GLOBALIZATION AND SOCIAL PROTECTION: THE IMPACT OF EU AND INTERNATIONAL RULES IN THE RATCHETING UP OF U.S. DATA PRIVACY STANDARDS[*]

The final version was published in *Yale Journal of International Law*, vol. 25, 1-88 (Winter 2000)

Abstract: Contemporary critiques of globalization processes often focus on the potential leveling of regulatory standards and the export by the United States of neoliberal norms of deregulation and market facilitation. This article, in contrast, examines the extra-jurisdictional impact of EU data protection policy on the behavior of private parties in the United States, leading to a ratcheting up of U.S. privacy standards. The article takes a socio-legal approach, exploring the many ways in which the EU Directive on the Processing of Personal Data affects U.S. practice through changing the stakes of U.S. players-- including regulators, businesses, privacy advocates, lawyers and privacy service providers-- and thereby changing the playing field in the United States on which competing interest groups clash. In examining the interaction of EU law, U.S. practice and international trade rules, the article finds that WTO law, rather than constraining the Directive's extra-jurisdictional impacts, provides the EU with a shield against U.S. retaliatory threats, thereby further facilitating a trading up of data privacy standards. The article concludes by examining the conditions under which cross-border exchange can lead to a leveraging up of social protections such as data privacy standards. These include, the desire for firms to expand their markets, subjecting themselves to foreign regulatory policy; European states' ability to enhance their bargaining power by acting collectively, using the large EU market as leverage to change foreign standards; the nature of data privacy protection as a luxury good demanded by residents of relatively wealthy, more powerful jurisdictions; the externalities of U.S. under-regulation of privacy protection, legitimizing EU intervention; and the constraints of WTO supranational trade rules on U.S. unilateral retaliatory threats. While the article focuses on the issue of data privacy, its analysis applies to broad areas of law affected by economic globalization.

---

[*] By Gregory Shaffer, Assistant Professor of Law, University of Wisconsin Law School.

GLOBALIZATION AND SOCIAL PROTECTION: THE IMPACT OF EU AND INTERNATIONAL RULES IN THE RATCHETING UP OF U.S. DATA PRIVACY STANDARDS[**]

[**] By Gregory Shaffer, Assistant Professor of Law, University of Wisconsin Law School.

1. Business Organization, Protest and Development of Codes
2. Caught in a Bind: Business' Support and Wariness of Commerce's Privacy Approach
3. Privacy Protection Exported: Spill-over Effects of U.S.-EU Negotiations on U.S. Business Practice
4. The Impact of EU Regulation in other Countries: Increasing Foreign Pressure on U.S. Actors

VI. Conclusion: Trading Up-- The Factors Which Facilitate Raising U.S. Data Privacy Standards

GLOBALIZATION AND SOCIAL PROTECTION: THE IMPACT OF EU AND INTERNATIONAL RULES IN THE RATCHETING UP OF U.S. PRIVACY STANDARDS

Gregory Shaffer[1]

The final version was published in *Yale Journal of International Law*, vol. 25, 1-88 (Winter 2000)

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? 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.[2] How may we review and control its use when technological advances permit rapid, low-cost compilation, storage and transfer of personal data?

Much of the compiling and transfer of personal information which is a daily occurrence in the United States is illegal in Europe. On October 24, 1998, 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 [hereinafter Directive][3] became effective. The Directive mandates significant

---

[1]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 go 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.

[2] 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 residents' whereabouts and other personal minutiae."). Given advances in technology since the publication of Rothfeder's book in 1992, the frequency of transfer of personal information is likely much greater. 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) [hereinafter REGAN, LEGISLATING PRIVACY].

[3] See Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 1 [hereinafter Directive]. Although the Directive was adopted and published in the Official Journal of the European Community on October 24, 1995, pursuant to Article 32.1 of the Directive, it did not become effective until "a period of three years from the date of its adoption"--that is, on October 24, 1998. See id.

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

regulatory controls over business processing and use of personal data. The 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.[4] The United States has taken an ad hoc patchwork approach to data privacy protection which, under the Directive's criteria, does not appear

---

integrated. Originally, the term used was the European Economic Community (EEC), formed pursuant to the 1957 Treaty Establishing the European Economic Community. The Treaty of European Union (TEU) of 1992 changed the name of the EEC to the EC (or 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 block. The first pillar concerned all traditional EC matters, as expanded by the TEU to cover, in particular, European economic and monetary union. 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 which encompasses all three pillars is the European Union (or EU). Technically, the Directive was enacted by the EC institutions governed under the first pillar. The broader terms EU and European Union, however, are most often used by Community authorities and news commentators, and are thus used in this article.

[4] Article 25 of the 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.

Directive, supra note ___, art. 25.

to be "adequate."[5] U.S. governmental representatives have reacted vehemently to the prospects of a European ban on data transfers to the U.S.

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 constrains domestic U.S. 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 business. In order to avoid EU data transfer restrictions, U.S. businesses implement new internal data privacy practices, with an eye on the EU's criteria. Through the publicity given to the Directive, U.S. privacy advocates press for more stringent business internal practices and further U.S. legislation. Privacy advocates' efforts 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 U.S. 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 ("EU") over the regulation of data privacy protection from the perspectives of transnational regulatory conflict and interdependence.[8] It assesses the impact of this conflict and interdependence

---

[5] See Parts III.C and V.C. concerning U.S.-EU negotiations over the adequacy of U.S. privacy protections.

[6] Increased cross-border activity spawns jurisdictional overlaps. As information technologies multiply, computing power and use expand, cross-border mergers, acquisitions, joint ventures and investments increase and companies generally expand their markets beyond national borders, cross-border flows of data concerning employees, clients, adversaries and others 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, Extraterritoriality and Multiterritoriality in Copyright Infringement, 37 VA J. INT'L L. 587, 590 (1997); 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, 156-159 (1997); Allan Stein, The Unexceptional Problem of Jurisdiction in Cyberspace, 32 INT'L LAW. 1167 (1998). For a Canadian perspective, 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." A. GIDDENS, THE CONSEQUENCES OF MODERNITY 64 (1990). For a recent analysis of the phenomena of "globalization," see DAVID HELD & ANTHONY MCGREW, DAVID GOLDBLATT & JONATHAN PERRATON, 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." See id. at 17.

[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,

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 upwards, 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

---

see INTERNATIONAL REGULATORY COMPETITION AND COORDINATION (William Bratton et al. eds., 1996); Anne-Marie Slaughter, The Real New World Order, FOREIGN AFF., Sept./Oct. 1997, at 183 -197; see also ABRAM AND ANTONIA CHAYES, THE NEW SOVEREIGNTY: COMPLIANCE WITH INTERNATIONAL REGULATORY AGREEMENTS (1995). For analysis of the effects of globalization on domestic politics, see INTERNATIONALIZATION AND DOMESTIC POLITICS (Robert Keohane & Helen Milner eds., 1996). For an earlier assessment of the impact of interdependence in international relations literature, see ROBERT KEOHANE AND JOSEPH NYE, POWER AND INTERDEPENDENCE: WORLD POLITICS IN TRANSITION (1977).

[9] See, e.g., DAVID VOGEL, TRADING UP: CONSUMER AND ENVIRONMENTAL REGULATION IN A GLOBAL ECONOMY 5-8 (1995) [hereinafter VOGEL, TRADING UP] (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); 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); and Richard Stewart, Environmental Regulation and International Competitiveness, 102 YALE L.J. 2039 (1993) (setting forth, among other matters, rationales for international harmonization of standards).

[10] See, e.g., 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); Katherine 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); Brian Langille, General Reflections on the Relationship of Trade and Labor (Or: Fair Trade is Free Trade's Destiny, in Jagdish Bhagwati & Robert Hudec, FAIR TRADE AND HARMONIZATION: PREREQUISITES FOR FREE TRADE? 231 (1996).

[11] See e.g. Donald King, Globalization Thinking: Commercial and Consumer Law Illustrations, 39 ST. LOUIS U. L.J. 865 (1995) (given at the VII International Conference of the International Academy of Commercial and Consumer Law) (examining different levels of policy determination in reaction to global processes).

[12] See, e.g., 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

article explores the intricacies of how external pressures affect the stakes of local actors, who in turn incite changes in domestic policy and practice. It presents how foreign and domestic policies are increasingly enmeshed, so that the traditional distinctions of domestic and foreign in the United States, and internal and external in the European Union, are misleading.[16] The 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 EU relies more on state regulation. In a globalizing economy, however, the actions of these institutions have impacts beyond national borders. U.S. under-regulation can jeopardize the privacy interests of EU residents. EU over-regulation can limit 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 vise-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

---

Pharmaceutical Industry, 72 TUL. L. REV. 1597 (1998) (discussing the role of transatlantic experts in reforming domestic regulations).

[13] See, e.g., David 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 polixy).

[14] See e.g. Christopher Mailades, Financial Information, 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, e.g., Stephen Choi, National Laws, International Money: Regulation in a Global Capital Market, 65 Fordham L. Rev. 1855 (1997) (suggesting possible ways to bring about a 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 (1997) (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 JAMES N. ROSENAU & ERNST-OTTO CZEMPIEL, GOVERNANCE WITHOUT GOVERNMENT: ORDER AND CHANGE IN WORLD POLITICS (1992); GLOBAL GOVERNANCE: DRAWING INSIGHTS FROM THE ENVIRONMENTAL EXPERIENCE (Oran R. Young ed., 1997). 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 calls the "law-in-action." For an introduction to "law and society" scholarship, see LAW & SOCIETY: READINGS ON THE SOCIAL STUDY OF LAW (Stuart Macaulay, Lawrence Freidman, John Stokey, eds) (1995). See also, Stuart Macaulay, Law and the Behavioral Sciences: Is There and There There? 6 LAW & POLICY 149 (1984) (noting some of the achievements of law and society scholarship and responding to critiques from critical legal studies scholars).

[17] See in particular Parts II.E and V.

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"). Foreign market power provides leverage for influencing regulatory policies and private practices in other countries. This article examines the role of market power both in intra-European negotiations over data privacy protection (Part IA) and U.S.-EU negotiations (Part IIIA).

- Third, the U.S.-EU dispute demonstrates that individual European countries, in transferring authority to EU institutions, enhance their autonomy and influence vis-a-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 EU.[19]

- Fourth, globalization critics often declaim 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

---

[18] See e.g. Malcolm Waters, Globalization 16 (1995) (stating, "The most imitated society becomes easy to specify: United States society.").

[19] See in particular Part III.A. To provide another example, by joining the World Trade Organization, smaller states may benefit from WTO rules to constrain the United States' 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) ("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." See Paul Krugman and 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 is 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 exploited by third parties. Silicon Valley, California is viewed as a location where firms and individuals generate many positive externalities. The producers of carbon gasses leading to global warming generate negative externalities to the extent that they are not taxed for that pollution and those taxes do not compensate affected third parties.

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 broadly affect national life styles (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-a-vis the demand for other goods as income levels rise.[22]

- Fifth, contrary to common perceptions, international trade liberalization rules appear not to significantly constrain 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 EU, 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 EU with a shield against U.S. threats to retaliate against the Directive's application, thereby further facilitating the Directive's extra-jurisdictional impact.

***

Parts I and II of this article introduce the U.S. and EU approaches to data privacy protection,

---

[21] See in particular 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 which 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." Vogel's book focuses on the effects of trade liberalization on environmental protection, which, in his view, exemplifies the California effect. See DAVID VOGEL, TRADING UP, supra note__, at 5-8. The analysis in Vogel's book, however, focuses on the role of large exporting firms who, once they adapt to higher foreign standards to sell and operate in a foreign market, support the raising of domestic standards because they now have a competitive advantage over local firms. This is not the case in the U.S.-EU dispute over data privacy. Rather, as depicted in Part V, 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 and that pressure's impact on political and regulatory processes and business practices in the United States.

[22] As used in this article, the term luxury goods refers to those goods whose demand increases proportionately greater than the demand for other goods when individual income increases. See JAMES GWARTNEY AND 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. at 457. 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 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. Id. at 457. This factor is further explored in Part VI.

[23] See in particular Part IV. The WTO refers to the World Trade Organization, the international organization based in Geneva, Switzerland which oversees "the common institutional framework for the conduct of trade relations among its members." See Article II of the Uruguay Round Agreement Establishing the WTO.

the U.S. purportedly focusing more on market regulation and the EU on government regulation. Part I introduces the Directive's regulatory approach to data privacy protection. It first examines the 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 upwards of European data privacy requirements. It then considers the additional costs imposed on businesses and consumers resulting from these requirements, which help explain U.S. businesses' confrontational response to the Directive. It concludes by presenting the 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, both as regards acts of government and the private sector and the problematics of the 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 which potentially constrain EU and U.S. actions. Part III examines the multiple means available under the Directive for the EU to restrict data transfers to the United States, and the on-going 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 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 EU in applying the 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 which permit regulatory requirements to be leveraged upwards 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 which 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, the section assesses the benefits and detriments of allocating decision-making authority to alternative institutional processes-- be it 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 KOMESAR, IMPERFECT ALTERNATIVES: CHOOSING INSTITUTIONS IN LAW, ECONOMICS, AND PUBLIC POLICY 3 (1994).

I. EU Data Privacy Rules and their Impact on Business

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

A. Trading Up in the EU: 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 EU from the threat of unilateral bans by individual EU member states[26] on account of their differing data privacy protection regimes. The EU, as a block, 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 Directive concurrently removed the threat to unhindered data flows between member states. As reflected in the 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:

> (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

---

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

[26] Member states is the term used to refer to the fifteen countries which 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 Cate, The EU Data Protection Directive, Information Privacy, and the Public Interest, 80 IOWA L. REV. 431, 438 (1995) (citing Deliberation no. 89-78 du 11 juillet 1989, reprinted in Commission nationale de l'informatique et des libertes, 10e Rapport au president de la Republique et au Parlement 1989, at 32-34 (1990) [hereinafter CNIL Rapport] (discussing the Italian transfer), and Deliberation 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 (March 1995) (citing Hessicher Datenschutzbeauftragter, 18 Tatigkeitsbericht 27-28, 43-45 (1989)).

[28] See Nick Platten, Background to the History of the Directive, in DAVID BAINBRIDGE, EC DATA PROTECTION DIRECTIVE 13, 23 (1996).

> 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...(emphasis added).

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 separate goals of protecting individual privacy, on the one hand, while ensuring trade liberalization within the European Union, on the other hand, were inseparable.[29] The link, however, was not because data protection and free data flows naturally go hand in hand.[30] Rather, they were inseparable for political reasons. While the EU could have mandated that no individual member state block data transfers regardless of the extent of privacy protection in any other member state, from a practical standpoint, this was inconceivable. 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

---

[29] The link between market regulation and higher social protection standards in Europe is not limited to data privacy protection. Article 100(a)(3) 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 or protection." TREATY ESTABLISHING THE EUROPEAN COMMUNITY, Feb. 7, 1992, O.J. (C 224) 1 (1992), art. 100(a)(3). As Christian Joerges states, the upward harmonization requirement under Article 100(a)(3) "has in fact been achieved." See Christian Joerges, The EC Regulatory Process: Bureaucratic Nightmare, Technocratic Regime and Dream of Good Transnational Governance, in Christian Joerges and Ellen Vos, eds. EU Committees: Social Regulation, Law and Politics 5 (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 and James Caparosa, From Free Trade to Supranational Polity: The European Court and Integration, in EUROPEAN INTEGRATION AND SUPRANATIONAL GOVERNANCE 92-132 (Wayne Sandholtz & Alec Stone Sweet eds., 1998).

[30] The natural connection between free data flows and data privacy protection is sometimes maintained by privacy advocates. Marc Rotenberg of EPIC affirmatively cites the statement by an early leading European advocate of data privacy protection, Jan Freese, who proclaimed "Privacy protection is necessary to ensure the free flow of information." (Rotenberg comments to an earlier draft of this article). 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 Sykes, The (Limited) Role of Regulatory Harmonization in International Goods and Services Markets, 2 J. OF INT'L. L. 49-70 (1999) (noting, however, that cooperation is necessary where production results in cross-border impacts).

information across the border to Italy which did not enforce similar controls. EU member states' institutional approaches to data privacy protection were thus interdependent.

Second, and most importantly, the most powerful states in the EU (Germany and France) demanded greater data privacy protection throughout the EU.[31] 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 which permitted the Directive to go forward. It was France and Germany's political exploitation of market power that enabled protection to be traded up throughout the EU.[32]

As a result, the Directive has twin "Objects," which are set forth in its first article. Paragraph 1 of Article I 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." 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."[33] Only by ensuring the protection of "fundamental" privacy rights throughout the EU could the EU ensure the "free" transferability of data.

---

[31] The background to 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 PHILIP AGRE AND MARC ROTENBERG, TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE, 219-242 (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). GLIC is funded by the Open Society Institute, a foundation created by the financier George Soros.

[32] Albert Hirschman has noted that the essence of economic power is the capacity to obstruct commercial exchange. A state's large market provides it with leverage on 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... 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."

See HIRSCHMAN, NATIONAL POWER AND THE STRUCTURE OF FOREIGN TRADE 16-17 (1945). Because Germany and France had important markets, their threat to cut off data flows to smaller states mattered. 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 EU, see TRADING UP, supra note ___, at 24-97.

[33] See Directive, supra note ___, art. 1.

B. Rights and Obligations: The Directive's Regulatory Controls over Data Processing. The EU, through its Directive, takes more of a legislative approach to data privacy protection than the United States, which relies more on private ordering through market processes.[34] The Directive is noteworthy for its broad scope of coverage of private sector activities and its creation of ex ante and ex poste controls over business processing and use of personal data. This Section provides an overview of the Directive's significant protections.

The Directive's first striking feature is that, except for public security, criminal law and related exceptions,[35] it covers all processing of all personal data by whatever means, and is not limited by business sector or field of use.[36] While U.S. regulation of data processing by the private sector is limited to specific sectors and limited categories of information, the Directive covers all private sector processing of personal data.[37]

Second, the Directive imposes ex ante controls on data "controllers,"[38] setting forth what enterprises must do before they process data. The 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.[39] The data can only be processed and used for the purposes specified, so that enterprises

---

[34] For the U.S. approach see infra notes __ and accompanying text.

[35] The 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." It also does not cover processing operations for "purely personal or household activity." See Directive, supra note ___, art. 3(2). EU member states considered that public security and criminal law matters remain within the sole competence of the member states. See Directive, supra note ___, recital 13, as well as discussion in Simitis, From the Market to the Polis, supra note__, at 453-54. An excellent overview of EU law is provided in JOSEPHINE SHAW, LAW OF THE EUROPEAN UNION (1996).

[36] 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." See Directive, supra note ___, art. 2.

[37] As regards the U.S., see infra Part II.B, notes___ and accompanying text. As regards EU regulation of private sector use of data, as Smitis 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, From the Market to the Polis, supra note__, at 452.

[38] 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." See Directive, supra note ___, art. 2(d).

[39] Directive, supra note ___, 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

are prohibited from even collecting information unnecessary for these purposes.[40]

Some controls, however, are subject to exceptions, providing flexibility for many business operations, more flexibility than many privacy advocates would like.[41] For example, the Directive prohibits data controllers from processing information unless the "data subject" "unambiguously"[42] consents to the processing. 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.[43]

DIRECTIVE 95/46/EC 40 (1998). This document is available on the Web site of EU Directorate General XV, which is responsible for overseeing implementation of the Directive. See <http://europa.eu.int/comm/dg15/en/media/dataprot/studies/masons.htm europa.eu.int/comm/en/media/datapost> (visited March 30, 1999). This obligation, however, no longer applies "where [the data subject] already has [such information]." This implies that the data subject only needs to be provided such information once, and not each time information is collected from him.

[40] See Directive, supra note ___, 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." This is sometimes referred to as the "finality" principle.

[41] See Spiros Simitis, From the Market to the Polis: The EU Directive on the Protection of Personal Data, supra note__, at 457. Not surprisingly, affected businesses engaged in considerable lobbying in an attempt to make the Directive more flexible. See Platten in Bainbridge, supra note __ at 27-28.

[42] There is some ambiguity in the EU Directive's reference 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." See Directive, supra note ___, art. 2(h). According to the EU Working Party formed pursuant to Article 30 of the Directive, "because 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." See 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 by the Working Party on 24 July 1998, at 24 [hereinafter Transfers of personal data to third countries]. In practice, except for "sensitive information as specified in Article 8 of the Directive (see below), 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) (Blackmer represents major companies in the United States and EU on data privacy issues. The interview concerned, among other matters, company practice in light of the Directive) [hereinafter Blackmer March 27 Interview].

