999 Safe Harbor Principles, *supra* note 251; EU Directive, *supra* note 2, art. 8.

334. *See, e.g., Comments of the DMA, supra* note 305; *Comments of the IIA, supra* note 312; *Comments of the Individual Reference Services Group (IRSG) on the Department of Commerce Draft Safe Harbor Principles* (visited Jan. 13, 1999) <http://www.ita.doc.gov/ecom/com1abc.htm#irsg>.

335. *See, e.g., Comments of Bell Atlantic, supra* note 312 (discussing lack of certainty and third-party transferees); *Comments of the ITIC, supra* note 312 (exhibiting concerns about third-party liability, among other objections); *Comments of Netscape, supra* note 312 (focusing on liability for third-party transferees' behavior); *Comments of Yahoo, supra* note 312 (discussing the outward transfer and access to information).

336. *See* April 1999 Safe Harbor Privacy Principles, *supra* note 251.

337. *Comments of the IDSA, supra* note 307 (discussing differences between current self-regulation guidelines and the Safe Harbor Principles); *see also Comments of the IRSG, supra* note 334; *Comments of the ITAA, supra* note 312; *Comments of the ITIC, supra* note 312.

338. *See Comments of the DMA, supra* note 305; *Comments of the IIA, supra* note 312; *Comments of McGraw-Hill, supra* note 307.

339. *See* April 1999 Safe Harbor Privacy Principles, *supra* note 251. In the initial Guidelines, Commerce's draft implied that the term "reasonable access" might signify that access would only be available for sensitive information, which was left undefined. *See* November 1998 Safe Harbor Privacy Principles, *supra* note 249. This vague reference has since been eliminated. *See* April 1999 Safe Harbor Privacy Principles, *supra* note 251.

should be made to "sanctions," "as it is unclear how sanctions provide a means for individuals to enforce privacy protection measures."[340] The Information Technology Association of America suggested that the Principles mandate "confidentiality of consumer complaints," to keep complaints out of the press.[341] In the revised guidelines, Commerce provided for no such limitations.[342]

Finally, in order to ensure that Safe Harbor Principles provide certainty, businesses demanded that the European Union and EU Member State authorities agree not to restrict data transfers to the United States on any grounds other than for failure to comply with the Principles—as opposed to the EU Directive.[343] In other words, while intra-European transfers would remain subject to the EU Directive, transatlantic transfers (from Europe) would only be subject to the Principles.[344] Otherwise, Safe Harbor Principles would merely increase pressure on businesses to enhance U.S. self-regulatory programs, without providing certainty vis-à-vis European regulators. Yet even if the European Union agrees to be bound by Safe Harbor Principles, it is still European authorities who will apply them when deciding whether to restrict transatlantic data transfers. At best, U.S. authorities would be notified by EU authorities, so that U.S. authorities could submit observations and attempt to mediate a conflict. It is European authorities that would ultimately make determinations under the Principles and decide on the consequences of any

340. *Comments of the ITIC, supra* note 312; *see also Comments of American Telephone & Telegraph on the Department of Commerce Draft Safe Harbor Principles* (visited Jan. 13, 1999) <http://www.ita.doc.gov/ecom/com3abc.htm#att>.

341. *Comments of the ITAA, supra* note 312. Similarly, the Information Industry Association and others recommended that companies be permitted to "self-certify" their practices and establish "internal review and certification mechanisms" as adequate enforcement schemes that do not have to be "independently" monitored. *Comments of the IIA, supra* note 312; *see also Comments of the DMA, supra* note 305; *Comments of the ITAA, supra* note 312; *Comments of McGraw-Hill, supra* note 307.

342. *See* April 1999 Safe Harbor Privacy Principles, *supra* note 251. Enforcement is one of the more contentious issues in the U.S.-EU negotiations over the Safe Harbor Principles' content. Not surprisingly, just as the European Union demands meaningful enforcement mechanisms to ensure data privacy protection, the United States does the same when it reviews the adequacy of foreign requirements, as in the *Shrimp-Turtle Case. See supra* Section IV.C. Under proposed implementing regulations of a law requiring foreign protection of endangered sea turtle species in order for shrimp to be imported into the United States, the U.S. Department of State permits "voluntary arrangements between government and fishing industry." Notice of Proposed Guidelines for the Implementation of Section 609 of Public Law 101-62 Relating to the Protection of Sea Turtles in Shrimp Trawl Fishing Operations, 64 Fed. Reg. 14,481, 14,484 (1999). Nonetheless, this regulation requires the voluntary arrangement to include "a governmental mechanism to monitor compliance with the arrangement and to impose penalties for non-compliance" to ensure the industry uses trawling methods that do not endanger sea turtles. *Id.*

343. *See, e.g., Comments of the DMA, supra* note 305; *Comments of Dun & Bradstreet, supra* note 309 (interpreting the principles as being independent of the EU Directive); *Comments of the ITAA, supra* note 312; *Comments of Time Warner, supra* note 307.

344. Ideally, U.S. businesses would like immunity from any data privacy lawsuit brought in the European Union by any EU resident so long as the business complies with the Safe Harbor Principles. *See, e.g., Comments of Allstate, supra* note 308; *see also Comments of the IRSG, supra* note 334. As the Individual Reference Services Group asserted, "organizations that voluntarily agree to comply with the safe harbor principles [should only] be challenged with respect to compliance, but not with respect to the adequacy of the principles." *Comments of the IRSG, supra* note 334. The IRSG creates information databases on individuals so that they may be identified and located "for a variety of beneficial purposes," assisting "law enforcement agents, the media, attorneys and private investigators." *Id.*

violation. The pressure on U.S. businesses to take account of potential lawsuits brought by European authorities would remain.

3. *Privacy Protection Imported: Spill-Over Effects of U.S.-EU Negotiations on U.S. Business Practice*

Although the negotiation of Safe Harbor Principles is intended to protect U.S. businesses from EU regulators, it also affects data privacy practices within the United States. Businesses realize this. As the Information Technology Association of America affirms,

> [w]hile [Commerce's] November 4th letter explicitly states that the Safe Harbor Principles are designed only to address the effect of the EU data protection directive on the U.S., we are sensitive to the fact that regardless of its intent, the safe harbor principles will inevitably have an impact on the domestic debate on privacy.[345]

While the Safe Harbor Principles do not formally apply to purely domestic data processing operations, they have de facto effects within the United States. Most importantly, once U.S. businesses adopt internal data privacy policies to avoid EU transfer restrictions, they subject themselves to potential FTC enforcement proceedings for failure to comply with proclaimed policies. In any case, it will be pragmatically difficult for businesses to employ two sets of data privacy practices, one for EU residents (providing for greater privacy protection) and one for U.S. residents (providing for less).[346] Business databases will often include information about EU and U.S. residents, in which case businesses will have to comply with the more exacting EU requirements.[347] In addition, if businesses provide greater data privacy protection for EU residents than for U.S. residents, they may prejudice their public image. Privacy advocates have already jumped on the issue of dual standards implicit under the Safe Harbor Principles.[348] They proclaim that "U.S. companies should be required to protect all their customers," so that "U.S. citizens should gain the same protections [as EU citizens]."[349] Otherwise, U.S. citizens would be effectively treated as second-class citizens

345. *Comments of the ITAA*, *supra* note 312; *see also Comments of the Magazine Publishers of America*, *supra* note 307 ("We are concerned, however, that, while you state that the Draft Principles are not intended to govern or affect U.S. privacy regimes, these principles will, in fact, do precisely that.").

346. *See Comments of the USCIB*, *supra* note 314. (The U.S. Council for International Business is the U.S. representative to the International Chamber of Commerce). Some U.S. companies nonetheless demand clarification that indeed they may continue to treat U.S. consumers separately under less costly and burdensome U.S. privacy regimes. *See, e.g.*, *Comments of National Retail Federation*, *supra* note 306. American Express is currently working to establish contracts between internal business units with the goal of preventing the names of European citizens held on computers in the United States from being used in direct marketing. *See* Gregory Dalton, *Privacy Law Worries U.S. Businesses—European Regulation Could Have Far-Reaching Impact*, INFO. WK., Oct. 26, 1998, at 26.

347. As Kagan notes in his summary of case studies involving a variety of industries, there is "evidence for a dynamic toward trans-national 'corporation-level' harmonization of regulatory compliance routines in multinational companies, keyed to compliance with the most stringent national standards (sometimes with a margin of error)." Kagan, *Regulatory Encounters*, *supra* note 82, at 4.

348. *See Comments of Mark Silbergeld*, *supra* note 107.