[43] The 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

Nonetheless, the 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."[44] 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.[45] 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 by (positively) checking a box indicating his or her agreement. 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."[46] The Directive also grants individuals 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)." See Directive, supra note ___, 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 Directive, supra note__. Blackmer March 27 Interview, supra note__. 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 where one of the conditions in (b) and (f) does not apply." Bainbridge, supra note __ at 54. Even Bainbridge, however, subsequently states that "the 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." Id. at 159. 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 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 protection of the data subject or of the rights and freedoms of others. See Directive, supra note ___, art 13(1). For a discussion of these exceptions, see Spiros Simitis, From the Market to the Polis: The EU Directive on the Protection of Personal Data, supra note__, at 457.

[44] See Directive, supra note ___, 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 ___, at 7.

[45] See Directive, supra note __, art 10(c). Bainbridge, however, argues that it may be sufficient to simply raise awareness among consumers of their right to apply to have their names removed from mailing lists under a "mailing preference scheme." Bainbridge, supra note __, at 66, 148-49.

[46] Article 8(1) provides, "[m]ember States shall prohibit the processing of personal information revealing racial or ethnic origin, political exceptions, religious or philosophical beliefs, trade union membership, and the processing of data concerning health or sex life." See Directive, supra note ___, 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)(a), which provides, "[p]aragraph 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

right to challenge any decision significantly affecting him or her that is based on an automatic processing of data, including in respect of his or her creditworthiness or employment.[47]

Third, the Directive imposes ex poste controls on enterprises, granting individuals rights to monitor and challenge the use of personal information after it is processed.[48] The 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.[49] 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 Directive grants individuals significant enforcement rights.[50] The Directive requires member states to provide a judicial remedy for infringements of data privacy rights, including the right to receive damages.[51] Individuals can also challenge the data's accuracy and collection procedures and block its further processing and transfer.[52] To support effective enforcement, member states must designate an independent public authority "responsible for monitoring the application within its territory" of the Directive's provisions.[53] 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

---

by the data subject's giving his consent." See Directive, supra note__, art 8 (emphasis added). The term "explicit" consent is understood to require that an individual must clearly grant consent by "opting in" to the scheme. Blackmer March 27 Interview, supra note ___.

[47] 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, etc." See Directive, supra note__, art. 15(1).

[48] There are also provisions protecting the "confidentiality of processing" and the "security of processing." See Directive, supra note ___, arts. 16-17.

[49] See Directive, supra note ___, 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 disincentive" for individuals to seek access. Bainbridge, supra note __, at 78.

[50] Enforcement of the Directive will inevitably determine how effective it will be in practice in accomplishing its goals. There is evidence of enforcement under prior member state laws. See Part 1.A, supra note__. Part V.B supra notes__ and accompanying text points out additional ways in which the Directive may be implemented.

[51] See Directive, supra note ___, art. 22-23.

[52] See Directive, supra note __, art. 12.

[53] Directive, supra note ___, art. 28.

legal proceedings" against violators of the rights guaranteed by the Directive.[54] 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 outcome.[55] Sanctions may, depending on member state law, include civil and criminal fines and imprisonment.[56]

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 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 Directive threatens not only U.S. sovereignty; more fundamentally, it constrains the sovereignty of private business decision-making.

First, the 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-- time which could otherwise be used to commercially exploit the data. 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. The BBA estimated that, in aggregate, the provision of such information to customers will cost each bank "millions" of pounds.[57] The Commission, on the other hand, appointed independent consultants to conduct a detailed cost-benefit study, which concluded

---

[54] Id. In addition, the controller must notify the national supervisory authority before carrying out 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. See Directive, supra note ___, art. 18. The minimal 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 Directive, supra note ___, 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." Directive, supra note ___, 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 Directive, supra note ___, art. 21.

[55] See Directive, supra note ___, art. 28(4).

[56] The nature of the sanctions will be defined by national law. The Directive merely requires member states to impose sanctions in case of infringement of the national provisions implementing the Directive. See Directive, supra note ___, art. 24.

[57] The BBA calculated that the cost of providing one client with "a simple and straightforward report" containing the information required by the Directive to be "in excess of 150 pounds." See FRED CATE, PRIVACY IN THE INFORMATION AGE 42 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 (Electronic Privacy Information Center), the non-profit advocacy group based in Washington D.C., counters that credit reports mandated by the Federal Credit Reporting Act are available in the United States for US $8 (comments to author on earlier draft).

that the financial impact would be minimal.[58]

Second, where informed consent is required, individuals may refuse to grant it. If most consumers refuse to grant consent, in theory, they could 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 to producers, but most might refrain because of a low but potentially catastrophic risk to a few.[59]

Third, where individuals withhold consent, businesses seek to obtain information through more costly means.[60] 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.[61] Privacy protection can also reduce enterprises' ability to make quick, informed contracting decisions, such as whether to grant customers credit. The Directive not only increases businesses' transaction costs to obtain information; it also reduces businesses' productivity when they fail to obtain it, resulting in

---

[58] See Pearce & Platten, Data Privacy in EU, supra note ___, at 537, and Bainbridge, supra note __ (Preface). 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 consenting individuals.

[59] 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 ___ and accompanying text. Second, to the extent 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 other than catastrophic risks, such as impaired reputation, job dismissal or rejection of insurance coverage. Many individuals object to the nuisance of being bombarded with unrequested marketing information, whether by phone or mail.

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

[61] 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 of 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, one's personal 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 powerful business interests well-positioned to do so.

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.[62] The U.S. direct marketing industry reportedly grew by 7% in 1998 and expects to maintain a 7% annual growth through 2002.[63] The EU direct marketing industry and its growth prospects are minute in comparison.[64]

To some commentators, the EU Directive views privacy as a "fundamental right and freedom"[65] which 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

---

[62] 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. The Direct Marketing Association 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 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 Internet Direct Marketing, supra. See also the DMA study Economic Impact: U.S. Direct Marketing Today, 1998 Update (on file), maintaining that, in 1998, 24.6 million workers were "employed throughout the U.S. economy as a result of direct marketing activities." Id., at 11.

[63] See Direct Hit, ECONOMIST, Jan. 9, 1999, at 55 (noting "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.

[64] While other factors, including cultural influences and other relevant legislation such as the EC Distant Selling Directive, may contribute to the discrepancy, data privacy protection regulations surely hamper direct marketing activities in Europe. See, e.g., Directive 97/7/EC of the European Parliament of 20 May 1997on the Protection of Consumers in Respect of Distance Contracts 1997 O.J. (L 144) 19 (known as the "EC Distant Selling Directive"). Although the implementation date for member states is June 4, 2000, relevant member state legislation already exists. For an overview of relevant EC consumer legislation, see STEPHEN WEATHERHILL, EC CONSUMER LAW AND POLICY (1997).

[65] See Directive, supra note ___, 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 REGULATORY PRIVACY, supra note__, at 22-37. See also Regan, Legislating Privacy, supra note__, at 24-42, 212-243 (critiquing purely individualistic grounds for protecting privacy and offering complementary collective social grounds).

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."[66] (emphasis added).

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,[67] and other matters for legislatures, regulators, courts and markets to take into account. 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 decisions on stereotypes, prejudicing those from a particular race or ethnic group.[68]

In practice, the Directive balances other concerns against privacy interests. The Directive creates exceptions for concerns such as "public security, State security... and the activity of the State in areas or criminal law."[69] The Directive also provides for "exceptions or derogations" for "processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression . . . ,"[70] as well as a limited exception for scientific research.[71] Privacy rights advocates nonetheless tend to employ a fundamental rights discourse to attempt to enhance the relative importance of their concerns vis-a-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.

---

[66] Unpublished address by Spiros Simitis on Information Privacy and the Public Interest (October 6, 1994), quoted in PRIVACY IN THE INFORMATION AGE, supra note ___, at 42.

[67] 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 which 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 (April 4, 1999) § 4, at 3.

[68] The Directive places specific limits on "the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs..." See Directive, supra note__, 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 ___.

[69] Directive, supra note__, art. 3(2).

[70] Directive, supra note__, art. 9.

[71] See Directive, supra note__, art. 13(2).

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, on average, are, in principle, higher than they would be without the EU's 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 mitigates these equity and efficiency concerns. Consumers more likely grant consent when they are compensated for information, making it more readily available. In return, consumers receive a greater share of the benefits from information processing, making it more equitable. The pricing of personal information can also increase economic efficiency by causing businesses to internalize privacy costs in the price of goods sold.[72]

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,[73] to prohibit all data transfers to a third

---

[72] If paid for their personal information, consumers more likely 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 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.*, 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, which 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); *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).

[73] The decision-making processes are set forth in Article 31 of the Directive, which in turn refers to decisions by a qualified majority vote (QMV) of member state representatives pursuant to the Treaty Establishing the European Community (as amended). 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 (formerly Article 148 at the time of the 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. Sixty-one out of a total of eighty-seven votes are required to pass an act by QMV following a Commission proposal. Article 31 provides, in relevant part:

> "The Committee
>
> 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:

country, including the United States, if it finds that it does not ensure "an adequate level of protection" of data privacy rights.[74] The meaning of the term "adequate" is not defined in the Directive, but is to be determined on a case-by-case basis. Pursuant to the Directive, the EU 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.[75] The Working Party, comprised

---

- 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."

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 which 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.

[74] Article 25 is quoted in full in supra note__. The United States is not specifically cited in the Directive. However, given the size of the U.S. market, the widespread use of data in the U.S., the lack of comprehensive data privacy legislation in the U.S., and the fact that the U.S. is the EU's largest trading partner, the EU first entered into negotiations with the U.S. over data privacy protection standards and these negotiations have been by far the most intensive. The EU is nonetheless also in discussions with other countries, and in particular Japan. 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, Belgium (June 23, 1999).

[75] The Working Party was formed pursuant to Article 29 of the Directive. The duties of the Working Party are spelled out in Article 30, which provides

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 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.
2. If the Working Party finds that divergences likely to affect the equivalence of protection for persons with regard to the processing of personal data in the Community are arising between the laws or practices of Member States, it shall inform the Commission accordingly.
3. The Working Party may, on its own initiative, make recommendations on all matters relating to the protection of persons with regard to the processing of personal data in the Community.
4. The Working Party's opinions and recommendations shall be forwarded to the Commission and to the committee referred to in Article 31.
5. The Commission shall inform the Working Party of the action it has taken in response to its opinions and recommendations. It shall do so in a report which shall also be forwarded to the European Parliament and the Council. The report shall be made public.
6. The Working Party shall draw up an annual report on the situation regarding the protection of natural persons with regard to the processing of personal data in the Community and in third countries, which it shall transmit to the Commission, the European Parliament and the Council. The report shall be made public.

Directive, supra note ___, art. 30.

of data protection commissioners from each EU member state and members of the Commission, prepared a Discussion Document,[76] 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's 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 effectively enforce the protections; the third county data recipient must be prohibited from transferring the information to other countries that, in turn, do not afford "adequate" levels of protection.[77] 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.[78]

II. U.S. Data Privacy Protection: Does it Fail to Meet the Directive's Criteria?

Unlike the broad scope of coverage and 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.[79]

---

[76] Since the 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 Directive relevant to third country transfers. In July 1998, it incorporated these in its Working Document entitled Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive, XV D/5025/98, adopted on July 24, 1998 [hereinafter Transfers of personal data to third countries]. The earlier documents were entitled Discussion Document: First Orientations on Transfers of Personal Data to Third Countries- Possible Ways Forward in Assessing Adequacy, adopted by the Working Party on 26 June 1997 [hereinafter First Orientations on Transfers of Personal Data to Third Countries]; Working document: Judging industry self-regulation: when does it make a meaningful contribution to the level of data protection in a third country?, adopted by the Working Party on 14 January 1998; and Working Document: Preliminary views on the use of contractual provisions in the context of transfers of personal data to third countries, adopted by the Working Party on 22 April 1998.

[77] See Transfers of personal data to third countries, supra note ___ at 6; see also First Orientations on Transfers of Personal Data to Third Countries, supra note ___, at 6.

[78] See First Orientations on Transfers of Personal Data to Third Countries, supra note ___, at 3. See also Al Gidari and Marie Aglion, EU Directive on Privacy May hinder E-Commerce, NAT'L L.J., June 29, 1998, at B7 (referring to "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 supra note ___.

[79] 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) [hereinafter FREER MARKETS, MORE RULES]; see also Peter Katzenstein, International Relations and Domestic Structures: Foreign Economic Policies of Advanced Industrial States, in INTERNATIONAL ORGANIZATION, 1, 14 (1976) (noting the United States is "a country marked by a strong society and a weak state"). As one New York Times correspondent states, the United States' 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, October 26, 1998 (Business Technology Section).

To a certain extent, the United States' handling of data privacy issues reflects Americans' traditional distrust of a centralized government.[80] U.S. 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 section begins with an overview of U.S. legal protection against data processing by government (Part A) and by the private sector (Part B), noting the problematics of this public-private distinction (Part 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 (Part D). It concludes by examining the need for comparative institutional analysis to take account of extra-jurisdictional impacts on the operation of national institutions (Part E).

A. U.S. Protections against Data Processing by Government. The Privacy Act of 1974 is the only federal omnibus act which protects informational privacy.[81] 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.[82] The Privacy Act also requires federal agencies

---

[80] 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." See Bob Kagan, Introduction to REGULATORY ENCOUNTERS: MULTINATIONAL CORPORATIONS AND AMERICAN ADVERSARIAL LEGALISM 16 (Bob Kagan ed., 1998) (book manuscript on file). Kagan finds that the U.S. "style" of regulation is "more adversarial and legalistic than regulation is in other countries." Id. at ___. See also Kagan, Adversarial Legalism and American Government, in THE NEW POLITICS OF PUBLIC POLICY 88-118 (Marc Landy & Martin Levin eds., 1995). As discussed below, however, whereas the fragmented nature of U.S. data privacy regulation meets with Kagan's analysis, 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." See also Fred Cate, Privacy and Telecommunications, WAKE FOREST L. REV. 1, 34 (1998) (referring to American's "distrust of powerful central government.")..

[81] See 5 U.S.C. § 552a (1994 & Supp. II 1996). In addition, the Freedom of Information Act provides important safeguards to third-party access to federal records. The primary focus of the Freedom of Information Act is its requirement that the federal government provide access to its records to the general public. However, the act contains exceptions to the release of information about private individuals. See 5 U.S.C. § 552.

[82] However, the Privacy Act contains a significant exception in the form of the "routine use exception." Paul Schwartz and Joel Reidenberg critique the "routine use" exception to the 1974 Privacy Act as a loophole which permits almost "any use" of personal data. The exception permits federal agencies to transfer information between themselves for what they justify as a "routine use."See PAUL M. SCHWARTZ AND JOEL R. REIDENBERG, DATA PRIVACY LAW: A STUDY OF UNITED STATES DATA PROTECTION 94-100 (1996) [hereinafter DATA PRIVACY LAW].

to designate a "Privacy Act official" to oversee the agency's compliance with the Act's requirements, as well as "Data Integrity Boards" to review inter-agency data matching activities.[83]

Because of the United States' federal system, the Privacy Act does not apply to the states. The vast majority of states lack omnibus privacy acts,[84] and rather offer scattered statutes applying to specific sectors or concerns, such as the regulation of "access to educational records and child abuse data banks."[85] Except for certain issue-specific legislation which is federally mandated,[86] there is little uniformity of state law, resulting in fifty different jurisdictions with distinct regimes. While provisions of the United States 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.[87]

B. U.S. Protections against Data Processing by the Private Sector. Unlike the EU, 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 Privacy Protection Act of 1994,[88]

---

[83] Commentators, however, find that the oversight practices of the Privacy Act officials and Data Integrity Boards are of limited effectiveness. See DATA PRIVACY LAW, supra note ___, at 120.

[84] In 1996, Schwartz & Reidenberg reported that "only thirteen states have general statutes that establish fair information practices for the government's processing of personal information." See DATA PRIVACY LAW, supra note ___, at 131. These states were Alaska, California, Connecticut, Hawaii, Indiana, Massachusetts, Minnesota, New Hampshire, New York, Ohio, Utah, Virginia and Wisconsin. See id.

[85] See id. at 130.

[86] 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. 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) [hereinafter Privacy and Participation]

[87] 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 first amendment rights to freedom of expression and association, the right to vote, the fourth amendment's protection against unreasonable searches and seizures, and the Supreme Court's recognition of a limited right to informational privacy. The central case on informational privacy is Whalen v Roe. See 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," it applied a lower level of scrutiny of the state law than "strict scrutiny," and thereby found that the New York statute provided adequate protection. See DATA PRIVACY LAW, supra note ___, at 76. Moreover, the Supreme Court has been increasingly protective of "state rights" in recent years.

[88] See 18 U.S.C. § 2721. The Driver's Privacy Protection Act regulates the dissemination of personal information held by Departments of Motor Vehicles.

the Video Privacy Protection Act of 1988,[89] The Electronic Communications Privacy Act of 1986,[90] the Cable Communications Policy Act of 1984,[91] and The Fair Credit Reporting Act of 1971.[92] Rather than engage in a concerted effort to protect individual privacy, in most cases, Congress has sometimes simply reacted to public scandals. In passing the Fair Credit Reporting Act, Congress responded "to consumer horror stories of dealings with credit reporting agencies."[93] 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. As a result, in the United States, "video rentals are afforded more federal protection than are medical records."[94]

As a consequence, while U.S. data privacy protection may be adequate under EU standards

---

[89] See 18 U.S.C. § 2710. The Video Privacy Protection Act prohibits the disclosure of film titles rented by specific customers and requires the destruction of personally identifiable information within a year of collection.

[90] See Pub. L. No. 99-508, 100 Stat. 1848 (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

[91] See 47 U.S.C. §551. The Act requires subscribers' cable-TV records to be kept confidential.

[92] See 15 U.S.C. §§ 1681- 1681u. 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.

[93] See NOTHING SACRED: THE POLITICS OF PRIVACY, supra note__, at 14 (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 determinated that the report was fabricated). See also 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 "public outrage" when Judge Bork's "video rental records... were publicized") [hereinafter Setting Standards].

[94] SHERI ALBERT, HASTINGS CENTER, SMART CARDS, SMARTER POLICY: MEDIAL 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 non-existent." Quoted in Bob Herbert, What Privacy Rights, NY TIMES, Sept. 27, 1998, sec 4, at 15. 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 pursuant to the Administrative Procedure Act, 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, NYT (Oct. 30, 1999), at A1, A9 [hereinafter, Rules of Privacy on Patient Data]. The proposed rules are nonetheless critiqued for failing to require patient consent for health plans and insurance companies to use such information. Id., at A9.

in some sectors, it was thought inadequate in most.[95] 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 poste perspective, individuals have no access to processed information and can not 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.[96] 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."[97] The attitude of many U.S. businesses are encapsulated in the remarks of the President of Sun Microsystems, "You already have zero privacy- get over it."[98]

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

---

[95] A sector-by-sector analysis of U.S. data privacy protection is contained in DATA PRIVACY LAW. See DATA PRIVACY LAW, supra note ___. 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 data protection in the telecommunications and credit reporting sectors, in most contexts, is likely to be found adequate under the Directive, while protections of health records and data marketing industries are likely to be found inadequate. See id. See also PETER SWIRE & ROBERT LITAN, NONE OF YOUR BUSINESS, WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE 169-172 (1998) [hereinafter NONE OF YOUR BUSINESS]. 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. In the fall of 1999, however, the Clinton administration proposed new rules on privacy protection of medical data. See Rules of Privacy on Patient Data, supra note__.

[96] Direct marketing companies may compile profiles of an individuals' 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, visa card purchases, warranty applications, and other places. See Setting Standards, supra note ___, at 523.

[97] See id. (citing Claritas advertisement of a profiling product, DM News, May 23, 1994, at 26). Schwartz & 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 United States' "largest mail order pharmacy," was to obtain access to Medco's collection of personal medical data for marketing purposes. See DATA PRIVACY LAW, supra note__ at 168.

[98] Quoted in John Markoff, Growing Compatibility Issue: Computers and User Privacy, N.Y. TIMES, Mar. 3. 1999, at A5.

National Telecommunications and Information Administration.[99] To date, these agencies do not coordinate their data privacy oversight.[100]

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 U.S., even the FBI seeks information for its investigations from private companies.[101] 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 United States' ad hoc approach to data privacy, U.S. regulation of the private sector largely depends on industry norms and individual company policies which 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,[102] these "self-regulatory" schemes remain voluntary, unenforceable, and, it appears, often ignored by the very companies advocating their use.[103] Privacy labeling programs are being created for companies to market their data privacy practices to attract customers, but there is

---

[99] See 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 addressed, ABA BANKING J., Dec. 1, 1997.