349. *Id.*

in their own country. Second, U.S.-EU attempts to avoid disrupting data flows by agreeing to a definition of "adequate" data privacy protections are an important step toward the harmonization of protection standards and business practices worldwide. As the general counsel to America Online states, "inevitably those Safe Harbor Principles will get imported into U.S. policy regimes and then adopted potentially by other countries as their data privacy regimes."[350] The U.S. Council of Better Business Bureaus confirms: "[I]t is realistic to expect that protocols endorsed by the Department of Commerce and the EU will enjoy wide currency and acceptance in the business community."[351] This is troublesome to U.S. businesses, which would prefer U.S.-EU negotiations to focus less on adapting U.S. laws and practices to meet EU adequacy requirements, and more on adapting EU laws to U.S. self-regulatory approaches.[352]

The spill-over effects of EU requirements on U.S. business practice are already occurring. Oracle responded to the EU requirements "by tightening access to its customer and employee databases."[353] When Citibank encountered problems with German data protection laws (which are similar to the EU Directive), in order to continue transmitting data transatlantically, it entered into an "Inter-Territorial Agreement" to assure adequate data privacy protection, which was subject to German law and could be enforced by German authorities.[354] Multinational firms that adapt their internal practices to EU requirements can, over time, have a reduced stake in retaining lower U.S. standards, potentially facilitating an upgrading of U.S. standards.[355] Within the United States, internal corporate privacy policies now proliferate. New monitoring and enforcement schemes are being developed. European Union

---

350. *EU Rejects U.S. Data Privacy Plan*, *supra* note 189, at 1963 (quoting George Vrandenberg).

351. *Comments of the Council of Better Business Bureaus*, *supra* note 283.

352. A number of business representatives critique the draft Safe Harbor Principles as a move toward a European model, even though the Principles are aimed in theory at promoting a private, industry-led, self-regulatory alternative. Businesses are concerned that the Department of Commerce's guidelines propel the United States toward a centralized "one-size-fits-all" EU-style privacy regime because Commerce's draft principles apply to all business operations. They maintain that this is contrary to the traditional U.S. sector-specific, problem-specific approach to data privacy regulation. *See, e.g.*, *Comments of the Associated Credit Bureaus*, *supra* note 310; *Comments of the Magazine Publishers of America*, *supra* note 307; *Comments of the Online Privacy Alliance*, *supra* note 314; *Comments of Stone Investments*, *supra* note 332; *Comments of Time Warner*, *supra* note 307. Some businesses propose that Commerce should not agree on a general, cross-sector set of Safe Harbor Principles with the European Union, but rather should agree on Safe Harbor Principles on a sector-by-sector basis. *See Comments of IBM*, *supra* note 312.

353. K. Oanh Ha, *European Privacy Protection Forces U.S. Firms To Scramble*, SAN JOSE MERCURY NEWS, Oct. 26, 1998, at 1E.

354. *See* Interview with Scott Blackmer, *supra* note 44 (Blackmer represented Citibank on this matter); *see also Transfers of Personal Data to Third Countries*, *supra* note 44, at 7; Andrews, *supra* note 81.

355. The firms' initial compliance costs resulting from modified consumer notices, consent forms, and data retention and access procedures, should be reduced and spread out over time. This latter point is stressed in David Vogel's work. *See* VOGEL, *supra* note 9, at 5–8. This point, however, is subject to an important caveat. To the extent that firms, even after adapting more protective data privacy practices, face significant litigation-related costs in the United States, they will continue to advocate strongly for lower U.S. standards—in the name of self-regulation.

authorities and U.S. domestic advocates demand that these schemes be made more stringent so that companies face real consequences for not doing what they say. In multiple ways, U.S. firms are being pressed to import the practices that Europe requires to the United States.

VI. CONCLUSION: TRADING UP—THE FACTORS THAT FACILITATE RAISING U.S. DATA PRIVACY STANDARDS

Through its political and economic clout and the demands of its marketplace, the United States influences foreign regulatory policy and business practice. The United States is often criticized for exporting its norms and imposing its standards on foreign countries.[356] The impact of the EU Directive demonstrates that the actions of other powerful states also shape U.S. regulation and business practice. Although the scope and content of U.S. regulation of data privacy protection depend substantially on domestic factors, EU regulatory policy significantly affects the playing field in the United States on which competing interest groups clash. External pressures from the European Union enhance the impact of U.S. internal pressures. The EU Directive prods U.S. businesses to change their behavior to avoid confrontations with EU regulators. It prompts U.S. regulators to press U.S. businesses to enhance their internal standards to avoid a regulatory conflict. It presents U.S. privacy advocates with a functioning alternative to U.S. law that they can promote. By changing the stakes of U.S. actors, the EU Directive changes the way all U.S. institutions—legislatures, regulators, courts, and markets—address data privacy issues. As Marc Rotenberg of EPIC affirms, "[a]ll the energy spent on the EU Directive has caused the U.S. to focus on privacy and raising our privacy standards."[357]

Where firms operate in multiple jurisdictions with differing regulatory requirements, they sometimes demand that requirements be harmonized so as to reduce their overall compliance costs. Critics of globalization maintain that this harmonization process can lead to low regulatory standards—the lowest common denominator. Yet the U.S.-EU conflict over data privacy protection demonstrates that in a globalizing economy, social protection levels are not necessarily driven downward in the United States. Regardless of the outcome of discussions between the United States and the European Union, U.S. companies with operations in Europe—even where those operations simply involve the gathering of information from a website—are pressed to conform their data processing practices toward EU standards.[358]

356. *See, e.g.*, Aviva Freudmann, *The US-EU Relationship*, J. COM., Mar. 29, 1999, at 14 (noting the EU critique of the Helms-Burton Act); Carey Goldberg, *Limiting a State's Sphere of Influence*, N.Y. TIMES, Nov. 15, 1998, at A4 (discussing the state of Massachusetts's attempts to sanction foreign businesses operating in Burma). Developing countries have also critiqued the U.S. imposition of intellectual property protection regimes and environmental policies. For a discussion of the WTO *Shrimp-Turtle Case*, in which developing countries challenged U.S. trade restrictions designed to change their domestic environmental protection policies, see Shaffer, *Shrimp-Turtle*, *supra* note 217.

357. Ha, *supra* note 353 (quoting Rotenberg).

358. Similarly, as discussed by Vogel, firms already required to meet high standards may prefer harmonization at a higher level that imposes disproportionate costs on their competitors who do not

There are five primary factors that explain why globalization pressures potentially drive U.S. social protection upward in the area of data privacy. They dovetail with the five central themes presented in this Article's introduction:

(i) The Link with Liberalization: Transnational Institutional Interdependence

First, economic liberalization and data privacy protection are intrinsically linked. Firms wishing to participate in a globalizing economy face conflicting regulations. The regulation of data privacy, in particular, matters to firms because it affects the exploitation of information, which is increasingly important in a technology-driven, network-linked, globalizing economy. Firms demand that conflicts be managed to ward off the threat of restrictions on their international operations. If firms did not extend their domestic operations abroad, there would be no conflict to resolve through harmonizing data privacy standards. There would be no transnational institutional interdependence.

Businesses' demand for greater trade liberalization paradoxically permits social protection to be leveraged upward and not necessarily downward in a "race to the bottom." Were U.S. companies to operate only domestically, they would be unconcerned with the EU Directive. When they wish to invest, operate, and trade between multiple jurisdictions, whether independently or through complex networks of affiliates and alliances, they must adapt to foreign regulatory policies. United States businesses must adapt practices in the United States to avoid EU restrictions and potential litigation before EU courts and administrative bodies.[359] United States regulatory authorities are instructed to fend off a regulatory conflict with the European Union having potentially significant financial repercussions. In the process, these officials are pressed to enhance U.S. domestic data privacy practices in order to defend the "adequacy" of U.S. protections. Ironically, companies' desire to increase revenue through trade and investment in the European Union ultimately permits U.S. privacy advocates and regulators to use the attention given to U.S.-EU clashes over the EU Directive to promote greater data privacy protection at home.[360]

---

already meet such standards. *See* VOGEL, *supra* note 9, at 12–13.

359. Ultimately, of course, the EU Directive's impact will largely depend on its enforcement. The Commission and Member State authorities remain understaffed so that enforcement is an issue. Yet Member State authorities already enforce Member State data privacy law. Moreover, as noted in Section V.B, *supra*, privacy advocates can act as private attorneys general, and privacy service providers, including legal advisors and in-house privacy directors, can also significantly affect business behavior. United States businesses have strongly reacted to the EU Directive because they feel its potential impact is significant.

360. The analysis of the "spill-over effects" in the context of European integration is the defining aspect of the neo-functionalist theory of Ernst Haas. *See generally* ERNST HAAS, THE UNITING OF EUROPE (1958). This Article, however, does not employ an apoliticized *spill-over* explanation for the link between trade liberalization and data privacy policy. Rather, while the links between trade liberalization and data privacy protection are important, the exercise of market power by the jurisdiction

Even without formal trade and investment liberalization, information passes through an increasingly borderless world.[361] The information revolution permits an increasing number of companies to engage in cross-border transactions. Even small U.S. enterprises have websites, engage in electronic commerce, and may collect information on EU residents, or will do so in the future. On account of their dependence on information and their participation in a globalizing economy, all of these U.S. businesses—large and small, from sector to sector—are potentially subject to and affected by the EU Directive.