[100] However, in March 1999, in large part in reaction to the 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 point of contact on international privacy issues." See Clinton Administration to name Swire as OMB's Privacy Policy Coordinator, 16 Int'l Trade Rep. (BNA) 396 (March 10, 1999). See infra note __ and accompanying text in Part V.A. concerning the Directive's impact.

[101] See Setting Standards, supra note ___, at 536 n.216 (citing Ray Schultz, FBI Said to Seek Compiled Lists for Use in Its Field Investigations, DM NEWS, at 1, (April 20, 1992)).

[102] See infra Part IV.C.

[103] See DATA PRIVACY LAW, supra note ___, 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 Web site each month. These Web sites exhibit a TRUSTe seal in order to build trust among customers. See TRUSTe Web site <http://www.truste.orgabout/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 infra note__. See Comments of Mark Silbergeld on the Department of Commerce, Draft Safe Harbor Principles, <http://www.ita.doc.gov/ecom/com1abc.htm#silbergeld> (visited Jan. 13. 1999). 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.

presently little to no external monitoring of labeling practices.[104] While privacy advocates assert that these "self-regulatory" measures are smoke-screens to impede government regulation, they nonetheless hope to use the Directive's regulatory mechanisms (and U.S.-EU negotiations over their application) to change regulatory policies and market practices in the United States. The timing of the sudden proliferation of self-regulatory schemes suggests that the Directive provides privacy advocates with significant leverage.

C. The Problematics of 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 society; around which crystallize our social problems and to which we look for their solution."[105]

The traditional distinction in the American legal system between the public and the private has long been critiqued.[106] The distinction's basis lies in liberal political theory, according to which individuals need be protected from collective control over their behavior.[107] Critics maintain that private entities' activities need be subject to similar controls-- as government's-- since both can coerce or otherwise significantly influence individual behavior.[108] For example, numerous

---

[104] In the case of TRUSTe, it monitors the very companies which 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).

[105] PETER FERDINAND DRUCKER, THE CONCEPT OF THE CORPORATION 6-7 (1946).

[106] See, e.g., Morton J. Horwitz, The History of the Public/Private Distinction, 130 U. PA. L. REV. 1423-1428 (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, 1354 (1982) (describing a theoretical progression whereby the public/private distinction has blurred such that the characteristics of one side are equally found in the other); GERALD TURKEL, DIVIDING PUBLIC AND PRIVATE: LAW, POLITICS, AND SOCIAL THEORY (1992) (exploring critiques of the distinction by major social theorists).

[107] See, e.g., Horwitz, supra note __, 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 what activities should be protected by a categorization of them as private).

[108] Many of the critics of the public-private distinction are also critics of liberalism itself. See, e.g., R. UNGER, LAW IN MODERN SOCIETY 192-93 (1976) (describing the incoherence of the public-private distinction); CHALLENGING THE PUBLIC/PRIVATE DIVIDE: FEMINISM, LAW, AND PUBLIC POLICY (Susan B. Boyd ed., 1997); Ruth Gavison, Feminism and the Public/Private Distinction, 45 STAN. L. REV. 1, 44-45 (1992) (critiquing the distinction from a feminist

constitutional law scholars critique the Supreme Court's well-entrenched "state action" doctrine, which limits the application of the fourteenth amendment's due process and equal protection requirements to federal governmental actions.[109] 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."[110] 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 their compliance, and the application of sanctions for non-compliance.[111]

---

perspective as perpetuating social power structures). However, strands of liberal theory also supports 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 10-11, 13 (1990) (citing 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," and also referring 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").

[109] 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); Erwin Chemerinsky, Rethinking State Action, 80 NW. U. L. REV. 503 (1985) (surveying the incoherence of the state action doctrine under various theories of rights and justifications of the doctrine); Paul Brest, State Action and Liberal Theory: A Casenote on Flagg Brothers v. Brooks, 130 U. PA. L. REV. 1296 (1982) (analyzing state action doctrine in the context of the Supreme Court's finding of no due process violation when a private company disposed of goods under a warehouseman's lien without any governmental hearing); Charles L. Black, Jr., "State Action," Equal Protection, and California's Proposition 14, 81 HARV. L. REV. 69, 91 (1967) (summarizing numerous critiques about the doctrine's inability to define meaningful categories).

[110] See, e.g., Morris R. Cohen, Property and Sovereignty, 13 CORNELL L.Q. 8 (1927) (arguing that state enforcement of property rights are 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); see also WILLIAM W. FISHER III ET AL., AMERICAN LEGAL REALISM 98-100 (1993) (summarizing the legal realist critique).

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. 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 boundaries between the 'public' and the 'private' sector..., [on account of] efforts to privatize or 'outsource' government functions." Bennett, The EU Directive: The North American Response, available ate www.cous.uvic.ca/poli/bennett/research/plb98.

[111] 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, internal corporate mechanisms for arbitration and protection against industrial espionage).

Private sector proposals for "self-regulation" of data privacy protections are an excellent example of private rule-making, 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." They lobby for legislative intervention providing for state enforcement of privacy rights.

D. Alternative Institutions: The Role of Markets, Legislatures and Courts in the Regulation of Private Sector Use of Personal Data in the United States. 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 U.S. 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.[112] Major U.S. companies have implemented data protection policies in response to negative publicity or to reduce its risk. Pacific Bell and America Online, two huge telecommunications companies, abandoned plans to sell information on their subscribers in response to widespread customer complaints,[113] and developed new company data privacy policies.[114] 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.[115] Equifax reputedly ceased marketing consumer names and

---

[112] 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.

[113] 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, §. 1, at 3, (cited in DATA PRIVACY LAW, supra note ___, at 247).

[114] See Pacific Bell Customer Privacy Guidelines, Privacy & American Business, Sept./Oct. 1993, at 15. See Comments of America Online on the Department of Commerce, Draft Safe Harbor Principles, <http://www.ita.doc.gov/ecom/com4abc.htm> (visited Jan. 13. 1998).

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

addresses altogether, even though it had earned $11 million in revenue from such sales the previous year.[116] Intel likewise reversed its decision to activate an identifying code number in its next generation of computer chips, Pentium III, which would enable companies to gather profiles of individual users of Web sites. It did so just hours after a consumer rights group (the Electronic Privacy Information Center) called for a boycott of the chip.[117] These companies did not react to law suits 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-a-vis competitors. In particular, they can potentially increase electronic sales through marketing their privacy protection policies.[118] Surveys have found that "consumers not using the Internet ranked concerns about the privacy of their personal information and communications as the top reason they have stayed off the Internet."[119] As 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

---

[116] See Shelby Gilje, Credit Bureau Won't Sell Names, SEATTLE TIMES, Aug. 9, 1991, at D6.

[117] 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, When Privacy is More Perilous than the Lack of it, supra note__.

[118]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 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." 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 Bill C-54, The House of Commons of Canada, An Act to support and promote electronic commerce by protecting personal information that is collected, used or disclosed in certain circumstances, by providing for the use of electronic means to communicate or record information or transactions and by amending the Canada Evidence Act, the Statutory Instruments Act and the Statute Revision Act (first reading, Oct. 1, 1998), <http://www.parl.gc.ca/36/1/parlbus/chambus/house/bills/government/C-54/C-54_1/C-54_cover-E.html> (visited April 4, 1999).

[119] See PRIVACY ONLINE, supra note ___, at 3 (citing Business Week/Harris Poll: Online Insecurity, BUS. WK., March 16, 1998, at 102); Alan F. Westin, *Netizens Want Better Privacy Rules and Practices for E-Commerce*, (June 1998) <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); Louis Harris & Associates & 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 there personal information were protected); 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).

safe."[120]

A number of U.S. commentators and policy makers advocate a "contractual approach to data privacy."[121] 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 dissemination of TRPI [telecommunications-related personal information]."[122] Proponents of contractual models claim that they 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," as that established by the Directive.[123] Under a contractual model, individuals can simply pay for privacy protection or threaten to take their business elsewhere.[124] Consumers may not be able to individually bargain with companies over their data privacy policies, but they can, according to this model, influence those policies by threatening to exit from transactions.[125]

These commentators also advocate 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."[126] The National Consumers League and others have designed projects

---

[120] Jamie Beckett and Dan Frost, FTC Sets Deadline on Internet Privacy Rules, S.F. GATE, Oct. 14, 1998.

[121] See e.g., Bibas, supra note ___; 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 such [personal] information").

[122] NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION, U.S. DEPARTMENT OF COMMERCE, PRIVACY AND THE NII: SAFEGUARDING TELECOMMUNICATIONS-RELATED PERSONAL INFORMATION Introduction C and III(1995), cited in PRIVACY IN THE INFORMATION AGE, supra note ___, 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.

[123] In support, Bibas cites the work of the free market economist Friedrich von Hayek, who advocates limited government involvement in the economy. See Bibas, supra note ___, at 605.

[124] As 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." PRIVACY IN THE INFORMATION AGE, supra note ___, at 104. The power of market constraints is demonstrated by the pressures placed on Pacific Bell, Lotus, Equifax and Intel. See supra notes ____.

[125] 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).

[126] Joshua Quittner, Invasion of Privacy, TIME, Aug. 25, 1997 at 35. This was the feature article of this issue of Time. Quittner was news director of Pathfinder, Time Inc.'s "mega info mall." He concludes, "[t]he only guys who insist on perfect privacy are hermits like the Unabomber."

to so educate consumers.[127] As Professor Fred Cate notes, consumers can learn to check help screens and instruction manuals, and, in general, develop a greater awareness of privacy issues, including their right to "opt out" of having their personal information used for other purposes.[128] In this way, market advocates argue, consumers may enforce privacy rights through contract (explicit or implicit) and threatened exit from contract.[129]

As efforts to regulate privacy through legislation and court intervention, however, private contract and market models, proffer no panacea. Markets (no surprise) are imperfect; knowledge is expensive; parties have unequal access to information. The market for data privacy protection is characterized by widely dispersed individuals, with low stakes,[130] 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 which they improve upon 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" which interfere with "mutually agreeable privacy protections."[131] 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

---

[127] See FEDERAL TRADE COMMISSION, PUBLIC WORKSHOP ON CONSUMER PRIVACY ON THE GLOBAL INFORMATION INFRASTRUCTURE, § IIIB. (1996), <http://www.ftc.gov/reports/privacy/privacy1.htm> (visited January 13, 1999) [hereinafter PUBLIC WORKSHOP ON CONSUMER PRIVACY]. Businesses, through the Online Privacy Alliance (a consortium of fifty-one large companies and business associations), also advocate educating consumers about privacy issues.

[128] See PRIVACY IN THE INFORMATION AGE, supra note ___, at 103.

[129] See Id.

[130] 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 which profits from violating it. Examples of significant harm are cited in ROTHFEDER, PRIVACY FOR SALE, supra note ___, including the murder of a sit com star by an emotionally-crazed admirer about her through computer data bases information about her through computer data base (at 15). See also reports on scandals leading to new privacy legislation, infra notes ___.

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

software technology,[132] encryption devices or "Smart Cards."[133] 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, as a proponent of a 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.[134] In critiquing the Directive for being "centrally planned" and thus inefficiently allocating privacy rights, Bibas fails to note that, in almost all cases under the Directive, consumers can "opt into" or "out of" the free dissemination of personal information about them.[135] The "opt in" right creates a different default rule around which market negotiations can take

---

[132] Novell has developed software that permits Internet users to control how much information may be collected from them by an Internet Web Site. The software "might also make it possible for users to sell or barter their personal information for rebates, discounts or other special considerations." See John Markoff, Novell to Offer Data-Privacy Technology for Internet, N.Y. TIMES, Mar. 22, 1999 at C1. See also discussion of 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," in Joel R. Reidenberg, Lex Informatica: The Formulation of Information Policy Rules Through Technology, 76 Tex. L. Rev. 553 (Feb. 1998).

[133] The FTC defines a Smart Card as "a stored value card bearing an implanted microprocessor. It permits its owner to enter into transactions anonymously and to transmit encrypted information via the Internet." PUBLIC WORKSHOP ON CONSUMER PRIVACY, supra note ___, § II n. 68.

[134] See A Contractual Approach to Data Privacy, supra note ___. Richard Posner, on the other hand, is clear in assigning the default rule, maintaining, "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." See Posner, The Right to Privacy, supra note ___, at 403 (arguing that a legal right of privacy should be "based on economic efficiency" and that, on account of transaction costs and the interest of obtaining creditable information, property rights in privacy should be assigned "away from the individual.") See also RICHARD POSNER, OVERCOMING LAW 531-551 (1995) (containing a subsequent confirmation of these views and a response to a critic, Kim Lane Schiepple, 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-economic approach, see Richard Murphy, Property Rights in Personal Information: An Economic Defense of Privacy, 84 GEO. L.J. 2381 (July 1996) (setting forth the economic rationale for a default rule assigning the property right to the individual). Murphy 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." See also Paul Schwartz, Privacy and the Economics of Personal Health Care Information, 76 TEX. L. REV. 1 (Nov. 1997). 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 better 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).

[135] On "opt in" and "opt out" rights under the Directive and their relation to the sensitive nature of the information, see infra notes__ and accompanying text. The Directive leaves it for 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."This is in turn subject to certain exemptions. See Directive, supra note ___, art. 8.

place than an "opt out" right or no right whatsoever.[136] 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 requring 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 over data privacy issues because they have greater per capita stakes.[137] Moreover, many Americans are somewhat ambivalent about privacy. While privacy advocates cite polls showing that 80% of Americans believe they have "lost all control over how companies collect and sue their personal information personal information,"[138] a majority of Americans nonetheless appear to accepts being targeted for marketing by mail based on consumer profiles.[139] In addition, the popular day-time shows of Jerry Springer, Oprah Winfrey, Sally, Ricky et al feed

---

[136] "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.

[137] Businesses pour millions of dollars into Congressional campaigns. See THE CENTER FOR PUBLIC INTEGRITY, NOTHING SACRED: THE POLITICS OF PRIVACY, at 5 and 55-61 (1998) (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, and breaking this down into tables). For a general analysis of the "privileged" position of business in U.S. politics, see CHARLES LINDBLOM, POLITICS AND MARKETS: THE WORLD'S POLITICAL-ECONOMIC SYSTEMS 170-200 (1977).

[138] In general, survey evidence indicates that a large majority of the public is concerned about privacy. See, e.g., Alan F. Westin, The Era of Consensual Marketing is Coming, (Dec. 14, 1998) <http://www.privacyexchange.org/iss/surveys/1298essay.html> (finding that nine out of ten Americans are concerned about threats to privacy); Lorrie Faith Cranor et al., Beyond Concern: Understanding Net Users' Attitudes About Online Privacy, AT & T LABS-RESEARCH TECHNICAL REPORT TR 99.4.3 (April 14, 1999) <http://www.research.att.com/library/trs/TRs/99/99.4/99.4.3/report.htm> (finding that only 13 percent of Internet users are unconcerned with privacy and noting that the level of Internet users' concern varies widely according to the type of information and the uses to which it is put). These and other privacy surveys are available at the Privacy Exchange website. See <http://www.privacyexchange.org> (visited March 30, 1999). Polls show that individual concern over threats to their privacy has consistently risen since the 1970s. See citations to Harris-Equifax Consumer Privacy Surveys since 1970 in Murphy, Property Rights in Personal Information, supra note__, at 2405.

[139] See Westin, The Era of Consensual Marketing is Coming, supra note__ (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 "businesses they patronize" and "products... that might be of interest," which should influence the data.

off self-exposure and voyeurism.[140] 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.[141] Businesses better promote their interests before Congress and administrative bodies than individual consumers facing considerable collective action problems.[142] When the Department of Commerce asks for comments on draft privacy guidelines, comments stream in from large multinational corporations and business associations.[143] As a result of successful industry lobbying, industry remains the dominant regulator

---

[140] This ambivalence toward privacy issues is captured on the cover of Newsweek Magazine the week the House of Representatives was to vote on President Clinton's impeachment, which read, HOT TICKET: Nicole Kidman bares all- about her daring Broadway debut, marriage to Tom Cruise and their fight for privacy. NEWSWK., Dec. 14, 1998 (cover). For Nicole Kidman, her fight for privacy obviously had a price, a price Newsweek was willing to pay so Americans could peep into it. The timing, paralleling the trial of the President over his concealment of a sexual affair, was apropos. In its competition against Time for market share, Newsweek had a "hot ticket." The cover of Time the same week read Who was Moses? TIME, Dec. 14, 1998 (cover).

[141] 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. Explanations nonetheless include the following: (i) European historical and cultural circumstances: In the aftermath of Naziism, 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 discrete 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 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. For a discussion of different forms of capitalism, see GOVERNING CAPITALIST ECONOMIES: PERFORMANCE AND CONTROL OF ECONOMIC SECTORS (J. Rogers Hollingsworth et al. eds.,1994); Robert Boyer, Capital-labour relations in OECD countries: from the Fordist Golden Age to contrasted national trajectories, in CAPITAL, THE STATE AND LABOUR: A GLOBAL PERSPECTIVE (Juliet Schor & Jong-Il You, eds., 1995).

[142] A significant part of the battle lies in the framing of the debate. Industry has so far successfully framed 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 to one of protecting fundamental human privacy rights from the publication of personal information by private commercial enterprises without the individual's consent. Or alternatively, advocates must invoke a balancing between privacy interests and economic interests, which 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 potentially manipulative anti-democratic aims.

[143] See infra Part V, notes __ - ___ and accompanying text. 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., Sam Pelzman, Toward a More General Theory of Regulation, 19 J.L. & ECON. 211 (1976); Roger Noll, Economic Perspectives on the Politics

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 Directive) under which courts and administrative bodies would recognize individual rights in personal information, could enjoin company use of it, issue civil and criminal fines, and award personal damages for rights violations. Others call for courts to independently expand tort law and recognize a cause of action for "tortious commercial dissemination of private facts."[144] Still others call for "legal recognition of property rights in personal information," enforceable before courts.[145] Personal information is valuable property and thus the business of trafficking it is rapidly expanding.[146] 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. In such 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 also limits to relying on courts.[147] 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 infinite number of transactions in which data privacy concerns arise, courts could not possibly handle all conflicts. Judicial budgets and staffs are finite.[148] And

---

of Regulation, in HANDBOOK OF INDUSTRIAL ORGANIZATION (R. Schmalensee & R.D. Willig eds., 1989).

[144] Jonathan P. Graham, Note, Privacy, Computers and the Commercial Dissemination of Personal Information, 65 TEX. L. REV. 1395, 1428, (1987). U.S. 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 William L. Prosser, 48 CAL. L. REV. 383 (1960); WILLIAM PROSSER, HANDBOOK OF THE LAW OF TORTS, 829-51 (3rd ed. 1964); RESTATEMENT (SECOND) OF TORTS § 652 (1977). The notion of a common law right to privacy was early espoused in the seminal article by Samuel Warren & Louis Brandeis, The Right to Privacy, 4 HARV. L. REV. 193 (1890) (maintaining that the privacy right "to be left alone" is based on the principle "of an inviolate personality."). See also Shorr, supra note ___, at 1776-1785.

[145] See Shorr, supra note ___, at 1818. See also Murphy, Property Rights in Personal Information, supra note__, and 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) (calling the individual's right to privacy "a type of property right in his electronic persona"). Mell, in her conclusion, however, calls for recognition of this property right by statute. See id. at 79.

[146] See infra note and accompanying text.

[147] See KOMESAR, supra note ___.

[148] The budgets and staffs of the data privacy supervisory authorities which are to oversee processing operations in each of the EU member states are similarly limited.

even if they weren't finite, 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 changed business practice. Even where this threat is limited in practice, human resource departments and in-house and external counsel will make businesses aware of its potential. This can lead to changed business practice.[149] The EU Directive alters the institutional balance in the United States, inciting such changes.

E. The Limits of Single Jurisdictional Analysis: The Need to Account for Transnational Institutional Interdependence. Comparative institutional analysis rightly identifies the key question "who decides who decides." Should decision-making be delegated to the markets and their pricing mechanisms, to legislatures and regulators to create fairer and more efficient default rules around which bargaining takes place, or to courts to balance competing concerns on a case-by-case basis? Which institutional mechanisms should predominate in which policy areas?[150]

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 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, it can affect the players' perception of their stakes. Data privacy regulation in Europe informs not only the tenor and context of debates in the United States; it shapes interest groups' appreciation of their options.[151] Under the Directive, U.S. businesses face potential litigation before European courts and administrative bodies. U.S. 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. From multiple directions, U.S. businesses are pressed to modify their data privacy practices. As a result of the confluence of these pressures, the 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 in terms of solely national

---

[149] See Part VB2, infra note ___.

[150] As noted above, however, we do not live in an ideal world of clearly differentiated alternative institutions. Institutions are typically complements to each other, not clean alternatives. Government regulations both shape market negotiations and facilitate their operation. See FREER MARKETS, MORE RULES, supra note ___, 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). Regulation "sets 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 229-238 (3rd ed. 1986).

[151] See infra Part V.

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 to simply segregate the foreign from the domestic, the external from the internal. In importing and exporting goods and services, countries can also import processing 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, institutions or courts) at alternative levels of social organization (be they sub-states, nations, 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.

III. The Transatlantic Context: Managing the Conflict over Privacy

This section first examines the roles of transatlantic economic liberalization and EU market power in U.S.-EU negotiations over data privacy standards (Part A). It then assesses the multiple public and private means through which Europe can restrict data transfers to the United States (Part B), and the attempts by U.S.-EU authorities to manage the resulting regulatory conflict (Part 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 EU exercises market power.[152] Simply put, the EU market matters to U.S. business. The EU is by far the United States' largest trading partner[153] and the site of most U.S. foreign investment. In 1997, the U.S. exported $253.6 billion of goods and services to the EU and imported $270.3 billion of goods and services from the EU.[154] 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.[155] This constituted "over half of all the foreign production of U.S. companies."[156] 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.

---

[152] See Hirschman's assessment of market power in infra note__.

[153] See BUREAU OF ECONOMIC ANALYSIS, INTERNATIONAL ACCOUNTS DATA: BALANCE OF PAYMENTS: TRANSACTIONS BY AREA (1997), <http://www.bea.doc.gov/bea/di/bparea-d.htm> (visited Jan. 12, 1998).

[154] 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, (1998) (Testimony of Assistant Secretary of Commerce Franklin Vargo), Federal News Service (May 7, 1998).

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

[156] 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."

EU 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 would be disproportionately vulnerable to access restrictions to the much larger U.S. market. U.S. retaliation against the EU, 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 EU as an independent political institution apart from the EU's fifteen member states. As Assistant Secretary of Commerce Franklin Vargo states, the New Transatlantic Agenda signed between the U.S. and EU in December 1995 "marks the first time that we are dealing with the EU as a political institution on a large scale."[157] A central purpose of the New Transatlantic Agenda is to coordinate and spur further trade and investment liberalization, both transatlantic and global.[158] 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's role in these negotiations.[159] Businesses on both sides of the Atlantic do not want

---

[157] Id. For an overview of the history of U.S.-EU economic relations since WWII together with recent institutional developments in the transatlantic relationship, see Mark Pollack & Gregory Shaffer, Introduction to TRANSATLANTIC GOVERNANCE IN A GLOBAL ECONOMY (introduction to working manuscript delivered as a paper at the Annual Meeting of the Political Science Association)(Sept. 2, 1999), available at http://www.polisci.wisc.edu/~pollack.

[158] 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." See The New Transatlantic Agenda <http://europa.eu.int/en/agenda/tr05.html> (visited March 12, 1999).

[159] 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 trans-Atlantic trade negotiations and policy coordination. See TABD Background <http://www.TABd.org/about/background.html> (visited Feb. 4, 1999).

In June 1997, under TABD-sponsored negotiations, the U.S. and EU 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 "$1 billion dollars annually in duplicate testing costs." See EU/US/Canada: Mutual Recognition Agreements Concluded, EUR. RPT., June 14, 1997; and Transatlantic Business Dialogue Convenes Third Annual Conference in Rome, Business America, Dec. 1, 1997. 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. RPT., Nov. 13, 1996. Within Europe, MRAs were earlier a major impetus to the completion of the EU'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 U.S. and EU 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 Before the Subcommittee on Trade of the U.S. House of Representatives Ways and Means Committee, (1997) (Testimony of Patrick Yahanan

officials sidetracked by disputes over data privacy protection.

In transferring negotiating authority to the European Commission over transnational data protection matters,[160] individual European countries enhanced their autonomy and influence vis-a-vis the United States. It has made the EU's threat to restrict transatlantic data transfers more credible. Before the EU Directive, a number of EU member states had data privacy legislation which, 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 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.[161]

By 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 U.S. 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 through threatening to retaliate against them. The United States is now more restrained. The threat of counter-retaliation by the EU is a powerful countervailing force.[162] The EU member states have not simply "lost" sovereignty in working through centralized EU authorities. They have reallocated it in a manner which effectively enhances their negotiating authority (and in

---

on behalf of The American Electronics Association). Charlene Barshefsy, the United States Trade Representative, testified to Congress that this "amounts to a global tax cut of $5 billion." Consumer Trade Issues Before the Senate Commerce Committee (1997) (Testimony of Charlene Barshefsky).

Finally, in 1998, the U.S. and EU successfully lobbied the 132 members of the World Trade Organization to adopt a multilateral tax-free policy on Internet transactions for a one year trial period. This was adopted in May 1998 in Geneva, Switzerland at the second WTO Ministerial meeting. See Bill Pietrucha, WTO Holds Line on Internet Tariffs, NEWSBYTES NEWS NETWORK, May 21, 1998 available in Westlaw, Worldrptr Database, 1998 WL 11722310.

[160] Not all enforcement authority was transferred. Under Article 25.4 of the 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. Directive, supra note ___ art. 25.4. Commission decisions to restrict data transfers are to be approved by member state representatives by a qualified majority vote (art. 31.2). "Member States shall [then] take the measures necessary to comply with the Commission's decision." Id.

[161] See Part V.A, supra notes__ and accompanying text.

[162] In speaking with a single voice, EU member states can now use their collective market power to reach better negotiating outcomes with the U.S. An example of this phenomenon is the constraint on U.S. use of unilateral retaliation against the EC vis-a-vis Section 301 of the 1974 U.S. Trade Act. While the United States was relatively successful in using Section 301 against Japan and the newly industrialized countries of Asia during the 1980s, it was considerably less so against the European Community. See PATRICK LOW, TRADING FREE: THE GATT AND US TRADE POLICY 91 (1993).

that way their autonomy) vis-a-vis the United States.[163]

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 leveraging upwards of data privacy protection. The European context itself demonstrated how efforts to ensure trade liberalization can strengthen social protection within a larger geographic area.[164] In the EU, data privacy regulation itself was not a barrier to trade. Rather, it was the lack of adequate harmonization of this protection which raised a potential barrier. By harmonizing data privacy protection, the EU 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 EU can potentially block data transfers to the United States. Similarly, it is because the EU 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 blocks that now facilitates the leveraging upwards of data privacy protection throughout the world. Where data privacy protection is a salient interest in a powerful state, the goals of ensuring data privacy protection and enhancing trade liberalization become twin goals.

B. Public and Private: The Multiple Means to Restrict Data Transfers to the U.S. EU data privacy regulation poses multiple threats to U.S. companies. As described in Part II, Article 25 of the 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 EU could ban transfers of health

---

[163] As Joel Trachtman states, "[s]overeignty, viewed as an allocation of power and responsibility, is never lost, but only reallocated." 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." Joel Trachtman, Reflections on the Nature of the State: Sovereignty, Power and Responsibility, supra note__, at 400.

Nonetheless, ongoing member state differences can still undercut a common EU position and weaken the Commission's negotiating stance. To the extent 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 which oversees and provides instructions to the Commission regarding the EU-U.S. negotiations over data privacy protection. Interview with UK and Danish permanent representatives and officials from DGXV, in Brussels, Belg. (June 23-24, 1999). Despite these internal disagreements, however, the point remains that the Directive has brought the U.S. to the table to negotiate enhanced U.S. data protection protections.

[164] See Part I.A, infra notes__ and accompanying text. 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 EU to take a more proactive role in international environmental negotiations, driving standards upwards in bargaining over international ozone layer protection and hazardous waste trade). Decisions in the EU over data privacy protection are similarly taken by a qualified majority (not unanimous) vote.

information or transfers for direct marketing purposes.[165] In either case, affected firms would have to process information separately in Europe, or apply for an exemption from member state supervisory authorities. Neither option allures.[166]

Member state authorities can also independently fine individual companies and enjoin them from transferring data, including to their U.S. affiliates.[167] 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.[168]

Individuals and, depending on member state 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 Web sites, can be subject to claims before European courts.[169] American companies are already subject to EU-based claims. The United Kingdom fined U.S. Robotics Corp. "for failing to register under the UK's Data Protection Act and for obtaining personal information about individual visitors

---

[165] 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 NONE OF YOUR BUSINESS, supra note ___, at 171-172.The consultant's lengthy report, European Commission Tender No. XV/97/18D, Application of a Methodology Designed to Assess the Adequacy of the Level of Protection of Individuals with Regard to Processing Personal Data: Test of the Method on Several Categories of Transfer, Presented by the University of Edinburgh on behalf of Charles Raab, Colin Bennett, Robert Gellman and Nigel Waters (Sept. 1998), is available at http://www.cous.uvic,ca/poli/bennett/research/index.htm.

[166] 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 - $50 million a year in hardware and maintenance, depending on the size of the center. See NONE OF YOUR BUSINESS, supra note ___, at 54. (citing David B. Yoffie and Tarun Khanna, Microsoft Goes Online: MSN 1996, Harvard Business School reprint N9-797-088 (as revised 1997)).

[167] The Directive arguably covers ad hoc transfers of information, such as by e-mail, concerning company employees, customers, or suppliers. The Directive could affect 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.

[168] Just before the Directive went into effect, Privacy International, a London-based privacy organization, warned that it will oversee the 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.

[169] 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. See supra note ___.

to its Web site and then using that information to market other products."[170] 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.[171] Other data transfers to the United States have been barred by British, French and German courts and administrative authorities.[172]

In liberal regimes, law is not the monopoly of the state and its representatives. The 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 draftsmen did not predict. In an institutionally interdependent world, 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 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 (advocating the market as primary institution).[173] U.S. Commerce officials defend U.S. practices, critiquing the EU for its "top-down approach" of "privacy czars and bureaucrats," antithetical to U.S. traditions of limited governmental intrusion in the private sector.[174] Yet to avoid a regulatory conflict, U.S. officials simultaneously prompt businesses to create "self-regulatory" procedures more protective of individual privacy. Entering the fray, U.S. privacy advocates, skeptical of "self-regulation," press for further legislation.[175]

---

[170] EU Directive on Privacy May hinder E-Commerce, supra note___.

[171] See David E. Kalish, U.S. Firms Fear Impact of EU Privacy Law, THE RECORD (Bergen County, NJ) Oct. 29, 1998.

[172] See The EU Data Protection Directive, Information Privacy, and the Public Interest, supra note ___, at 438, (citing prohibitions on data transfers to the U.S. from Britain (involving sales to a direct mail organization) and France (involving patient records)).

[173] See David Banisar, The Privacy Threat to Electronic Commerce, COMM. WK. INT'L, June 1, 1998. However, there are divisions within the administration on privacy issues as presented in Part VA below.

[174] See European Law Aims to Protect Privacy of Personal Data, supra note ___. See also U.S. GOVERNMENT WORKING GROUP ON ELECTRONIC COMMERCE, FIRST ANNUAL REPORT (1998), at 18 (critiquing the EU's "broad, centralized, top-down approach to privacy protection" which could disrupt "the free flow of information") [hereinafter WORKING GROUP FIRST ANNUAL REPORT].

[175] The privacy advocate Marc Rotenberg (of EPIC) critiques, "at 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." See Internet Commerce Study Stresses Self-Regulation, N.Y. TIMES, Nov. 30, 1998. One problem with the self-regulatory approach advocated by the U.S. Department of Commerce is that, even if one has the right to choose to have personal data disclosed, the right is meaningless if it is not accompanied by a right to do anything about its being disclosed. The Department of Commerce critiques the EU approach as "top-down," yet the EU approach gives individuals rights to act as private

The EU has delayed enforcing the Directive's provisions on third country transfers while negotiations take place.[176] 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.[177] EU commercial interests press their member state representatives and EU officials to avoid a transatlantic trade war over data privacy issues. A ban would impede not only data transfers, it would hamper negotiations over further tariff negotiations and mutual recognition agreements in areas mutually important to large U.S. and EU commercial interests.[178]

In addition, only a minority of the fifteen EU member states have so far enacted legislation implementing the Directive, even though they were all to have done so by October 25,1998.[179] Even though member state failure is due primarily to legislative inertia and not to opposition to data

---

attorney generals 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 note__ and accompanying text.

[176] 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).

[177] This raises the questions why the United States' exercise of market power will not cause the EU's 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 EU's internal situation, the following points are noted. First, there are powerful internal reasons why the EU 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 Directive were initially negotiated. These reasons were outlined earlier. See supra note__. In addition, now that EU businesses are subject 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. See discussion of the protectionist aspects of the Directive, infra note__. Nonetheless, the Directive grants member states flexibility in its implementation. As Bainbridge notes, there remain some pressures on member states to implement the Directive in a business-friendly manner, where permissible, so as to attract data processing operations to locate within their jurisdiction. See Bainbridge, supra note __, at 73.

[178] To give just one example, the EU 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).

[179] 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 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) (July 30, 1999). Nonetheless, under the EU's "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 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, <http://europa.eu.int/comm/dg15/en/media/dataprot/news/925.htm > (visited January 13, 1999). 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 L. Mogg, director-general for internal market and financial services at the European Commission, who said that "even without implementation by every member state ... the directive will take effect under the EU's 'direct effect' doctrine"). For an overview of the "direct effect" doctrine, see JO SHAW, LAW OF THE EUROPEAN UNION, at 251-282 (1996).

privacy controls per se, their failure undermines the Commission's negotiating position. Were the EU to ban data transfers to the United States before all member states themselves implement the Directive's protections, the ban could be more vulnerable to a U.S. claim that it violates international trading rules.[180] EU authorities act in the shadow of a supranational institution, the World Trade Organization, and the constraints imposed by its rules.

The United States proposes that the EU and U.S. 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.[181] The U.S. maintains that compliance must provide companies with a "safe harbor" against any challenge by EU authorities of their data processing practices. The EU, however, rejected the United State's initial proposals as inadequate. Although U.S.-EU discussions may soon result in a negotiated compromise,[182] the EU has confirmed that it will enforce the Directive's provisions banning data transfers to third countries if a satisfactory solution is not reached. EU authorities note that, were the EU to agree to "safe harbor" provisions to remove the threat of a ban, EU residents will retain their right to file private complaints before EU member state courts and administrative bodies against companies which violate agreed principles.[183] 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 Directive's extra-jurisdictional impacts could be beneficial (if the U.S. currently under-regulates data privacy protection) or detrimental (if the EU 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 section commences by presenting the grounds for a U.S. claim that the Directive violates the supranational rules of the world trading system which constrain countries' abilities to restrict trade (Part A). It then evaluates why the United States would likely not prevail under WTO rules (Part B), in particular in light of the procedural concerns articulated in recent WTO jurisprudence (Part C). The section 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 EU from U.S. retaliation against application of the Directive. Ironically, contrary to popular conceptions, by constraining the United States' ability to retaliate against the Directive's application, WTO rules reinforce the Directive's extra-jurisdictional effects

---

[180] See infra Part IV. As one EU representative confirmed, "[b]ut 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).

[181] See supra notes ___.

[182] See, e.g., EU, U.S. Predict Data Accord by End of '99, NEWSBYTES (Sept. 24, 1999); EC Official Encouraged by Greater Clarity in U.S. Stance on Data Privacy Enforcement, Int'l Trade Rep. (BNA) (Sept. 21, 1999).

[183] See EU Rejects U.S. Data Privacy Plan, supra note ___ (noting remarks of Gerrit de Graaf, first secretary of the European Union).

(Part D). They thereby enable a trading up of U.S. standards.

A. WTO Constraints on the EU: Claims that the Directive Violates WTO Rules. There are arguably some protectionist motives behind the Directive. U.S. businesses are more advanced in the use of information technology than EU businesses. EU businesses, unable to forestall EU regulation, would like the playing field to be leveled so that U.S. businesses must operate under similar constraints.[184] In an attempt to ward off EU action, U.S. officials implicitly threatened to challenge any ban imposed by the EU before the Dispute Settlement Body of the World Trade Organization (WTO).[185] The threshold issue under WTO rules[186] is whether the transfer of data involves a sale of goods or of services. If a sale of goods, the transfer is covered by the General Agreement on Tariffs and Trade (GATT) 1994. If a service, the transfer is covered by the General Agreement on Trade in Services (GATS).[187]

Data is typically transferred across the Atlantic electronically, as part of an electronic

---

[184] The potential protectionist impacts of the Directive are discussed in NONE OF YOUR BUSINESS, supra note__, at 145-146, 189-196. A primary protectionist concern is that, through causing the U.S. to raise its data privacy requirements, the EU would level the playing field by raising 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 Directive could favor EU data processors (to the extent firms decide to use separate data processing facilities in Europe) and EU service providers (to the extent EU-based firms decide to do business with EU-based firms to whom they can freely transfer data, and not with U.S.-based firms). However, these impacts are difficult to measure and, as discussed below, are not the result of de jure discrimination since all firms would still be subject to the Directive's requirements.

[185] For example, Ira Magaziner, formerly responsible for U.S. discussions on electronic commerce issues, including privacy, stated that, "In general, we in the U.S. 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, March 2, 1998.

[186] 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. Telephone Discussion with Donald Abelson, Chief Negotiator for Communications and Information of the Office of the United States Trade Representative (USTR), concerning a draft of this section, (April 19, 1999). However, in other contexts, USTR officials praise the WTO for being a "rule-based" institution. The different positions depend on whether, before Congress, the USTR is defending the need for WTO rules to protect U.S. export interests, or defending the autonomy of U.S. policy-making despite WTO rules. While it is true that many WTO provisions are more like principles than detailed rules (such as the principle of non-discrimination), and that countries can pay compensation to other WTO members harmed by their infringing practices in lieu of changing those practices, 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, which can ultimately result in WTO-authorized sanctions against the infringing WTO member. This can constrain government action.

[187] 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., WTO Appellate Body Report, European Communities--Regime for the Importation, Sale and Distribution of Bananas, WT/DS27/AB/R, (Sept. 9, 1997), 37 I.L.M. 243, 244 (1998).

message. In March 1998, the WTO Secretariat issued a report entitled Electronic Commerce and the Role of the WTO which addresses, among other matters, the coverage of electronic transactions under present WTO agreements.[188] As noted by the report, "Electronic commerce could be characterized as trade in goods, trade in services, or as something different from either of these."[189] 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."[190] To the extent personal data is a non-standardized product, its transfer should thus be covered under GATS, and not GATT 1994.[191]

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's 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.[192] The EU has made market access commitments for "Telecommunications Services" (including "basic" and "value-

---

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

[189] See id. at 50.

[190] 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.

[191] 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 further review electronic commerce issues under the relevant WTO Agreements, including under GATT 1994 and GATS. See Work Programme on Electronic Commerce, adopted by the WTO General Council, WT/C/274 (Sept. 30, 1998). In the WTO Work Programme, the issue of "protection of privacy" is to be treated under "the GATS legal framework." See 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 which showed that WTO members have been unable to overcome their long-standing disagreement on whether all electronic deliveries are services or if 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 EU maintains that all electronic transactions should be classified as trade in services while the U.S. maintains that some should be classified as trade in goods. This report is to be modified and combined with others for purposes of the November 1999 WTO Ministerial meeting held in Seattle, Washington. 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.

[192] See European Communities and their Member States: Schedule of Specific Commitments GATS/SC31 (April 15, 1994), as 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 (April 11,1997); GATS/SC/31/Suppl.3 (April 11, 1997); GATS/SC/31/Suppl.4 (Feb. 26, 1998) [collectively hereinafter EU Schedules].

added telecommunications"), which could cover data transfers.[193] It has also made commitments for numerous other service sectors and activities which 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.[194] Since the telecommunications commitments only cover the "transport of electromagnetic signals" and not the "content" of those signals, arguably only sector-specific commitments would apply.[195]

If a data transfer is covered under one of the EU's commitments, then the EU is obliged to treat U.S. service providers no less favorably than EU service providers (GATS Article XVII), and to apply its domestic regulation in a "reasonable" manner (GATS Article VI).[196] It is the claim of reasonableness which could lie at the core of a U.S. action. In addition, were the EU to ban data transfers only to the United States, but not to other WTO members which inadequately protect data privacy under the EU's criteria, the EU could violate the GATS most-favored nations clause under Article II.[197]

---

[193] See id. Confirmed in telephone interview with Donald Abelson, Chief Negotiator for Communications and Information, USTR (Dec. 7, 1998).

[194] See EU Schedules, supra note__

[195] 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's 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." EU Schedules, supra note ___.

[196] There are other technical, legal defenses that the EU might invoke before a WTO panel were a case brought. 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 acords to its own like services and service suppliers." Arguably this provision only applies to EU internal requirements for the provision of services, and not to the export of services. This was pointed out to the author in an e-mail exchange with Eric White of the Legal Services division of the European Commission (May 24, 1999).