(ii) EU Market Power

Second, the authority of EU regulation is bolstered by EU market power. The EU's huge internal market enables it to exercise considerable clout in the negotiation of rules—in particular, harmonizing rules governing firm behavior.[362] The EU Member States collectively harness this market power through coordinating and reallocating decision-making from the individual Member State level to the EU level.[363]

The EU's large internal market provides leverage when the European Union threatens to restrict data transfers to the United States on account of its inadequate data privacy protections. A similar challenge from a country that does not attract significant U.S. investment or trade would have little impact. Not only would U.S. commercial interests be less exposed financially, a country with a small economy would be more prone to a U.S. retaliatory threat. Affected U.S. businesses would harness U.S. power to defend their interests. The United States could tailor retaliation to comply with its WTO legal obligations by eliminating development aid, curtailing preferential trade benefits, or discriminating in sectors not covered by WTO obligations. It would do so knowing that the U.S. market is simply too important for that country to ignore. Correspondingly, there would be little pressure on U.S. authorities to draft Safe Harbor Principles or otherwise promote effective U.S.

---

enforcing higher social protection standards is a key variable.

361. Broad sectors of the U.S. economy increasingly depend on information and information technology. As Cate notes, "[d]uring the 1980s, U.S. businesses alone invested $1 trillion in information technology, and since 1990 they have spent more money on computers and communications equipment than on all other capital equipment combined." CATE, *supra* note 59, at 5. Anne Branscomb calls information "the lifeblood that sustains political, social, and business decisions." Anne Wells Branscomb, *Global Governance of Global Networks: A Survey of Transborder Data Flow in Transition*, 36 VAND. L. REV. 985, 987 (1983); *see also* ANNE WELLS BRANSCOMB, WHO OWNS INFORMATION? (1994). It is estimated that the information technology sector is the fastest growing in the United States, now "accounting for one quarter of economic growth in the United States." WORLD TRADE ORGANIZATION, WTO ANNUAL REPORT 1998, at 35. The Department of Commerce is reported to have recently increased the estimate to "at least a third of the nation's economic growth between 1995 and 1998." *Commerce Report Describes Economic Benefits From Internet*, N.Y. TIMES, June 23, 1999, at C8; *see also* Mark Suzman, *IT Plays Leading Role in U.S. Growth*, FIN. TIMES, Apr. 16, 1998, at 6 (citing Commerce Department study showing that information technology accounts for eight percent of the economy). The variety of companies and business associations that replied to the Department of Commerce's call for comments on its Safe Harbor Principles underscores the importance of information to these sectors. *See supra* notes 304–312.

362. *See supra* Sections I.A., III.A.

363. *See supra* Section III.A.

business practices to avoid a regulatory conflict. It is the conjunction of state market power and high state standards that facilitates standards elsewhere to be ratcheted upward.

While many EU Member States, such as Germany and France, have large economies, they enhance their clout vis-à-vis the United States when acting collectively. The EU Member States have pooled their sovereignty, enabling them to speak with a single, more powerful voice, backed by enhanced market power. The timing of the U.S. reaction to the threat of bans on data transfers from Europe demonstrates this. Before the EU Directive went into effect, many EU Member States had data privacy laws that permitted them to ban data transfers to countries without adequate data privacy protection.[364] Yet it was not until the EU Directive went into effect that U.S. authorities drafted Safe Harbor Principles and increased pressure on companies to raise their internal standards. When the threat moved to the EU level, it was taken more seriously.

(iii) Data Privacy as a Luxury Good More Likely Demanded by Citizens from Wealthy Jurisdictions, Facilitating a Trading Up of Standards

Third, the European Union is rich, and data privacy protection is a good that individuals increasingly demand when they become richer.[365] Even further, data privacy is arguably a luxury good, that is, a good whose demand increases disproportionately vis-à-vis the demand for other goods, as income levels rise.[366] Since the demand for data privacy protection is not easily met at low cost through private contract, individuals are more likely to support governmental intervention to protect their privacy. Goods such as data privacy regulation are thus demanded more in wealthy jurisdictions, and these wealthy jurisdictions are more likely to exercise market power to demand protection abroad. Within the EU itself, the most powerful and richest Member State, Germany, often has the greatest amount of social regulation, facilitating the leveraging up of standards throughout the EU, including—as already seen—data privacy protection standards. When wealthy jurisdictions coordinate their efforts, as have EU Member States, they increase the market impact of their regulatory intervention on foreign trading partners, such as the United States. They use their market power to achieve their domestic policy goals—in this case, pressing for foreign protection of the privacy interests of their citizens.

---

364. *See, e.g.*, Amy Monahan, *Deconstructing Information Walls: The Impact of the European Data Directive on U.S. Businesses*, 29 L. & POL'Y INT'L BUS. 275, 287 (1998) (citing applicable Member State laws).

365. According to a 1998 survey, "it is the prime consumer audience of better-educated and higher-income groups that register the strongest privacy concerns." Westin, *supra* note 144 (summarizing the 1998 Harris-Westin privacy survey "Privacy Concerns and Consumer Choice").