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 U.S. (as claimant) might contend, on the one hand, than an export ban generally prejudices the supply of services by U.S.-owned service providers in the EU, since they are more likely to be affected than EU-owned service providers. The EU might respond that such an indirect effect on the provision of services in the EU could not be covered under GATS because ultimately all measures have indirect effects. The U.S. might, in turn, counter that a ban on data transfers to the U.S. clearly has foreseeable effects on the provision of services by U.S.-owned service providers in the EU market, so that they are discriminatory and thus prohibited under GATS.

[197] Under the most favored nations clause, the EU cannot accord less favorable treatment to U.S. services and service suppliers than to those of any other WTO members. See GATS art. II. This latter obligation is not subject to any limitation by sector or otherwise.

B. Why the U.S. 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 Directive applies equally to transfers to all countries and thus should not violate the GATS most-favored nations clause.[198] 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.[199] So long as the EU does not clearly discriminate against the U.S. or U.S. service providers in its application of the Directive, the United States would likely not prevail.

Second, the EU 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, Article XIV, explicitly authorizes WTO members to restrict commerce in order to protect "the privacy of individuals." This provision significantly bolsters the EU's defense. While GATS' thrust is to liberalize trade in services, under GATS Article XIV, WTO members may adopt and enforce measures relating to services which:

> "Subject to the requirement that such measures 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,... [are] necessary to secure compliance with laws or regulations not inconsistent with the provisions of this Agreement, including those relating to:... (ii) 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"(emphasis added).[200]

---

[198] See GATS art. II.

[199] See GATS art. XVII. The U.S. recognizes this. As Assistant Secretary of Commerce Franklin Vargo reports to the U.S. Congress, "The 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__.

[200] See GATS art. XIV. 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 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 GATT Article XI which prohibits quantitative restrictions, including bans, on "the exportation or sale for export of any product" to another WTO member. 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 (Article XX), provided the EU does not apply the ban in a clearly discriminatory manner. GATT Article XX provides that WTO members may adopt and enforce measures which do not constitute "arbitrary or unjustifiable discrimination... (b) necessary to protect human life or health" or "(d) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement...." GATT art. XX. These exceptions were the model for those contained in GATS so that a similar analysis should apply. In particular, the express inclusion of "the protection of the privacy of individuals" as an example of such "laws or regulations" in the GATS exception clause gives meaning to the more general terms of Article XX. The more general language of GATT Article XX should thus provide the same protection against a U.S. challenge under GATT 1994 to the EU Directive, as against a challenge under GATS. In the end, the characterization of transferred data as a good or a service should be irrelevant.

Given that the privacy interests of EU residents are directly at stake, it is unlikely that a WTO panel would find the Directive's content to be "unreasonable."[201]

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." In support, the U.S. would note that prior trade panels have interpreted the term "necessary" to require a measure to be the "least trade-restrictive" available,[202] and that, in general, exceptions to GATS obligations are to be restrictively applied. The U.S. would contend that its policies are adequate under international norms, and EU restrictions are thus neither reasonable nor necessary.[203] In all events, the U.S. 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.[204]

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 EU-- as opposed to outside the EU-- are directly at stake. Under media scrutiny, WTO dispute settlement panels would prefer to refrain from engaging in a close balancing

---

[201] Lax foreign regulations have externalities that can undermine the Directive's goal of protecting the privacy of EU residents. See supra note___.

[202] See Thailand- Import Restrictions on Importation of and Internal Taxes on Cigarettes, adopted 7 Nov. 1990, BISD 37S/200, para. 75. See also Appellate Body Report on United States- Standards for Reformulated and Conventional Gasoline, adopted 20 May 1996,WT/SD2/R.

[203] The U.S. might argue, for example, that the EU and other developed countries have negotiated and agreed to a set of privacy principles, which reflect a multilateral consensus of what is "reasonable." These principles, agreed 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), and are available on the EU Web site at http://www.europa.eu.int/comm/dg15/en/media/dataprot/inter/priv.htm. For information on the OECD, see the OECD's Web site at <http://www.oecd.org/dtsi/sti/it/secur/prod/priv_en>. However, the OECD principles are merely hortatory and not enforceable, nor do the they bind the EU in its determination of what is "reasonable" to protect its citizens and residents. Moreover, it is questionable whether the U.S. actually complies with the OECD guidelines. The U.S. might also argue that the 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 Directive was first enacted. To the extent the Directive applies to most electronic mail communications, the U.S. might argue that this is excessive. See NONE OF YOUR BUSINESS, supra note ___, at 189-193. The EU may respond, however, that these technological developments render the need for privacy protection even more important.

[204] The U.S. would also note that the introductory clause to Article XIV sets forth an additional condition-- the EU's restrictions must not constitute "arbitrary or unjustifiable discrimination." If the EU were, in practice, to apply the Directive in a discriminatory manner vis-a-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, "if all the enforcement heat falls on a handful of U.S. multinationals, the U.S. can bring a complaint in the World Trade Organization's new dispute resolution body." See Will Amex and EDS Privacy Lawsuits in Europe?, supra note ___.

of competing trade and privacy interests, and rather review the process by which the EU takes account of foreign privacy protections. This is the approach recently taken by the WTO Appellate Body in an analogous case.

C. A Focus on Process: The Directive under the WTO's New Criteria. The EU's regulation of data privacy protection is "extra-jurisdictional" in its focus in that it is concerned with the adequacy of data privacy protection outside of the EU's jurisdiction. The recent WTO Appellate Body Report in the U.S. shrimp-turtle case,[205] 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 United States' application of its law violated GATT rules and was not protected by the GATT general exception clause (Article XX),[206] the Appellate Body enumerated a number of relevant criteria which support an EU defense. The Appellate Body held that the United States' 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. The U.S. thus failed to comply with Article XX's conditions on the following procedural grounds relevant to the EU's Directive:

(i) The U.S. required all exporting WTO members to adopt "essentially the same [conservation] policy," and not merely "comparable" ones;
(ii) The U.S. failed to take "into consideration the different conditions which may occur in the territories... of different members;"
(iii) The U.S. did not seriously attempt to reach a multilateral solution;
(iv) Under its country-wide ban, the U.S. prohibited shrimp imports even where vessels caught them using U.S.-prescribed methods; and
(v) The U.S. certification process was not transparent or predictable.[207]

---

[205] See Communication from The Appellate Body: United States – Import Prohibition of Certain Shrimp and Shrimp Products available in Westlaw, 1998 WL 716669 (W.T.O.). For an overview and analysis of the Appellate Body shrimp-turtle decision, see Gregory Shaffer, The U.S. Shrimp-Turtle Appellate Body Report: Setting Guidelines toward Moderating the Trade-Environment Conflict, BRIDGES, Oct., 1998, at 9; and Gregory Shaffer, United States-- Import Prohibition of Certain Shrimp and Shrimp Products, 93 AM J. OF INT'L L. 507 (April 1999) [hereinafter Shaffer, Import Prohibition]. The shrimp-turtle case applied Article XX of GATT 1994 (the general exception provisions) to the United State's ban on certain imports of shrimp from South and Southeast Asian countries where the shrimp were caught with methods that did not protect endangered sea turtles. The U.S. prescribed a particular method, the use of devices known as TEDs (or turtle exclusion devices), 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 id.

[206] On Article XX, on which the GATS exception clause was modeled, see supra note__.

[207] 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 TEDs technology to certain developing countries than others. See Shaffer, Import Prohibition, supra note ___. 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 U.S.

The EU's application of the Directive should meet these Appellate Body criteria for permissible extra-jurisdictional measures. First, unlike the U.S. guidelines applied to foreign shrimping practices, the Directive only requires "adequate" privacy protection, not essentially the same protection. Second, whereas the United States did not examine differentiating conditions in individual countries, the EU has created a Working Group to report on individual country practices and conditions that affect the privacy of EU residents. The EU even commissioned a report from two U.S. law professors specialized in data privacy law, 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.[208]

Third, the EU has engaged in prolonged, detailed discussions with U.S. representatives to examine data privacy safeguards which could be applied. If the U.S.-EU discussions do not result in a negotiated solution and restrictions are ultimately imposed, the EU will have strong grounds to claim that they 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 U.S. did not offer to enter into negotiations with the concerned countries in South and Southeast Asia until after its ban went into effect.

Fourth, the 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. Even were the EU to find U.S. data protection laws inadequate, individual companies could obtain exemptions by demonstrating that they employ adequate internal policies.[209] The Directive also creates six express exceptions to a general ban, including (i) where the individual data subject "unambiguously" consents to the transfer and is informed as to how the data will be used, and (ii) where "the transfer is necessary for the... performance of a contract concluded in the interest of the data subject."[210] The United States' shrimping guidelines, on the other hand, did not permit any

---

[208] See DATA PRIVACY LAW, supra note __. See also European Commission Tender No. XV/97/18D, Application of a Methodology Designed to Assess Adequacy, infra note__.

[209] Article 26(2) of the 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.

Directive, supra note ___, art. 26(2).

[210] 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 U.S. 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. Article 26 provides:

> Derogations
>
> 1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a 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) may take place on condition that:

exceptions to its country-wide ban, even where individual companies implemented the very measures mandated by the United States.

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 Directive and its applications. This access has been both direct and in coordination with EU companies through the Transatlantic Business Dialogue.[211] 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 the United States' territorial waters. From a WTO perspective, the Directive is more defensible because it regulates product-related standards that affect EU residents, and not non-product-related production

---

(a) the data subject has given his consent unambiguously to the proposed transfer; or
(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request; or
(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or
(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or
(e) the transfer is necessary in order to protect the vital interests of the data subject; or
(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.
2. Without prejudice to paragraph 1, a Member State may authorize a transfer or a 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.
3. The Member State shall inform the Commission and the other Member States of the authorizations it grants pursuant to paragraph 2.
If a Member State or the Commission objects on justified grounds involving the protection of the privacy and fundamental rights and freedoms of individuals, the Commission shall take appropriate measures in accordance with the procedure laid down in Article 31 (2).
Member States shall take the necessary measures to comply with the Commission's decision.
4. Where the Commission decides, in accordance with the procedure referred to in Article 31 (2), that certain standard contractual clauses offer sufficient safeguards as required by paragraph 2, Member States shall take the necessary measures to comply with the Commission's decision.

Directive, supra note ___, art. 26.

[211] See discussion of TABD in supra note __ and accompanying text.

processes that affect only foreign residents. In the case of the Directive, its aim is to protect the privacy of persons residing within the EU, not outside of it.[212]

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 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 effectively raise its data privacy standards. Rather, WTO rules constrain the United States' ability to unilaterally retaliate against the EU for harming U.S. commercial interests. Were the U.S. to so retaliate, it would itself violate WTO rules and be subject to an EU complaint before the WTO's Dispute Settlement Body.[213]

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 which result in foreign environmental harm or foreign labor repression.[214] Paradoxically, in the case of data privacy, rather than protecting the U.S. from coercion to raise U.S. privacy standards, WTO rules shield the EU from a countervailing retaliatory threat. WTO rules thereby reinforce pressure on the U.S. to negotiate with the EU a set of

---

[212] 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's 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. See also 1952 Panel Report on Belgian Family Allowances, G/32, adopted Nov. 7, 1952 (concerning the impermissibility of import restrictions on products from countries imposing lower social charges on companies).

[213] The WTO does not permit unilateral retaliatory measures, as exemplified by the U.S.-EU dispute regarding the EU's ban on meat from cows fed with certain hormones that has lasted over ten years. After consultations did not resolve the conflict, the U.S. unilaterally retaliated in 1989 with duties imposed on various EU imports. After the creation of the WTO, the EU requested (in 1996) that the WTO establish a panel challenging the U.S. retaliatory tariffs, and the U.S., a month later, removed them in the shadow of a likely adverse panel decision. Instead, the U.S. brought its own WTO claim challenging the EU's ban on such U.S. meat. Only after WTO dispute settlement panels ruled in favor of the U.S. and the EU failed to comply with such ruling, was the U.S. permitted to take retaliatory measures. The WTO rulings are available at <http://www.wto.org/wto/dispute/distab.htm> (visited Oct. 5, 1999). See also Kenvin 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).

[214] See supra note__. 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 discussion in DANIEL ESTY, GREENING THE GATT (1994).

"positive," more stringent, data privacy requirements.[215] WTO rules thereby contribute to a trading up of U.S. standards.

V. The Directive's Extra-Jurisdictional Effects in the United States: Changing the Stakes of Domestic Players.

Because the Directive applies to data transfers worldwide, it has extra-jurisdictional effects. U.S. businesses feel the greatest impact because they engage in more European transactions than other foreigners and they make the most sophisticated use of information on account of their technological edge. The 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 and enhance it in order to fend off a regulatory conflict with the European Union (Part 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 and thereby affect demand for businesses' products (Part B). It has pressed U.S. businesses to enhance self-regulatory efforts to forestall EU restrictions on data transfers to the United States, divert demands for stricter and broader U.S. regulation and counter negative publicity (Part C). The context in which U.S. domestic debates over data privacy protection take place has been altered.[216] U.S. 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."[217] 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

---

[215] Negative rules are those which tell countries what they can't do-- such as restrict the import of foreign goods in order to benefit a national industry. Positive rules are those which mandate what countries must do-- such as enforce defined environmental and intellectual property protections. An example of positive international intellectual property protection requirements is the TRIPS Agreement (Trade-related Aspects of Intellectual Property Rights), which, among other matters, requires countries to recognize and enforce certain patent, copyright, trademark and trade secret rights.

[216] This is in line with "constructivist" theory which focuses on the way knowledge, agenda and norms are shaped through communicative processes, including through interactions among policy makers and private parties. *See, e.g,.* MARGARET KECK & KATHERINE SIKKINK, ACTIVISTS BEYOND BORDERS 1 (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 this case, however, issues are being shaped in the United States more on account of the harnessing of pressures from foreign regulators by domestic actors to advance their distinct goals.

[217] Mr. David Aaron, of the Department of Commerce, 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. See European Law Aims to Protect privacy of Personal Data, supra note ___, (quoting David Aaron, Undersecretary of Commerce).

rights" guaranteeing on-line privacy, in particular as regards medical and financial records.[218] 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 online data privacy protection for children,[219] and generally criticized the online data collection practices of U.S. businesses for failing to provide adequate privacy protection.[220] Although privacy advocates were critical of the FTC's

---

[218] 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." See WORKING GROUP FIRST ANNUAL REPORT, supra note ___. 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 (Transcript of President Clinton's State of the Union Address), and of financial records in a May 4, 1999 address, see Remarks by the President on Financial Privacy and Consumer Protection (visited Sept. 8, 1999) <http://www.whitehouse.gov/WH/New/html/19990504-1925.html>. This was followed in late October 1999, when the Clinton administration proposed new regulations to protect the privacy of medical records. These are intended to be finalized and adopted as law by Feb. 21, 2000. See Rules of Privacy on Patient Data, supra note__. The number of bills pending before federal and state legislators are cited in Online Privacy Protection: Testimony of Commissioner Sheila F. Anthony Before the U.S. Senate Subcommittee on Communications (visited Sept. 8, 1999) <http://www.ftc.gov/os/1999/9907/SFAtestimony.htm>; see also inra note ____.

[219] This culminated in Congress' passing the Children's Online Privacy Protection Act in October, 1998, which now requires Web sites to provide actual notice and to obtain prior parental consent before companies collect information about children under the age of thirteen. See Pub. L. No. 105-277, 112 Stat. 2681 Title XIII (1998) ("COPPA"). 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 Web sites 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 U.S. Urges New Rules to Guard Privacy of Children on Internet, N.Y. Times, April 21, 1999, at__.

[220] See FTC, PRIVACY ONLINE: A REPORT TO CONGRESS (June 1988) (available at http://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. See id., at 41. After completing a three year study, the FTC concluded, "[I]ndustry's efforts to encourage voluntary adoption of the most basic fair information practices have fallen short of what is needed to protect consumers." See FEDERAL TRADE COMMISSION, FTC RELEASES REPORT ON CONSUMERS' ONLINE PRIVACY (June 4, 1998) <http://www.ftc.gov/opa/1998/9806/privacy2.htm>. In a survey of Web sites 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." See PRIVACY ONLINE, at 23; see also Joel Brinkly, FTC surfs the Web and Gears up to Demand Privacy Protection, NY TIMES, Sept 21,

ensuing July 1999 report to Congress entitled Self-Regulation and Privacy Online because the report did not recommend new legislation,[221] 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."[222] The FTC continues to monitor self-regulatory developments and support other privacy legislation. In addition to recently drafting the implementing regulations protecting children's online privacy, 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.[223]

The FTC and Congress remain under pressure to act, as do state legislatures and regulatory agencies. Numerous bills to enhance data privacy are pending.[224] 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.[225] Media reports on the "adequacy" of U.S.

1998.

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."See Mozelle W. Thompson, Solutions for Data Protection and Global Trade, Remarks Before the EU Committee of AMCHAM (Dec. 3, 1998) <http://www.ftc.gov/speeches/thompson/speech123.htm>. Such statements weaken the United States' position in its negotiations with the EU over the "adequacy" of U.S. business self-regulation.

[221] See Hearing on Privacy on the Internet Before the Subcomm. On Communications of the Sen. Commerce Comm., 106th Cong. (July 27, 1999) (statement of Marc Rotenberg, Director, Electronic Privacy Information Center).

[222] See 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, 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 progress in industry self-regulation efforts." See Federal Trade Commission, Self-Regulation and Privacy Online: A Report to Congress (July 1999), available, at http://www/gov/privacy/index.html [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 -20% of the most active websites offer all of the four basic "substantive fair information practices": "Notice/Awareness, Choice/Consent, Access/Participation, and Security/Integrity."

[223] See FTC Chairman Testifies Before House Subcommittee on the Privacy Provision of H.R. 10, (July21, 1999) <http://www.ftc.gov/opa/1999/9907/hr10.htm>.

[224] 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, March 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."

[225] See FTC June 1998 Report on Privacy Online, supra note__, at 41. See also FTC July 1999 Report on Self-Regulation, at 14 (noting "A second task force will address how incentives can be created to encourage the development of privacy enhancing technologies.").

protections under the Directive keeps these data privacy issues in the spotlight.[226]

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.[227] The 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 avoid lawsuits brought in the EU.[228] As the FTC's most conservative member on privacy regulation states, "In 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."[229]

While defending U.S. commercial interests in data privacy negotiations with the EU, the Department of Commerce ("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 Richard 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.[230] 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 EU 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, the Department of Commerce issued draft "Safe Harbor Principles" in

---

[226] See infra note ___ and accompanying text.

[227] The FTC initiated these workshops in April 1995. See Internet Privacy Before the Subcommittee on Courts and Intellectual Property of the House Committee on the Judiciary (1998) <http://www.ftc.gov/os/1998/9803/privacy.htm>.

[228] See, e.g., FTC Staff Report on "Public Workshop on the Global Information Infrastructure," (Dec. 1996) <http://www.ftc.gov/reports/privacy/privacy1.htm> (examining privacy online); see also FTC July 1999 Report on Self-Regulation, supra note ___.

[229] See Separate Statement of Commissioner Orson Swindle, annexed to FTC July 1999 Report on Self-Regulation, supra note ____. 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." See Prepared Statement of the Federal Trade Commission on "Consumer Privacy on the World Wide Web,"before the Subcommittee on Telecommunications, Trade and Consumer Protection of the Committee on Commerce, United States House of Representatives, July 21, 1998 <http://www.ftc.gov/os/1998/9807/privac98.htm> (presented by Chairman Robert Pitofsky).

[230] See Business Leaders to Propose Charter to Address Problems of Internet Regulation, 15 Int'l Trade Rep. (BNA) 1179 (July 8, 1998).

November 1998, within a month of the Directive becoming effective.[231] Commerce's draft guidelines were made subject to public comment for a fifteen day period, although they were not published in the Federal Register.[232] Following internal consultations with industry and intensive external negotiations with EU authorities over the substance of the principles, the Department of Commerce issued a revised set of Safe Harbor Principles on April 19, 1999.[233] The proposed principles, as revised by Commerce through September 1, 1999, 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 parties to which it discloses the information, and the... means... for limiting its use and disclosure"; [234]

(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

---

[231] The DOC's initial draft Safe Harbor Principles are available on the DOC Web Site. See <http://www.ita.doc.gov/ecom/menu.htm#Safe> (visited January 12, 1999). See also EU States Endorse Standstill with U.S. on Transfers of Data During Privacy Talks, 15 Int'l Trade Rep. (BNA) 1780 (Oct. 28, 1998).

[232] 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 on the Department of Commerce, Draft Safe Harbor Principles, <http://www.ita.doc.gov/ecom/com1abc.htm#silbergeld> (visited Jan. 13, 1999). 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 the DOC "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." See id.; see also Comments of the ACLU on the Department of Commerce, Draft Safe Harbor Principles, <http://www.ita.doc.gov/ecom/com2abc.htm#aclu> (visited Jan. 13, 1999).

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

[234] The first Safe Harbor Principle provides:

> NOTICE: An organization must inform individuals about the purposes for which it collects information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or discloses it to a third party.

April 1999 Safe Harbor Principles, supra note ___.

in) choice";[235]
(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";[236]
(iv) "Security": Organizations must take reasonable measures to assure the reliability of information and protect it from disclosure or loss;[237]
(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";[238]
(vi) "Access": Organizations must grant individuals "[reasonable] access to personal information held about them and the opportunity to have it corrected;[239]

---

[235] The second Safe Harbor Principle provides:

> CHOICE: An organization must offer individuals the opportunity to choose (opt out) whether and how personal information they provide is used or disclosed to third parties (where such use is incompatible with the purpose for which it was originally collected or with any other purpose disclosed to the individual in a notice). They must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise this option. For 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.(4)

April 1999 Safe Harbor Principles, supra note ___.

[236] The third Safe Harbor Principle provides:

> ONWARD TRANSFER: An organization may only disclose personal information to third parties consistent with the principles of notice and choice. Where an organization has not provided choice because a use is compatible with the purpose for which the data was originally collected or which was disclosed in a notice and the organization wishes to transfer the data to a third party, it may do so if it first either ascertains that the third party subscribes to the safe harbor principles or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant safe harbor principles.(5)

April 1999 Safe Harbor Principles, supra note ___.

[237] The fourth Safe Harbor Principle provides:

> SECURITY: Organizations creating, maintaining, using or disseminating personal information must take reasonable measures to assure its reliability for its intended use and reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction.

April 1999 Safe Harbor Principles, supra note ___.

[238] The fifth Safe Harbor Principle provides:

> DATA INTEGRITY: Consistent with these principles, an organization may only process personal information relevant to the purposes for which it has been gathered. To the extent necessary for those purposes, an organization should take reasonable steps to ensure that data is accurate, complete, and current.

April 1999 Safe Harbor Principles, supra note ___.

[239] The sixth Safe Harbor Principle provides:

> ACCESS: Individuals must have [reasonable] access to personal information about them that an organization holds and be able to correct or amend that information where it is inaccurate. [Reasonableness of access depends on the nature and sensitivity of the information collected, its

(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."[240]

The drafting, reception of public comments and revisions of these "principles" is analogous to negotiated rule making under U.S. administrative law.[241] Yet it is a negotiated rule making 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.[242]

> intended uses, and the expense and difficulty of providing the individual with access to the information.](6)

April 1999 Safe Harbor Principles, supra note ___.

[240] The seventh Safe Harbor Principle provides:

> ENFORCEMENT: Effective privacy protection must include mechanisms for assuring compliance with the safe harbor principles, recourse for individuals to whom the data relate affected by non-compliance with the principles, and consequences for the organization when the principles are not followed. At a minimum, such mechanisms must include (a) readily available and affordable independent recourse mechanisms by which an individual's complaints and disputes can be investigated and resolved and damages awarded where the applicable law or private sector initiatives so provide; (b) follow up procedures for verifying that the attestations and assertions businesses make about their privacy practices are true and that privacy practices have been implemented as presented; and (c) obligations to remedy problems arising out of failure to comply with these principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations.

April 1999 Safe Harbor Principles, supra note ___.

[241] For discussions of negotiated rule making, see Philip Harter, Negotiating Regulations: A Cure for Malaise, 71 GEO. L.J. 1 (1982); Lawrence Susskind and Gerard McMahon, The Theory and Practice of Negotiated Rulemaking, 3 YALE J. ON REG. 133 (1985); Henry Perritt, Negotiated Rulemaking before Federal Agencies: Evaluation of Recommendations by the Administrative Conference of the United States, 74 GEO. L.J. 1625 (1986). For a critique of negotiated rule making, see William Funk, When Smoke Gets in your Eyes: Regulatory Negotiation and the Public Interest--EPA's Woodstove Standards, 8 ENVTL. L. 55 (1988).

[242] 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 Compa & Tashia Hinchcliffe Carricarrere, 1996 Private Labor Rights Enforcement Through Corporate Codes of Conduct, in LANCE COMPA & STEPHEN DIAMOND, HUMAN RIGHTS, LABOR RIGHTS, AND INTERNATIONAL TRADE (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-- from production to disposal. See, e.g., 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, 245 (1994). Shareholder activists pressure corporate groups

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."[243] The FTC has, in fact, already brought two enforcement actions in the last year.[244] Were there no 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 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 EU, however, has so far rejected the United States' proposals as inadequate.[245] While the outcome of U.S.-EU negotiations may not

---

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)). International organizations, such as ISO (the international standard organization), 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 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 (1999). 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 can potentially 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.

[243] See Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45(a)(6).

[244] In 1998, the brought an enforcement action against Geocities, which has "one of the most popular sites on the Web," for having suggested that GeoCities was collecting personal information, when the personal information was rather going directly to third parties. GeoCities agreed to settle this pursuant to a consent order finalized in February 1999. See In re Geocities, Docket No. C-3850 (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 a second enforcement action 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 subject for comments. See In re Liberty Financial Companies, File No. 982 3522 (May 6, 1999) (releasing a 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 Report on Self-Regulation, supra note..., at 16, n. 16.

[245] See, e.g., EU, U.S. Will Not Sign Data Privacy Pact at Upcoming Bonn Summit, Officials Say, Int'l Bus. & Fin. Daily (BNA) (June 2, 1999). Grounds on which EU authorities initially focused were inadequate provisions concerning individual access to records, prior notification of transfers of personal information to third parties and effective enforcement. Blackmer March 27 Interview, supra note ___. 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 ___.

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, 21 June 1999,

satisfy U.S. data privacy advocates, at a minimum, the Directive has provided leverage to press large U.S. businesses to adopt fair information practices that they otherwise would ignore.

The Directive has not only shaped U.S. baseline rules, it has spurred the creation of new institutional developments. The Department of Commerce has consistently critiqued the European scheme of empowering national supervisory authorities as an anachronistic reliance on big government, opposed to the United State's decentralized approach.[246] Yet under pressure from the 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.[247] While the creation of a single position is far from 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.[248] It was the EU's pressure which 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 Directive has altered the domestic context. It has bolstered public pressure for regulatory reform. It has incited state and federal officials (from the more consumer-friendly FTC to the more business-friendly DOC) to press businesses to develop enhanced private data protection schemes. It has created new 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

---

<http://www.europa.eu.int/comm/dg15/en/media/dataprot/news/summit.htm>.

[246] See infra note __.

[247] 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 ___. 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, a chapter to appear in VISIONS FOR PRIVACY IN THE 21ST CENTURY (Colin Bennet & Rebecca Grant eds.) (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).

[248] See Clinton Administration to Name Swire as OMB's Privacy Policy Coordinator, supra note__. While it is impossible to separate domestic factors from the Directive's pressures in the analysis of the new position, certainly the Directive and the ongoing negotiations with the EU have played an important role, as indicated by the job's portfolio.

of foreign regulators-- the European Commission and EU member state authorities.[249]

B. An Opportunity for Public Advocacy Groups and Privacy Service Providers. Data privacy advocates have attempted to use the Directive to challenge lax business practices in the United States. Beginning in the fall of 1998 when the 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,[250] among other journals read by business representatives and policy makers. Numerous symposia were held which addressed the "adequacy" of U.S. data protection practices in light of the Directive.[251] The Directive and the publicity it received drew attention to data privacy advocates and provided leverage for their efforts.[252] It has also provided free advertising for developing service industries, including legal counsel, which profit from assisting firms comply with EU requirements.

1. The Role of Privacy Advocates. Privacy advocates play an important role because they are "repeat players" in on-going negotiations over U.S. data privacy rules.[253] They are, in this way, different than individuals who transact with companies on an ad hoc basis and commence (possibly) "one-shot" disputes when they feel their privacy interests are seriously impinged. As repeat players, privacy advocates have larger time horizons in which to implement strategies to maximize gain. As

---

[249] Similarly, the European Commission acts within the shadow of other bodies. The Commission is accountable to both EU member state representatives (from below) and the World Trade Organization (from above). 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).

[250] See European Law Aims to Protect Privacy of Personal Data, supra note ___ (N.Y.Times); Elizabeth Weise, EU Privacy Paradigm May Lock U.S. Frims Out, USA TODAY, Oct. 21. 1998, at 6D; Robert O"Harrow, 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; EU and US Seek Solution, FIN. TIMES, Oct. 27, 1998, at 4.

[251] The 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 Nov. 5-6 in San Francisco and Nov. 16-17 in New York City, sponsored by The American Lawyer, The National Law Journal, The Recorder and New York Law Journal. The author was part of one such symposia held in Madison, Wisconsin on November 14, 1998, portions of which were later broadcast on Wisconsin Public Radio.

[252] Even Congressional representatives have met with European officials over data privacy legislation. See Goodlatte Calls on Administration to Begin Talks with Congress on Data Privacy Issues, 16 BNA INT'L TRADE REP. 502 (March 24, 1999) (noting remarks of Robert Goodlatte, co-chair of Congress' "Internet Caucus" concerning his meeting with John Mogg, director-general of the European Commission for Internal and Financial Affairs who leads the EU delegation on data privacy discussions, as well as other meetings involving Congressional delegates and EU officials, both in Washington and Brussels).

[253] 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).

repeat players, they have an incentive to expend resource to influence the making of relevant data privacy rules, whether through threatened product boycotts, legislative lobbying or judicial challenge.

Privacy advocates jumped on the opportunity to pressure 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 used the opportunity to criticize Commerce for focusing on protecting U.S. businesses from EU privacy requirements, instead of protecting U.S. consumers from business exploitation of private information.[254] They objected to Commerce's advocacy of self-regulatory mechanisms, responding that "self-regulation has been a lot of smoke and mirrors."[255] In line with the Directive, they maintained that the United States too needs "a comprehensive approach to privacy protection,"[256] not a fragmented scandal-specific one.

For privacy advocates, individuals must be able to control the commercial use of personal information about them. They critiqued the Safe Harbor Principles for their loopholes and noted ways these could be closed. On the issue of "Choice," 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 an "opt in" right so that personal data may not be used or transferred unless the individual affirmatively consents.[257] On the issue of "Access," advocates asserted that an individual's right must cover all information collected about her, and not just "sensitive" information (which was initially left undefined).[258] On "Enforcement," they contended that business data processing practices must be "independently" monitored, and that so-called "self-certification" by business is a travesty.[259] Some advocates called for the creation of a new U.S. privacy protection agency, analogous to the supervisory authorities mandated by the EU.[260]

---

[254] See, e.g., Comments of Mark Silbergeld, supra note ___ (comments submitted on behalf of a number of privacy advocate groups).

[255] See Jeri Clausing, Internet Commerce Study Stresses Self-Regulation, N.Y. TIMES Nov. 30, 1998 (quoting Marc Rotenberg of EPIC).

[256] See Comments of Mark Silbergeld, supra note ___.

[257] Privacy activists also advocate limiting the collection of information to only that which is necessary for purposes consented to by the individual. See id.(emphasis added).

[258] In the DOCs revised draft guidelines on April 1999, the draft's implication that access only applied to sensitive information was removed. See infra note__ and accompanying text.

[259] 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.

[260] See id. Others advocates acknowledged that this may be unrealistic given current attitudes in Congress. Telephone Interview with Deirdre Mulligan, Center for Democracy and Technology (Dec. 8, 1998). Given that Congress is currently considering closing existing agencies, it is unlikely to authorize funds for a new one. On the other hand, a

Yet even though privacy advocates critique 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.[261] The Directive induces the creation of new legal tools within the United States which 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"),[262] one of the leading privacy advocates in the United States (though consisting of only three attorneys), works in association with Privacy International, a group based in London, England.[263] While EPIC has lobbied Congress for greater privacy protection, commented on proposed DOC guidelines, and generally tried to follow U.S. business practices, Privacy International has announced that it will monitor data transmissions of major U.S. multinational companies and ensure the Directive is enforced.[264] Through their coordination, privacy advocates enhance the Directive's impact on U.S. business practice.

The U.S. and EU recently facilitated the formation of a Transatlantic Consumer Dialogue (TACD), consisting of consumer advocates on both sides of the Atlantic.[265] The TACD held its first

---

division within the FTC, DOC or other agency could be made responsible for overseeing and providing consumer support on all data privacy issues. See also note__ and accompanying text (concerning the creation of a new position in the executive branch to coordinate U.S. domestic policy on privacy protection).

[261] For example, EPIC conducted and published its own review of web site data processing practices a year before the FTC conducted and published its own critique. EPIC's report is entitled Surfer Beware: Personal Privacy and the Internet (June 1997) and can be obtained from EPIC's web site (see supra note__).

[262] EPIC's website contains the following description of the organization:

> EPIC is a public interest research center in Washington, D.C. It was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values. EPIC is a project of the Fund for Constitutional Government. EPIC works in association with Privacy International, an international human rights group based in London, UK and is also a member of the Global Internet Liberty Campaign, the Internet Free Expression Alliance and the Internet Privacy Coalition.

<http://www.epic.org/#about> (visited Jan. 11, 1999).

[263] See <http://www.privacy.org/pi/> (visited Jan. 11, 1999). EPIC and Privacy International have organized national conferences on data privacy issues since 1994 (comments of Marc Rotenberg of EPIC on an earlier draft).

[264] Privacy International specifically mentioned 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." See Noah Shachtman, EU Privacy Law is Awkward for US, WIRED, Oct. 23, 1998. See also, Stephen Baker, Europe's Privacy Cops, BUS. WK., Nov. 2, 1998.

[265] The Transatlantic Consumer Dialogue now has offices in London, bringing together advocates on both sides of the Atlantic to monitor developments and provide input on a host of consumer-related issues. It has a Web sit available

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 forthwith passed a resolution urging "the European Commission and the Member States to reject the [United States'] Safe Harbor Proposal."[266] U.S. consumer advocates knew that EU member state and European Commission 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 Directive not only permits privacy advocates to more effectively challenge lax business practices, it also increases the demand for their 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, pursuant to 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 "Privacy and American Business," and works with multinational companies in drafting codes of conduct to meet the Directive's requirements.[267] 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. 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.[268] Similarly, Alan Westin, provides consulting services to the Better Business Bureau OnLine on its new privacy seal program.[269] The 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 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

---

at <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. Interview with Deirdre Mulligan, supra note__.

[266] The Resolution on "Safe Harbor and International Convention on Privacy Protection" adopted by the TACD Electronic Commerce Working Group is available at <http://www.tacd.org/meeting2/electronic.html#safe>

[267] The Center is based in Hackensack, New Jersey. See the Privacy and American Business website at <http://www.pandab.org>; see also NONE OF YOUR BUSINESS, supra note ___, at 170.

[268] The Electronic Frontier Foundation's web site is located at http://www/eff.org. The TRUSTe web site is at <http://www.truste.org> (visited Jan. 12, 1999). The latter organization was initially named eTRUST.

[269] Telephone interview with Gary Laden, Director BBB OnLine Privacy Program, April 21, 1999. See also BBB OnLine Privacy Program Created to Enhance User Trust on the Internet, a press release obtained from the Better Business Bureau web site at http:/www.bbb.org/alerts/BOLprivacy.html.

as a provider of timely, reliable certification services under its new program BBB OnLine.[270] 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."[271] TRUSTe similarly works with major accounting firms, such as Coopers & Lybrand and KPMG, who are paid to review information processing practices of firms displaying the TRUSTe seal.[272] To drum up business, TRUSTe consistently refers to the Directive, noting how TRUSTe looks "for ways to incorporate 'adequacy' as defined in the Directive into our program"[273] and "bridge the Internet privacy gap for companies who do business in Europe or are thinking of forging an international presence."[274] U.S. businesses join these programs with an eye on EU (not just U.S.) regulators.[275]

Accountants, through their national organization the American Institute of Certified Public

---

[270] In its comments on the draft Safe Harbor Principles, contrary to other businesses, the Council for Better Business Bureaus declared that "neither self-certification of compliance by a business, nor routine, mandatory CPA firm audits are appropriate or workable requirements." It contended that only reviews by independent organizations, such as itself, are dependable See Comments of the Council of Better Business Bureaus on the Department of Commerce, Draft Safe Harbor Principles, <http://www.ita.doc.gov/ecom/com1abc.htm#bbb> (visited Jan. 13, 1998). The Council is the umbrella organization for 135 U.S. Better Business Bureaus. The Council has created a subsidiary, BBB OnLine, that started operating a "Privacy Seal Program" in March 1999. Though funded by major corporations, the Council operates with a degree of independence. Its goal is to foster goodwill between business and consumers and thereby 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 for businesses to litigation. Nonetheless, BBB OnLine's auditing of company practices and 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 is "not binding on the consumer, so consumers will be free to exercise available judicial remedies in addition to the remedies offered by BBB OnLine." Testimony of Russell Bodoff, Chief Operating Officer of BBB OnLine before the U.S. Senate in late April 1999, available at http://www.BBBOnLine.org/about/senate_testimony.html.

[271] Id.

[272] See TRUSTe Program Principles, <http://www.truste.org/webpublishers/pub_principles.html> (visited Jan. 12, 1999). See also, eTrust Launches Pilot Program (Dec. 20, 1996), at http://www.eff.org/effector/effect09.15.

[273] See e.g. Anne Jennings, The European Union Data Directive: What Does It Really Mean for your Business?, Truste Reporter (fall 1998), at <http://www.truste.org/newsletter.fall98.html> (describing the effects the Directive will have on U.S. policy).

[274] EU Directive-- Bridging the Privacy Gap with Europe, Truste Reporter (summer 1997), at http://www.truste.org/newsletter.summer97.html..

[275] For example, it was reported that the "American Electronics Association agreed to promote use of the BBBOnline privacy seal among its 3000 high-tech member companies in a move likely to ease tensions on the current dispute between the United States and the European Union over data privacy." EU Commissioner for DGXV, John Mogg had stated a month earlier in Washington that an effective BBBOnline system could "greatly contribute to the resolution of a number of our concerns." See Gary Yerkey, AEA will Promote Corporate Use of BBBOnline to Ensure Privacy on Internet, 16 Int'l Trade Rep. 627 (BNA) (April 14, 1999).

Accountants (AICPA), have created an analogous program entitled CPA WebTrust, under which they propose to evaluate web sites, conduct audits of firm's privacy practices and recertify participating firms every three months.[276] The 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 Web Trust guidelines, formulated in September 1997, focused more on the security of payment mechanisms to promote e-commerce than on privacy protection.[277] The initial guidelines have would merely confirmed that a certified company publishes a privacy policy, whatever that policy may be.[278] Since then, however, privacy protection has become a central part of the Web Trust 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."[279] However, through the threat of data transfer restrictions and foreign litigation under the Directive, the EU 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 to be certified.

The 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 Directive and U.S. privacy legislation,[280] write memoranda on privacy issues which they distribute within firms, and generally increase firm awareness of privacy issues. In formulating and overseeing the implementation of company policies, they affect internal business culture, fostering company compliance with existing legal requirements and norms, including foreign ones.[281]

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

---

[276] See CPA WebTrust Seal means greater security, at http://www.cpawebtrust.org/shared/eval/eval.html (visited April 21, 1999).

[277] E-mail exchange with Anthony Pugliese, who is responsible for privacy issues at AICPA (Aug. 8, 1999).

[278] Telephone Interview with Linda Dunbar, Public Relations Director of AICPA (May 4, 1999).

[279] Telephone Interview with Paola Benassi, Product Operations Manager of TRUSTe, April 21, 1999.

[280] At a symposia on data privacy organized by Westin's group, the Center for Social and Legal Research, in the fall of 1998, allegedly over 170 people, primarily from corporate human resource departments, attended. Interview with Peter Swire, now White House Chief Counsel for Privacy in Washington D.C., March 26, 1999.

[281] See Lauren Edelman, Steven Abraham and Howard Erlanger, Professional Construction of Law: The Inflated Threat of Wrongful Discharge, 26 L. & SOC'Y REV. 47 (1992). In their study of wrongful discharge law, they conclude that "the 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." This has resulted in more labor friendly company discharge policies. Id. at 53.

the law seriously.[282] 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 Directive, its substantive requirements and sanctions, including the draconian 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 Directive's legal provisions.[283] Their memoranda highlight why U.S. businesses must pay close attention to the Directive's requirements.[284] At symposia, they market contractual precautions which can be drafted and implemented to reduce the risk of European intervention.[285] Ironically, in providing legal counsel to their clients on the 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, a dispute must arise, requiring two sides. For example, unlike in the United States, there is little practice of environmental law in continental Europe because there is little environmental litigation.[286] The Directive, through its threat of restrictions on transatlantic data transfers, creates and reinforces that other side within the United States. The 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.