366. This definition of luxury goods is explained in economic terms at *supra* note 22. While I have found no econometric study specifically addressing whether data privacy protection is a luxury good, the proposition is a logical one. Consumers with low income levels should tend to focus on more immediate demands than data privacy protection. Moreover, data privacy concerns rise as individuals use modern technologies—such as credit cards, private telephones, and the Internet—which are more likely to be used by individuals in states with relatively high median income levels.

The United States, of course, is also rich, yet so far mandates less encompassing data privacy protection. Yet in other areas of public policy, the U.S. has been the first to raise standards, which in turn has similarly served to ratchet up European standards. This has been noted in the area of environmental protection,[367] which also arguably constitutes a luxury good whose demand cannot easily be met at low cost through private contract.[368] As David Vogel notes, in the field of environmental protection, European producers selling in the large U.S. market adapt their products to comply with U.S. requirements. Having acquired the experience and technology to meet higher standards, they now have a competitive advantage in complying with them over European producers that do not operate in or export to the United States.[369] A rise in European standards disproportionately raises their domestic rivals' costs. They thus support raising Member State and EU environmental standards or, in any case, less forcefully oppose the efforts of domestic advocates of higher standards.

In both cases—the raising of data privacy protection in the United States and of environmental protection in Europe—standards on one side of the Atlantic have been used to ratchet up standards on the other. There has been no race to the bottom. Social protection has been leveraged up, not leveled down.

---

367. *See* VOGEL, *supra* note 9, at 261–62.

368. There is a significant amount of economic analysis supporting the proposition that environmental standards tend to rise as income levels rise. *See, e.g.*, WERNER ANTWEILER ET AL., IS FREE TRADE GOOD FOR THE ENVIRONMENT? 41 (National Bureau of Economic Research Working Paper No. 6707, 1998), *available at* <http://www.nber.org/papers/w6707> (maintaining that "freer trade is good for the environment," in large part because decreases in pollution associated with increased income outweigh other increases in pollution); Gene M. Grossman & Alan B. Kreuger, *Environmental Impacts of a North American Free Trade Agreement, in* THE MEXICO-U.S. FREE TRADE AGREEMENT 13 (Peter Garber ed., 1993); *cf.* Judith M. Dean, *Trade and the Environment: A Survey of the Literature, in* INTERNATIONAL TRADE AND THE ENVIRONMENT 15 (Patrick Low ed., 1992). Where environmental standards constitute "luxury goods," which should typically be the case, the impact of rising income levels on the demand for environmental protection becomes even more dramatic. While labor standards may also constitute luxury goods, it is easier for individuals with relatively high income levels to enter into a single private employment contract to protect themselves than to enter an almost infinite number of data privacy contracts. Because of the more widespread use of private employment contracts by wealthy individuals, baseline labor standards have differing effects on different segments of society. Environmental and data privacy regulation similarly are more likely than labor regulation to meet the fourth and fifth factors enumerated below, again explaining why they are more susceptible to upward leveraging than labor regulation.

369. This argument is employed by Vogel in *Trading Up*. *See* VOGEL, *supra* note 9, at 5–8 (referring, for example, to the support of Germany's automobile manufacturers for stricter EU fuel efficiency requirements, as well as to the role of more stringent U.S. regulation of chemical products). To cite another product area, toy firms must meet U.S. and EU product safety standards to sell toys in the U.S. and EU markets. Because they reduce their overall costs by producing toys using a single product design and a single production line, these companies will likely comply with U.S. and EU standards for all toys they produce wherever produced (often in China) and wherever sold in the world. The argument employed in this Article, however, is different than Vogel's, as U.S. firms, large and small, have so far opposed further U.S. data privacy regulation. *See supra* Section V.C. Large firms and trade associations have, nonetheless, taken the lead in developing new privacy self-regulatory regimes, such as through the new Online Privacy Alliance. *See id.*

(iv) Externalities of Data Privacy Practices and Policies

Fourth, data privacy policies have significant externalities.[370] Data is collected and exploited by companies located in multiple jurisdictions about individuals residing in multiple jurisdictions, so that the regulatory policy of one jurisdiction affects constituents of others. For EU data privacy policy to be effective, its cross-border effects cannot be avoided because under-regulation in the United States of data privacy protection affects the privacy interests of the EU as well as the U.S. resident. In order to safeguard the privacy of its residents, the European Union regulates the transfer of information not only within the European Union, but also to other jurisdictions. Otherwise, the EU data privacy goals could easily be circumvented through the transfer of information abroad, which is then recompiled, used, and marketed, including back into the European Union itself, whether directly or over the Internet.[371]