---

[282] In the field of wrongful discharge law, it has been noted how "employer'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." See Lauren Edelman, Steven Abraham and Howard Erlanger, Professional Construction of Law, supra note __.

[283] For example, Mason's Solicitors published a Handbook on Cost Effective Compliance with Directive 95/46/EC. See supra note ___. The author has also received unsolicited copies of law firm manuals on the EU Directive. Examples of articles by lawyers include, [Beck & Arad, LLP (New York City law firm), EU and U.S. Data Protection Law–and Soon the Twain Shall Meet, THE 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) (noting that Zinger is a lawyer at Baker McKenzie's San Francisco Office) (on file). As a lawyer in Paris, France, the author helped prepare memoranda for U.S. and European clients on data privacy issues in the mid-1990s, just before the EU Directive was signed.

[284] 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 at the symposia of Scott Blackmer of the law firm Wilmer, Cutler & Pickering in Washington D.C.).

[285]Id. (noting "a panel of attorneys recommends that companies use contracts to address security and access to help ensure that data flows continue.")

[286] This was highlighted to the author in a conversation with the French sociologis Yves Dezalay, confirming the author's own experience in private legal practice in Paris, France.

The Directive also stimulates the development of new technology which protects privacy interests. NCR, the information technology company, offers new database software that facilitates "a consumer's right of access to information,"[287] 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 comply with EU and U.S. governmental requirements and self-regulatory objectives. The Directive's threat to business concerns stimulate 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.[288]

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

1. Business Organization, Protest and Development of Codes. U.S. businesses have vehemently objected to the EU's demands. They work independently and join sector-specific and cross-sectoral 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.[289] They spend large sums on lobbying because they calculate that new data privacy legislation will significantly raise business compliance, transaction, operational and opportunity costs.[290]

Businesses from a wide variety of business sectors presented detailed comments to Commerce's Safe Harbor Principles, reflecting the Directive's broad impact on U.S. commercial

---

[287] The software permits users to "manage and audit a consumer's choice to opt-in or opt-out of personal data collection." See NCR Announces Consumer Data Privacy Initiative; Opt-out/Opt-in Features to be built into Company Software, PR NEWSWIRE, Oct 5, 1998.

[288] See supra notes__. A firm named PrivaSeek Inc. recently offered software "that enables users to control the level of information they pass on to websites." See PrivaSeek Unveils Personal 1.1, Network Briefing ISSN 1360-1369 (August 12, 1999) available on Westlaw.

[289] The Online Privacy Alliance has hired forrmer 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.

[290] See supra Part II.C., notes ___ and accompanying text.

interests.[291] These sectors included the direct marketing,[292] retail,[293] publications,[294] insurance,[295] financial,[296] credit,[297] pharmaceutical and health industries.[298] The information technology industry

---

[291] These businesses had to react quickly, being granted only fifteen days in November 1998 to submit their comments. See Letter from David Aaron, Undersecretary of Commerce for International Trade, to Industry Representatives (Nov. 4, 1998) <http://www.ita.doc.gov/ecom/menu.htm>.

[292] 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, <http://www.ita.doc.gov/ecom/com2abc.htm#dma> (visited Apr. 4, 1999). The DMA is very active on this issue. In a letter submitted to the Department of Commerce, H. Robert Wientzen, the President and CEO of the Direct Marketing Association, 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.

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

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

[295] 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 Direct Marketing Association on the Department of Commerce, Draft Safe Harbor Principles, <http://www.ita.doc.gov/ecom/com2abc.htm#dma> (visited Apr. 4, 1999); Comments of The Direct Marketing Association on the Department of Commerce, Draft Safe Harbor Principles, <http://www.ita.doc.gov/ecom/com2abc.htm#dma> (visited Apr. 4, 1999); Comments of The Direct Marketing Association on the Department of Commerce, Draft Safe Harbor Principles, <http://www.ita.doc.gov/ecom/com5abc.htm#lexis> (visited Apr. 4, 1999).

[296] 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, <http://www.ita.doc.gov/ecom/com4abc.htm#citi> (visited Jan. 13, 1999); Comments of The American Banker's Association on the Department of Commerce, Draft Safe Harbor Principles, <http://www.ita.doc.gov/ecom/comabc.htm#aba> (visited Apr. 4, 1999); Comments of The Securities Industry Association on the Department of Commerce, Draft Safe Harbor Principles, <http://www.ita.doc.gov/ecom/com4abc.htm#sia> (visited Apr. 4, 1999); Comments of Dun & Bradstreet on the Department of Commerce, Draft Safe Harbor Principles, <http://www.ita.doc.gov/ecom/com2abc.htm#d&b> (visited

was the most active, both through individual company and collective submissions by industry organizations.[299]

Because businesses have high per capita stakes,[300] 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.[301] Large multinational businesses

---

Apr. 4, 1999).

[297] 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, <http://www.ita.doc.gov/ecom/com2abc.htm#dma> (visited Apr. 4, 1999); Comments of The Associated Credit Bureaus on the Department of Commerce, Draft Safe Harbor Principles, <http://www.ita.doc.gov/ecom/com2abc.htm#dma> (visited Apr. 4, 1999).

[298] 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, <http://www.ita.doc.gov/ecom/com4abc.htm#phrma> (visited Apr. 4, 1999); Comments of The Health Industry Manufacturers Association on the Department of Commerce, Draft Safe Harbor Principles, <http://www.ita.doc.gov/ecom/com1abc.htm#health> (visited Apr. 4, 1999); Comments of Eli Lilly and Company on the Department of Commerce, Draft Safe Harbor Principles, <http://www.ita.doc.gov/ecom/com5abc.htm#eli> (visited Apr. 4, 1999); Comments of Novartis on the Department of Commerce, Draft Safe Harbor Principles, <http://www.ita.doc.gov/ecom/com3abc.htm#novartis> (visited Apr. 4, 1999).

[299] Individual companies submitting comments included America Online, Netscape, Yahoo, Bell Atlantic, IBM and Compaq. See Comments of America Online on the Department of Commerce, Draft Safe Harbor Principles, <http://www.ita.doc.gov/ecom/com5abc.htm#aol> (visited Apr. 4, 1999); Comments of Netscape on the Department of Commerce, Draft Safe Harbor Principles, <http://www.ita.doc.gov/ecom/com1abc.htm#netscape> (visited Apr. 4, 1999); Comments of Yahoo on the Department of Commerce, Draft Safe Harbor Principles, <http://www.ita.doc.gov/ecom/com1abc.htm#yahoo> (visited Apr. 4, 1999); Comments of Bell Atlantic on the Department of Commerce, Draft Safe Harbor Principles, <http://www.ita.doc.gov/ecom/com1abc.htm#bell> (visited Apr. 4, 1999); Comments of IBM on the Department of Commerce, Draft Safe Harbor Principles, <http://www.ita.doc.gov/ecom/com2abc.htm#ibm> (visited Apr. 4, 1999); Comments of Compaq on the Department of Commerce, Draft Safe Harbor Principles, <http://www.ita.doc.gov/ecom/com2abc.htm#compaq> (visited Apr. 4, 1999). 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 on the Department of Commerce, Draft Safe Harbor Principles, <http://www.ita.doc.gov/ecom/com1abc.htm#iti> (visited Apr. 4, 1999); Comments of the Information Technology Association of America on the Department of Commerce, Draft Safe Harbor Principles, <http://www.ita.doc.gov/ecom/com1abc.htm#itaa> (visited Apr. 4, 1999); Comments of the Information Industry Association on the Department of Commerce, Draft Safe Harbor Principles, <http://www.ita.doc.gov/ecom/com1abc.htm#iia> (visited Apr. 4, 1999).

[300] See supra note__ and accompanying text.

[301] Cross-sectoral associations which 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, <http://www.ita.doc.gov/ecom/com2abc.htm#uschamber> (visited Apr.

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.[302]

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 plethora of data privacy protection "principles," "guidelines," model contracts, and other schemes. The Paris-based International Chamber of Commerce has developed model contract provisions.[303] The Direct Marketing Association (DMA) has created "Guidelines for Personal Information Protection."[304] 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.[305] Companies such as Intel, Microsoft and Disney have announced that "they will forgo

---

4, 1999); Comments of the U.S. Council on International Business on the Department of Commerce, Draft Safe Harbor Principles, <http://www.ita.doc.gov/ecom/com1abc.htm#uscib> (visited Apr. 4, 1999); Comments of the Coalition of Service Industries on the Department of Commerce, Draft Safe Harbor Principles, <http://www.ita.doc.gov/ecom/com3abc.htm#csi> (visited Apr. 4, 1999); Comments of the Online Privacy Alliance on the Department of Commerce, Draft Safe Harbor Principles, <http://www.ita.doc.gov/ecom/com2abc.htm#opa> (visited Apr. 4, 1999).

[302] See supra note___. The TABD, like other business organizations, supports self-regulatory mechanisms through the development of model private contractual provisions to address privacy concerns arising from trans-border 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, <http://www.tabd.org/resources/content/apr98.html> (visited Jan. 12, 1999).

[303] International Chamber of Commerce. ICC Model Clauses for Use in Contracts Involving Transborder Data Flows (1998). See Weidlich, supra note ___.

[304] The DMA recommends these to its members, which include most direct marketing companies. See Setting Standards, supra note ___, at 510.

[305] A group of fifty one major businesses and business associations affected by data privacy issues, formed the Online Privacy Alliance. A month later, the Alliance proposed guidelines for a self-regulatory approach to data privacy protection designed to overcome the criticism of current self-regulatory schemes. 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 to first 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 and 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, July 21, 1998, at

advertising on sites that do not adhere to fair information practices."[306] Numerous other businesses and associations have adopted or are developing privacy codes, guidelines and other measures.[307] The timing of these multiple efforts in conjunction with the Directive's coming into force in October 1998 is no coincidence. These self-regulatory schemes are the Directive's bastard offshoots-- the unplanned offspring of the Directive's encounter with U.S. business.[308] The 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.[309] U.S.-EU negotiations over Safe Harbor Principles help determine self-regulation's contours.

2. Caught in a Bind: Business' Support and Wariness of Commerce's Privacy Approach. Business groups are caught in a bind by Commerce's Safe Harbor Principles. On the one hand, they strongly support Commerce's efforts to negotiate a "safe harbor" with EU authorities which 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,[310] and (ii) to ensure that EU authorities are bound

---

<http://www.privacyalliance.org/resources/Varney_July_21.pdf>. For the Online Privacy Alliances's guidelines on enforcement issues, see <http://www.privacyalliance.org/resources/enforcement.shtml> (visited Jan. 12, 1999).

[306] Id. at 12-13.

[307] For example, the International Digital Software Association (IDSA), which represents businesses which sell video and computer games, has adopted privacy guidelines. See Comments of IDSA on the Department of Commerce, Draft Safe Harbor Principles, <http://www.ita.doc.gov/ecom/com1abc.htm#idsa> (visited Jan. 13. 1999). IDSA claims that its guidelines "closely conform" to the DOC's draft Safe Harbor Principles. See also the "Privacy Principles" of the IBAA, the Bankers Roundtable, the American Bankers Association, and the Consumer Bankers Association, at <http://www.ftc.gov/reports/privacy3/comments/012b.htm>; see also private sector guidelines referred to in Comments of The Information Technology Association of America (ITAA) on the Department of Commerce, Draft Safe Harbor Principles, <http://www.ita.doc.gov/ecom/com1abc.htm#itaa> (visited Jan. 13, 1999).

[308] 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 Directive's proponents.

[309] 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 ___, at 6. The FTC cites two studies by Professor Mary Culnan of the McDonough School of Business of Georgetown, available at <http://www.msb.edu/faculty/culnanm/gippshome.html>

In the process of developing guidelines, businesses are also pressured to make them more stringent. The Online Privacy Alliance hired former FTC Commissioner Christine Varney, who has openly criticized self-regulatory approaches for lacking "a reliable enforcement mechanism, a specific recourse for people who feel that information has been collected or used without their consent." See Christine Varney, You Call this Self-Regulation?, WIRED, June 1998.

[310] 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 Companies on the Department of Commerce, Draft Safe Harbor Principles,

by the Principles and cannot restrict data transfers on other grounds.

A primary reason U.S. businesses are more wary of the 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.[311] Individuals are more likely to bring suit against companies in the United States, the costs of litigation (and particularly 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 Untied 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.[312] Thus, U.S. businesses' adverse reactions to the Directive are not solely on account of the Directive's contents, but also of businesses' experience of U.S. legal culture. Even if not formally stated, a large part 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 retain maximum autonomy to profit from the use of personal data. Businesses thus

---

<http://www.ita.doc.gov/ecom/com1abc.htm#mcgraw> (visited Jan. 13, 1999). Others argue certain pharmaceutical and medical research should be excluded in order to promote the development of new health products. See Comments of Eli Lilly Company on the Department of Commerce, Draft Safe Harbor Principles, <http://www.ita.doc.gov/ecom/com5abc.htm#eli> (visited Jan. 13, 1999), see also Comments of the Pharmaceutical Research and Manufacturers of America on the Department of Commerce, Draft Safe Harbor Principles <http://www.ita.doc.gov/ecom/com4abc.htm#phrma> (visited Jan. 13, 1999); Comments of the Health Industry Manufacturers Association on the Department of Commerce, Draft Safe Harbor Principles <http://www.ita.doc.gov/ecom/com1abc.htm#health> (visited Jan. 13, 1999).

[311] For a presentation of the costs of U.S. legal culture, what Kagan calls "adversarial legalism," see Kagan, supra note__. 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 more affected 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.

[312] This is particularly true in continental Europe. In large part, this reflects a systemic difference in U.S. and European systems of governance. The U.S. 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, e.g., Katzenstein, supra note__(discussing German corporatism and French centralism); see also infra notes ___. In addition, the procedural rules of European legal systems provide fewer incentives for private groups to engage in socially activist litigation. Unlike in the U.S., 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 Capalli & Claudio Consolo, Class Actions for Continental Europe? A Preliminary Inquiry, 6 TEMPLE INT'L. & COMP. L.J. 217 (Fall, 1992).

critiqued each of Commerce's seven principles for unreasonably hampering business operations. A review of businesses' comments highlights how, if business had its way, the principles would be words without impact. Yet it appears businesses will largely be unsuccessful. Although privacy advocates too may be unsatisfied, Commerce's revised guidelines, published in April 1999, primarily retained or enhanced the stringency of the initial principles.[313]

On the "Notice" principle, businesses argued that the amount of information Commerce required to be provided in notices was unduly burdensome,[314] and that timing requirements for providing notice should be loosened.[315] Although Commerce took some comments into account, the core of the principle remains. 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.[316] They insisted that "opt out" rights should not apply to "public" or "proprietary" information, or information needed to combat consumer fraud, even if "sensitive."[317] However, Commerce's revised guidelines instead eliminated

---

[313] See FTC April 1999 Guidelines, supra note ____.

[314] See, e.g., Comments of the Direct Market Association, on the Department of Commerce, Draft Safe Harbor Principles, <http://www.ita.doc.gov/ecom/com2abc.htm#dma> (visited Jan. 13, 1999); Comments of the Magazine Publishers of America on the Department of Commerce, Draft Safe Harbor Principles, <http://www.ita.doc.gov/ecom/com2abc.htm#mpa> (visited Jan. 13, 1999) (proposing that the current U.S. regime should be maintained); and Comments of The Information Technology Association of America, supra note ___. The DMA states that providing consumers with an opt-out right is sufficient so that there should be no requirement that the potential type of recipients (such as direct marketers) be notified to consumers. Similarly the Information Technology Association of America wishes to limit the information which must be provided concerning how they collect information (claiming this is proprietary) and to whom they will disclose it.

[315] In particular, they maintained that businesses 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 the Direct Market Association, supra note ___; Comments of the National Retail Federation on the Department of Commerce, Draft Safe Harbor Principles <http://www.ita.doc.gov/ecom/com2abc.htm#nrf> (visited Jan. 13, 1999); Comments of Time Warner, Inc.,on the Department of Commerce, Draft Safe Harbor Principles <http://www.ita.doc.gov/ecom/com1abc.htm#time> (visited Jan. 13, 1999); Comments of McGraw-Hill, supra note ___.

[316] See, e.g., Comments of The Information Technology Association of America on the Department of Commerce, Draft Safe Harbor Principles, <http://www.ita.doc.gov/ecom/com1abc.htm#itaa> (visited Jan. 13. 1998). The ITAA wishes 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). Citigroup proposes the term "informed consent" be substituted for the term "opt in." See Comments of Citigroup on the Department of Commerce, Draft Safe Harbor Principles, <http://www.ita.doc.gov/ecom/com4abc.htm#citi> (visited Jan. 13, 1999).

[317] See, e.g., Comments of the American Council of Life Insurance on the Department of Commerce, Draft Safe Harbor Principles, <http://www.ita.doc.gov/ecom/com3abc.htm#acli> (visited Jan. 13, 1999); Comments of the National Fraud Center on the Department of Commerce, Draft Safe Harbor Principles, <http://www.ita.doc.gov/ecom/com1abc.htm#national> (visited Jan. 13, 1999); and Comments of Stone Investment, Inc., on the Department of Commerce, Draft Safe Harbor Principles, <http://www.ita.doc.gov/ecom/com1abc.htm#stone> (visited Jan. 13, 1999).

the vague qualification that the principles "do not apply to proprietary" information, retained the "opt in" choice for sensitive information, and defined the term "sensitive" broadly, taking the definition from Article 8 of the Directive.[318]

Businesses wanted the third principle, entitled "Onward Transfer," deleted and merged into the "Notice" and "Choice" provisions.[319] They did not want to risk liability for the actions of their third party transferees, contending that this would result in unreasonable secondary liability.[320] They rather wished to limit their obligations to providing notice to consumers that information may be transferred to third parties unless the consumer "opts 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.[321]

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."[322] They likewise asserted that a requirement for them to retain only

---

[318] See FTC April 1999 Guidelines, supra note__.

[319] See, e.g., Comments of America Online on the Department of Commerce, Draft Safe Harbor Principles, <http://www.ita.doc.gov/ecom/com5abc.htm#aol> (visited Jan. 13, 1999); Comments of the DMA on the Department of Commerce, Draft Safe Harbor Principles, <http://www.ita.doc.gov/ecom/com2abc.htm#dma> (visited Jan. 13. 1998) ; Comments of the Information Industry Association (IAA)on the Department of Commerce, Draft Safe Harbor Principles, <http://www.ita.doc.gov/ecom/com1abc.htm#iia> (visited Jan. 13, 1999); and Comments of the Individual Reference Services Group (IRSG) on the Department of Commerce, Draft Safe Harbor Principles, <http://www.ita.doc.gov/ecom/com1abc.htm#irsg> (visited Jan. 13, 1999).

[320] See, e.g., Comments of Netscape Communications Corporation on the Department of Commerce, Draft Safe Harbor Principles, <http://www.ita.doc.gov/ecom/com1abc.htm#netscape> (visited Jan. 13, 1999) (focusing on liability for third party transferees' behavior); Bell Atlantic on the Department of Commerce, Draft Safe Harbor Principles, <http://www.ita.doc.gov/ecom/com1abc.htm#bell> (visited Jan. 13, 1999) (discussing lack of certainty and third party transferees); Yahoo on the Department of Commerce, Draft Safe Harbor Principles, <http://www.ita.doc.gov/ecom/com1abc.htm#yahoo> (visited Jan. 13, 1999) (discussing the outward transfer and access to information); and Comments of the Information Technology Industry Council (ITIC) on the Department of Commerce, Draft Safe Harbor Principles, <http://www.ita.doc.gov/ecom/com1abc.htm#iti> (visited Jan. 13, 1999) (exhibiting concerns about third party liability, among other objections).

[321] See FTC April 1999 Guidelines, supra note__. EU authorities so far insist that all third party transferees must abide by the Safe Harbor Principles or the individual data subject must grant explicit (opt in) consent to such transfer. Commerce prefers to provide that the third party transferee may sign a separate side agreement with the transferor agreeing to abide by principles providing at least the same level of privacy protection as the Safe Harbor Principles, without any requirement of a data subject's explicit consent.