The data privacy issue is analogous to many other cross-border and global regulatory issues. With regard to cross-border and global environmental protection, for example, the European Union is necessarily concerned by fallout from the operation of nuclear power plants in Eastern Europe. Particles, whatever their properties, do not stop at national, regional, local, or purely private borders. Similarly, the United States is necessarily concerned by the use of ozone-depleting substances in other countries. Despite internal U.S. policies constraining or eliminating the use of CFC-emitting products, the actions and inactions of producers and consumers in other countries affect U.S. residents.[372]

---

370. For the meaning of the term "externalities" in economics, see *supra* note 20.

371. Existing business tax havens could similarly become havens against data privacy regulation. Bermuda, for example, is striving to become "an e-commerce hub." Duncan Hall, *Bermuda Bids To Become Beachhead for E-Business*, NAT'L L.J., Aug. 30, 1999, at B9 (concerning Bermuda's new Electronic Transactions Act, passed on July 16, 1999).

372. This is *not* to say that in a globalizing economy, all social protection will be leveraged upward in all countries. First, there will be no such pressure in countries whose economies are not integrated in the global economy. *See, e.g.*, DANI RODRIK, HAS GLOBALIZATION GONE TOO FAR? (1997). Second, there is little pressure for labor protection to be enhanced in the United States while, on the contrary, European countries are pressed to make their labor policies more "flexible." *See, e.g.*, Martin Rhodes, *Globalization, Labour Markets and Welfare States: A Future of 'Competitive Corporatism,' in* THE FUTURE OF EUROPEAN WELFARE: A NEW SOCIAL CONTRACT 178 (Martin Rhodes & Y. Mény eds., 1998); Wolfgang Streeck, *Neo-Voluntarism: A New European Social Policy Regime*, 1 EUR. L.J. 39 (1995). Yet labor regulation is different from data privacy protection not only because wealthy individuals more easily protect their working conditions through private employment contracts. *See supra* note 368. In addition, labor protection in one jurisdiction only *directly* affects residents in that jurisdiction. Human rights violations in Burma are only directly suffered by the Burmese. They are not physically suffered by the residents of Massachusetts.

It can be said that, while the effects are less direct, low labor standards in other jurisdictions still have external effects in the United States and Europe. Low labor standards can be morally offensive to purchasers of products in the United States and Europe. Moreover, they can reduce labor's negotiating power vis-à-vis capital in the United States and Europe on account of capital's ability to migrate to countries with lower standards. Yet, although the United States and the European Union have engaged in some efforts to raise foreign labor standards, these efforts have been minimal, and they have also been hampered by constraints imposed by supranational trade rules. *See, e.g., U.S. Labor Standards Proposal Draws Chilly Reception at WTO*, 16 Int'l Trade Rep. (BNA) 203 (Feb. 3, 1999) (discussing U.S. and EU demands that compliance with fair labor standards be integrated into WTO rules). Section 301 in the

(v) Constraints of Supranational Rules

Fifth, international trade rules do not significantly constrain the EU's extra-jurisdictional reach. WTO rules, which otherwise constrain a country's ability to restrict imports and exports, provide for exceptions to address the externalities of data privacy practices and policies. Without the constraint of "negative" supranational rules, positive harmonization is required to manage regulatory conflicts over policies with significant external effects. As a result, trade liberalization rules do not abate the pressure on the United States to raise effectively its data privacy standards. On the contrary, they constrain the ability of the United States to retaliate, again further facilitating a trading up of standards.[373]

In short, the U.S.-EU dispute over data privacy protection is a story of foreign political pressure backed by foreign market power which, in turn, incites new domestic political and regulatory interactions and constrains domestic market practices. The EU Directive's effect on U.S. data privacy practice is made possible because (i) U.S. businesses demand foreign market liberalization in order to exploit foreign markets and, by exploiting the EU market, thereby subject themselves to EU data privacy laws; (ii) EU data privacy laws can be viewed as luxury goods demanded by EU citizens. As the wealth of EU citizens rises, the demand for data privacy protection does likewise; (iii) EU data privacy laws must necessarily affect foreign as well as domestic practices if they are to accomplish their objective of protecting the data privacy of the EU's residents, resulting in a regulatory conflict; (iv) EU Member States use their market power to help satisfy their citizens' demands and Member States increase their market power when they act collectively; and (v) supranational rules do not significantly constrain the EU's application

---

Trade Act of 1974, 88 Stat. 2041 (1975), codified as amended, 19 U.S.C. § 2411(d)(3)(B)(iii) (1994), provides for trade restrictions where a country does not comply with a defined set of fair labor standards. However, this provision has been rarely used.

Were labor interests sufficiently powerful in the United States and Europe, they could harness U.S. and EU market power to attempt to pressure other states or provide side payments to them in exchange for agreeing to modify WTO rules. Labor interests have been unsuccessful in pressuring their governments to do so, in large part due to the relative costs of higher labor standards. Firms engaged in international transactions more forcefully oppose a revision of trade rules permitting trade restrictions based on foreign labor standards because labor costs are a much higher percentage of industry's total costs than are data privacy protection costs.

373. Trade restrictions imposed on the grounds of foreign labor practices, on the other hand, are less defendable under WTO trade rules. While the exploitation of personal data abroad affects the privacy interests of EU residents, foreign labor practices only directly affect the rights of foreign residents. In WTO-GATT trade terms, labor regulations constitute "non-product related production processes." *See supra* note 229. WTO rules treat less favorably trade restrictions based on non-product related production processes because they can be used to coerce foreign countries to change regulatory practices on competitiveness grounds in a context where the health and safety of domestic residents are not directly at issue. Product characteristics, on the other hand, directly affect the residents of the regulating country. For example, pesticide residue on an imported apple directly affects the health of an importing country's residents. Lax foreign data protection practices similarly directly prejudice EU residents' privacy interests. While these product-related standards can also be imposed for coercive or protectionist reasons, panels are more deferential because of the difficult balancing of the interests at issue. *See supra* Part IV.

of its data privacy laws but, rather, constrain the ability of the United States to retaliate against such application.

In a globalizing economy where businesses wish to freely transfer information across borders, domestic regulatory policies over data privacy are increasingly interdependent. Companies' multinational operations are subject to potentially conflicting regulatory requirements unless domestic regulatory requirements are harmonized. Through pooling their sovereignty and acting collectively, EU Member States have increased their influence in shaping the contours of data privacy policies throughout the world. The EU Directive has already helped incite other countries to adopt data privacy protection regulations,[374] again affecting U.S. businesses trading, investing, or otherwise transacting in those countries. Countries are also initiating discussions toward the forging of international data privacy standards under the auspices of the International Organization for Standardization (ISO).[375] Whether the harmonization be de jure (through government regulation) or de facto (through private business practice and "self-regulation"), foreign businesses and officials are being pressed to require and provide greater data privacy protection. This only intensifies the pressure on U.S. businesses and officials.

The nexus between data privacy protection and trade and investment liberalization is full of ironies. In this information-rich world, each time we consume, information about us is consumed. On the one hand, liberalized trade and investment bring us a greater variety of goods and services at lower prices. On the other hand, on account of a complex set of interactions made possible by trade and investment liberalizations, we may also import foreign regulatory policies, including policies mandating how information about us is consumed. In the case of data privacy protection, the adoption of these foreign policies could result in higher prices of the very goods and services liberalization was meant to lower. These higher prices, however, pay for the increased data privacy protection individuals receive.

For privacy advocates, globalization is both an opportunity and a threat. It is a threat because, on account of technological advances, information about us can be more easily compiled and diffused throughout the world to jurisdictions with lower data privacy standards, and then made available

374. *See, e.g.*, Colin J. Bennett, *Convergence Revisited: Toward a Global Policy for the Protection of Personal Data?*, *in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 99, 100–120 (Philip Agre & Marc Rotenberg eds., 1997) (noting the impact of the EU Directive on developments in Eastern Europe, New Zealand, Hong Kong, Quebec, and Canada, leading to what he refers to as growing U.S. isolation and "exceptionalism," and concluding that, while there are "limits to the evaluation of policy success . . . the EU Directive will not only be an instrument for harmonization within Europe; it will have a more coercive effect on countries outside"); Fred Chilton et al., *1996 Computer and Telecommunications Law Update New Developments: Asia-Pacific*, 15 J. MARSHALL J. COMPUTER & INFO. L. 99 (1996) (concluding that the EU Directive puts pressure on Pacific Rim nations to adopt privacy regulations, including controls on the export of personal data); *see also supra* Subsection V.C.3 (listing comments of U.S. business representatives).

375. Discussion has already begun under ISO auspices about the possibility of an ISO privacy standard. *See* Bennett, *supra* note 374, at 123; *see also* Peter Chapman, *Commission Raises Prospect of EU Data Protection Norm*, EUR. VOICE, June 17–23, 1999 (referring to calls for "the EU standards body CEN to examine the scope for creating a Union data protection norm" and "for the International Standardisation Organization (ISO) to develop a world norm for data protection").

locally (including via the Internet) to those prying into our habits and homes. It is an opportunity because foreign laws can be used as leverage to force domestic regulators and businesses to raise privacy standards at home, wherever that home may be. How far U.S. businesses will go in implementing fair information practices remains an open question. Yet the EU Directive has helped push them further than they would have otherwise gone.