[322] See, e.g., Comments of the DMA, supra note ___; Comments of America Online, supra note ___; Comments of The Information Technology Association of America, supra note ___; Comments of The Interactive Digital Software Association on the Department of Commerce, Draft Safe Harbor Principles, <http://www.ita.doc.gov/ecom/com1abc.htm#idsa> (visited Jan. 13, 1999) (discussing differences between current

"current" and "complete" data would result in costs beyond any compensating benefit to consumers.[323] Commerce's revised guidelines concerning "Security," "Integrity" and "Access," however, apply to all information. In particular, Commerce eliminated a vague qualification that access would only be required for information derived "from non-public records." While under the Access principle, Commerce is attempting to retain a qualification that access only need be "reasonable," the EU is demanding this limitation be eliminated or more narrowly defined.[324]

As regards the key issue of "Enforcement," businesses demanded that enforcement may be permitted through "self-regulatory" mechanisms which alone would decide on the appropriate "consequences" of violations. In particular, businesses wished to exclude any private right of action before courts or administrative tribunals to sue for damages. One organization, the Information Technology Industry Council, went so far as to maintain that no reference should be made to "sanctions," "as it is unclear how sanctions provide a means for individuals to enforce privacy protection measures."[325] The Information Technology Association of America suggested that the Principles mandate "confidentiality of consumer complaints," to keep complaints out of the press.[326] In the revised guidelines, Commerce provided for no such limitations.[327]

---

self-regulation guidelines and the Safe Harbor principles); Comments of the ITIC, supra note ___; and Comments of the IRSG, supra note ___.

[323] See Comments of the DMA, supra note ____; Comments of the IIA, supra note ___; and Comments of McGraw Hill, supra note ___.

[324] See FTC April 1999 Guidelines, supra note__. In the initial Guidelines, Commerce's draft implied that the term reasonable access might signify that access would only be available for sensitive information (left undefined). This vague reference has since been eliminated.

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

[326] Comments of the ITAA, supra note ___. 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 which do not have to be "independently" monitored. See Comments of the DMA, supra note ___; Comments of the IIA, supra note ___; see also Comments of the Magazine Publishers of America on the Department of Commerce, Draft Safe Harbor Principles, <http://www.ita.doc.gov/ecom/com2abc.htm#mpa> (visited Jan. 13, 1999); Comments of McGraw Hill, supra note ___; and Comments of the ITAA, supra note ___.

[327] See Revised April 19, 1999 Guidelines, supra note__. 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 EU demands meaningful enforcement mechanisms to ensure data privacy protection, the U.S. does the same when it reviews the adequacy of foreign requirements, as in the WTO shrimp-turtle case (see Part IV.C above). Under its proposed implementing regulations of a law requiring foreign protection of endangered sea turtle species in order for shrimp to be imported into the U.S., the U.S. Department of State permits "voluntary arrangements between government and fishing industry." Nonetheless, it 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 which do not endanger sea turtles. See Notice of Proposed Guidelines for the Implementation of Section 609

Finally, in order to ensure that Safe Harbor Principles provide certainty, businesses demanded that EU 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 Directive.[328] In other words, while intra-European transfers would remain subject to the Directive, transatlantic transfers (from Europe) would only be subject to the Principles.[329] Otherwise, Safe Harbor Principles would merely increase pressure on businesses to enhance U.S. self-regulatory programs, without providing certainty vis-a-vis European regulators. Yet even if the EU 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. Yet it is European authorities that would ultimately make determinations under the Principles and decide on the consequences of any violation. The pressure on U.S. businesses to take account of potential lawsuits brought by European authorities would remain.

3. Privacy Protection Exported: 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, "While [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."[330]

U.S.-EU attempts to avoid disrupting data flows by agreeing to a definition of "adequate"

---

of Public Law 101-162 Relating to the Protection of Sea Turtles in Shrimp Trawl Fishing Operations, 64 Fed. Reg. 57,14481 (1999).

[328] See, e.g., Comments of the DMA, supra note ___; Comments of the ITAA, supra note ___; Comments of Time Warner, supra note ___; Comments of America Online, supra note ___; and Comments of Dun & Bradstreet on the Department of Commerce, Draft Safe Harbor Principles, <http://www.ita.doc.gov/ecom/com2abc.htm#d&b> (visited Jan. 13, 1999) (interpreting the principles as being independent of the Directive).

[329] Ideally, U.S. businesses would like immunity from any data privacy lawsuit brought in the EU by any EU resident so long as the business complies with the Safe Harbor Principles. See, e.g., Comments of Allstate Insurance Company on the Department of Commerce, Draft Safe Harbor Principles, <http://www.ita.doc.gov/ecom/com5abc.htm#allstate> (visited Jan. 13, 1999). See also Comments of the IRSG, supra note ___. 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 ___. The IRSG creates information data bases 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. It remains unclear, however, if EU authorities will agree to limit the rights of EU residents under the Directive to apply, in full, only to data transfers within the EU.

[330] Comments of the ITAA, supra note ___. See also Comments of the Magazine Publishers of America, supra note ___ ("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").

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."[331] The U.S. Council of Better Business Bureaus confirms, "it 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.[332] 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.[333]

While the Safe Harbor Principles do not formally apply to purely domestic data processing operations, enterprises recognize that it will be difficult for them to segregate data processing for U.S. domestic purposes. First, it will be difficult for businesses to use two sets of data privacy practices, one for EU residents (providing for greater privacy protection), and one for U.S. residents (providing for less).[334] Business data bases will often include information about EU and U.S. residents, in which case businesses will have to comply with the EU's more exacting requirements.[335] In addition, if businesses provide greater data privacy protection for EU residents

---

[331] EU rejects U.S. Data Privacy Plan, supra note ___.

[332] See Comments of the Council of Better Business Bureaus, supra note ___.

[333] A number of business representatives critique the draft Safe Harbor Principles as a move toward a European model, even though, in theory, the Principles are aimed at promoting a private, industry-led, self-regulatory alternative. They are concerned that Commerce's guidelines propel the United States toward a centralized "one-size-fits-all" EU-style privacy regime, since Commerce's draft principles apply to all business operations. They maintain this is contrary to the traditional U.S. sector-specific, problem-specific approach to data privacy regulation. See, e.g., Comments of Online Privacy Alliance, supra note ___; Comments of the Magazine Publishers of America, supra note ___; Comments of Time Warner, supra note ___; Comments of the Associated Credit Bureaus on the Department of Commerce, Draft Safe Harbor Principles, <http://www.ita.doc.gov/ecom/com1abc.htm#acb> (visited Jan. 13, 1999); and Comments of Stone Investment, Inc., supra note ___. Some businesses propose that the DOC not agree on a general, cross-sectoral set of Safe Harbor Principles with the EU, which the EU is unlikely to agree to in any case, but rather agree on Safe Harbor Principles on a sector-by-sector basis. See Comments of IBM on the Department of Commerce, Draft Safe Harbor Principles, <http://www.ita.doc.gov/ecom/com2abc.htm#ibm> (visited Jan. 13, 1999).

[334] See Comments of the U.S. Council for International Business (USCIB)on the Department of Commerce, Draft Safe Harbor Principles, <http://www.ita.doc.gov/ecom/com1abc.htm#uscib> (visited Jan. 13, 1999) (USCIB is the U.S. representative to the International Chamber of Commerce (ICC)). 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. Safe Harbor Comments of National Retail Federation. 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 U.S. from being used in direct marketing. See Privacy Laws Worries U.S. Businesses – European Regulation Could Have Far-Reaching Impact, supra note ___.

[335] As Kagan notes in his summary of the results 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, supra note ___, at 4.

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.[336] 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]."[337] Otherwise, U.S. citizens would be effectively treated as second class citizens in their own country. Second, 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.[338]

The spillover 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 data bases."[339] In conjunction with its joint venture with Bertellsmann, the German media conglomerate, America Online announced, "we will do whatever needs to be done in full compliance with the [EU] law."[340] When Citibank encountered problems with German data protection laws (which are similar to the 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.[341] Multinational firms which 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.[342] Within the U.S., internal company privacy policies now proliferate. New monitoring and enforcement schemes are developed. EU authorities and U.S. domestic advocates demand that they 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 export the practices that Europe requires to the United States.

VI. Conclusion: Trading Up-- The Factors Which Facilitate Raising U.S. Data Privacy Standards

---

[336] See Comments of Mark Silbergeld, supra note ___.

[337] See id.

[338] See supra note __ and accompanying text.

[339] K. Oanh Ha, European Privacy Protection Forces U.S. Firms to Scramble," SAN JOSE MERCURY NEWS, Oct. 26, 1998.

[340] See Noah Shachtman, EU Privacy Law is Awkward for US, WIRED, Oct. 23, 1998. See also, Europe's Privacy Cops, supra note ___.

[341] Blackmer March 27 Interview,supra note ___ (Blackmer represented Citibank on this matter); see also Transfers of personal data to third countries, supra note___, at 7; Andrews, supra note ___.

[342] 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 Vogel's work. See TRADING UP, supra note__. This point, however, is subject to an important caveat. To the extent firms, even after adapting more protective data privacy practices, face significant litigation-related costs in the U.S., they will continue to strongly advocate lower U.S. standards -- in the name of self-regulation.

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.[343] 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 the United States' 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. EU external pressures enhance the impact of U.S. internal pressures. It 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 which they can promote. By changing the stakes of U.S. actors, the Directive torques the way all U.S. institutions-- legislatures, regulators, courts and markets-- address data privacy issues. As Marc Rotenberg of EPIC affirms, "All the energy spent on the EU Directive has caused the U.S. to focus on privacy and raising our privacy standards."[344]

Where firms operate in multiple jurisdictions with differing regulatory requirements, they often 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 downwards 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 Web site-- are pressed to conform their data processing practices toward EU standards.[345]

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

---

[343] See, e.g., Aviva Freudmann, The US-EU Relationship, J. COM., Mar. 29, 1999 (noting the EU's critique of the Helms Burton Act); Carey Goldberg, Limiting a State's Sphere of Influence, N.Y.TIMES, Nov. 15, 1998, at § 1, p. 4 (discussing the state of Massachusetts' 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. See Shaffer, supra note__, 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.

[344] See European Privacy Protection Forces U.S. Firms to Scramble, supra note ___.

[345] 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 already meet such standards. See VOGEL, TRADING UP, supra note __.

(i) The Link with Liberalization: Transnational Institutional Interdependence.[346] 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 upwards, and not necessarily downwards in a "race to the bottom." Were U.S. companies to operate only domestically, they would be unconcerned by the 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. U.S. businesses must adapt practices in the United States to avoid EU restrictions and potential litigation before EU courts and administrative bodies.[347] U.S. regulatory authorities are instructed to fend off a regulatory conflict with the EU having potentially significant financial repercussions. In the process, these officials are pressed to promote enhanced 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 EU ultimately permits U.S. privacy advocates and regulators to use the attention given to U.S.-EU clashes over the Directive to promote greater data privacy protection at home.[348]

Even without formal trade and investment liberalization, information passes through an increasingly borderless world.[349] The information revolution permits an increasing number of

---

[346] See theme 1, the theme of transnational institutional interdependence, in the introduction. See in particular Parts II.E and V.

[347] Ultimately, of course, the Directive's impact will depend, in large part, on its enforcement. The Commission and member state authorities remain understaffed so that enforcement is an issue. Yet as earlier discussed, member state authorities already enforce member state data privacy law. See supra notes__. Moreover, as noted in Part VB, privacy advocates can act as private attorneys general and privacy service providers, including legal advisors and company in-house privacy directors, can also significantly affect business behavior. See infra notes ___ and accompanying text. U.S. businesses have strongly reacted to the Directive because they feel its potential impact is significant.

[348] 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 ERNST HAAS, THE UNITING OF EUROPE (1958). This article, however, does not employ an a-politicized 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 enforcing higher social protection standards is a key variable.

[349] 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." PRIVACY IN THE INFORMATION AGE, supra note ___, at 5. Author Anne Branscomb calls information "the lifeblood that sustains political, social, and business decisions." Anne Wells Branscromb, Global Governance of Global

companies to engage in cross-border transactions. Even small U.S. enterprises will engage in electronic commerce in the future. Even small enterprises have Web sites through which they collect information on EU residents. 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.[350] 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.[351]

The EU's large internal market provides leverage when the EU threatens to restrict data transfers to the United States on account of its inadequate data privacy protections. A similar challenge from a country which 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, including through 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. 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 upwards.

While many EU member states, such as Germany and France, have large economies, they enhance their clout vis-a-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 United States' reaction to the threat of bans on data transfers from Europe demonstrates this. Before the Directive went into effect, many EU member

---

Networks: A Survey of Transborder Data Flow in Transition, Vanderbilt Law Rev., 985, 987 (May 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 Untied States." WTO Annual Report 1998, at 35 (citing Martin Wolf, A Bearable Lightness, FIN. TIMES, Aug. 12, 1998). 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." See Commerce Report Describes Economic Benefits from Internet, N.Y. TIMES, June 23, 1999. See also Mark Felsenthal, Administration Highlights Efforts to Fill Information Technology Jobs, 1998 DER 08 D43 (BNA) Jan. 13, 1998. The variety of companies and business associations which 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__.

[350] See theme 2, the theme of foreign market power, in the introduction. See in particular Parts IA and IIIA.

[351] See theme 3, the theme of reallocated sovereignty, in the introduction. See in particular Part IIIA.

states had data privacy laws which permitted them to ban data transfers to countries without adequate data privacy protection.[352] Yet it was not until the 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.[353] Third, the EU is rich, and data privacy protection is a good that individuals increasingly demand when they become richer.[354] Even further, data privacy is arguably a luxury good, that is, a good whose demand increases disproportionately vis-a-vis the demand for other goods, as income levels rise.[355] 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, 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.

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,[356] which also arguably constitutes a luxury good whose demand cannot

---

[352] See, e.g., Amy Monahan, Deconstructing Information Walls: The Impact of the European Data Directive on U.S. Businesses, 29 LAW & POL'Y INT'L BUS. 275, 287 (1998) (citing applicable member state laws).

[353] See theme 4, the theme of trading up, in the introduction.

[354] According to a 1998 survey, "it is the prime consumer audience of better-educated and higher-income groups that register the strongest privacy concerns." Alan F. Westin, The Era of Consensual Marketing is Coming, (Dec. 14, 1998) <http://www.privacyexchange.org/iss/surveys/1298essay.html> (summarizing the 1998 Harris-Westin privacy survey "Privacy Concerns and Consumer Choice").

[355] This definition of luxury goods is taken from JAMES GWARTNEY & STROUP, ECONOMICS: PRIVATE AND PUBLIC CHOICE, and further explained in economic terms in supra note ___. While the author has 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, technologies more likely to be used by individuals in states with relatively high median income levels.

[356] See TRADING UP, supra note ___, at 261-262.

easily be met at low cost through private contract.[357] As 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.[358] 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.

(iv) Externalities of Data Privacy Practices and Policies. Fourth, data privacy policies have significant externalities.[359] 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 the EU's data privacy policy to be effective, its cross-border effects can not be avoided, since 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 EU regulates the transfer of information not only within the EU, but

---

[357] There is a significant amount of economic analysis supporting the proposition that environmental standards tend to rise as income levels rise. See e.g. Gene M. Grossman and Alan B. Kreuger, Environmental Impacts of a North American Free Trade Agreement, in Peter Garber, ed., THE MEXICO-U.S. FREE TRADE AGREEMENT 13-56 (1993); and Judith M. Dean, Trade and the Environment: A Survey of the Literature, in Patrick Low, ed., INTERNATIONAL TRADE AND THE ENVIRONMENT 15-28 (World Bank Discussion Papers, 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 an almost infinite number of data privacy contracts, thereby slackening their demand for broad-based national labor standards. Because of the more widespread use of private employment contract 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 upwards leveraging than labor regulation.

[358] This argument is employed by Vogel in TRADING UP, supra note __, at 5-8 (referring, for example, to the support of Germany's automobile manufacturers of 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 infra note.... 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 Part VC, infra notes... and accompanying text.

[359] For the meaning of the term "externalities" in economics, see supra note __.

also to other jurisdictions.[360] Otherwise, the EU's data privacy goals could easily be circumvented through the transfer of information abroad which is then recompiled, used and marketed, including back into the EU itself, whether directly or over the Internet.[361]

The data privacy issue is analogous to many other cross-border and global regulatory issues. As regards cross-border and global environmental protection, for example, the EU 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 third countries. Despite internal U.S. policies constraining or eliminating the use of CFC-emitting products, the actions and inactions of producers and consumers in third countries affect U.S. residents. The concerns of the EU over data privacy protection are no different.[362]

---

[360] See also theme 4, the theme of trading up, in the introduction. See in particular Parts IA, ID, IVB and IVC.

[361] Existing business tax havens could similarly become havens against data privacy regulation. Bermuda, for example, is striving to become a "hub for e-commerce." 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).

[362] This is not to say that, in a globalizing economy, all social protection will be leveraged upwards in all countries. First, there will be no such pressure in countries whose economies are not integrated in the global economy (see the first factor listed above). 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." Yet labor regulation is different than data privacy protection not only because wealthy individuals more easily protect their working conditions through private employment contracts (see infra note__). 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 countered that, while the effects are less direct, low labor standards in other jurisdictions still have external effects in the U.S. and Europe. Low labor standards can be morally offensive to purchasers of products in the U.S. and Europe. Moreover, they can reduce labor's negotiating power vis-a-vis capital in the U.S. and Europe on account of capital's ability to migrate to countries with lower standards. Yet although the U.S. and EU have engaged in some efforts to raise foreign labor standards, these efforts have been minimal, and they have, in addition, been hampered by constraints imposed by supranational trade rules. 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 an account of the relative costs of higher labor standards. Firms engaged in international transactions more forcefully oppose a revision of trade rules to permit 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.

Concerning the impact of trade liberalization on labor and labor standards, see e.g., DANI RODRIK, HAS GLOBALIZATION GONE TOO FAR? (1997). On the pressure to make EU labor policies more flexible, see e.g. Martin Rhodes, Globalization, Labour Markets and Welfare States: A Future of 'Competitive Corporatism' in MARTIN RHODES AND Y. MENY, THE FUTURE OF EUROPEAN WELFARE: A NEW SOCIAL CONTRACT (1998); and Wolfgang Streeck, Neo-Voluntarism: A New European Social Policy Regime, 1 EUROPEAN L.J. 39 (1995). On the relatively minimal efforts exercised so far by the U.S. and EU to incorporate labor standards in international 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). See also Section 301, Trade Act of 1974, 88 Stat. 2041 (1975), as amended, 19 U.S.C. § 2411(d)(3)(B)(iii) (providing for trade

(v) Constraints of Supranational Rules.[363] 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 effectively raise its data privacy standards. On the contrary, they constrain the United States' ability to retaliate, again further facilitating a trading up of standards.[364]

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 protection 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 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) the EU uses its market power to help satisfy its citizens demands, and EU member states' market power increases when they act collectively; (v) supranational rules do not significantly constrain the EU's application of its data privacy laws, but rather constrain the United States' ability 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 Directive has already helped incite other countries to

---

restrictions where a country does not comply with a defined set of fair labor standards), which has been rarely used.

[363] See theme 5, the theme of WTO supra-national constraints, in the introduction. See in particular Part IV.

[364] 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 the EU's 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." 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 Part IV, infra notes___ and accompanying text.

adopt data privacy protection regulations,[365] 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 standards organization, ISO.[366] Whether the harmonization be de jure (through government regulation) or de facto (through private business practice and "self-regulation"), foreign businesses are being pressed to require and provide greater data privacy protection. The pressure on U.S. businesses and officials intensifies.

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 brings us a greater variety of goods and services at lower prices. On the other hand, with it, we may 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 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 Directive has helped push them further than they would have otherwise gone.

---

[365] See e.g., Fred Chilton, Simon Cant & Emma Moloney, 1996 Computer and Telecommunications Law Update New Developments: Asia Pacific, 15 J. MARSHALL J. COMPUTER & INFO. L. 99 (Fall 1996) (concluding that the EU Directive puts pressure on Pacific Rim nations to adopt privacy regulations, including controls on the export of personal data), and Colin Bennet, Convergence Revisited: Toward a Global Policy for the Protection of Personal Data? in Philip Agie & Marc Rotenberg eds., TECHNOLOGY AND PRIVACY; THE NEW LANDSCAPE (1997) (noting the impact of the 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," at 109-20). See also the comments of U.S. business representatives cited in Part V.C.3, supra notes ____.

[366] Discussion has already begun under ISO auspices about the possibility of an ISO privacy standard. See Colin Bennet, Convergence Revisited. Toward a Global Policy for the Protection of Personal Data?, in AGRE & ROTENBERG, TECHNOLOGY AND PRIVACY, 116, 123 (note 55), supra note__. See also Parker Chapman, Commission Raises Prospect of EU Data Protection Norm 22 EUROPEAN 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 Standardization Organization (ISO) to develop a world norm for data protection").