5

Negotiating Privacy across Arenas: The EU-US "Safe Harbor" Discussions

Henry Farrell

Much recent theoretical attention has been devoted to the provision of common goods across arenas. The normal problems of common good provision (Olson 1968; Hardin 1982) are exacerbated when these problems spill across arenas (there are usually no actors capable of imposing hierarchical solutions), but there are also new difficulties. Solutions in one particular arena of policy-making may be incompatible with the solution or broader regulatory mechanisms in another arena. Furthermore, states, which may solve some common goods problems seem to be losing some decision making competencies in the global arena. While non-state actors may provide at least some common goods (Ronit and Schneider 1999), it is unlikely that these forms of provision can be generalized in any meaningful way. Many authors believe that globalization makes it vastly more difficult to solve international common good problems (Cerny 1995).

Yet this pessimism may at least be partly misplaced. The globalization literature argues both that common problems spill over state borders ever more (common good difficulties are internationalized) and that the capacity of states to respond to these problems is ever weaker (there is insufficient capacity to provide common goods internationally). While the first of these claims is true in many areas, the second is at least arguable. States may still try to solve collective action problems through unilateral action, through coordination among themselves, and through new forms of policy which mix public and private action. The second and third of these types of solution typically require negotiations which seek to harmonize forms of common good provision across arenas, or at least to ensure the compatibility of different solutions in different arenas. This layer of international negotiation provides new opportunities for actors in domestic arenas.

The third kind of solution – public actors working together with private actors, or indeed delegating substantial enforcement authority to them – has attracted much recent attention. On the one hand, advocates of this approach (especially in business and government) suggest that it allows a much greater degree of flexibility than “traditional” regulation. On the other hand, critics

(who often seek to protect consumer or citizen interests) believe that it is symptomatic of a wider trend towards the abdication of public matters to private self-interested actors, with consequent problems of democratic legitimacy (Cutler, this volume). The differences between these two views of public-private action has given rise to vigorous policy debates and discussions over the introduction of new "hybrid" approaches to common goods problems.

This chapter examines one such set of discussions – the negotiations between the EU and US over the so-called "Safe Harbor" arrangement on data protection and privacy.[1] These negotiations provide a good test case for arguments about common goods provision across national borders (Shaffer 2000). By examining the course of the negotiations, we may come to arrive at a better understanding of the forces dictating both actors' negotiating positions, and the bargaining power which they have to realize those positions. The strategic interaction which leads (or does not lead) to a particular form of common good provision, involves actors with differing interests and objectives. Insofar as common goods are provided, this will likely emerge from struggles between actors who differ both according to their interests and their conception of how the relevant good is best provided, the latter often being determined by the former. In this particular instance, such an enquiry may help us understand why a hybrid institution involving both public and private actors resulted from negotiations, given the relative goals and bargaining positions .

This chapter adopts an approach which can be characterized as a form of "actor centered institutionalism" (Scharpf 1997). I seek to show that this form of analysis is well suited to the examination of bargaining and negotiation over multi-arena common goods, and the agreements reached between actors. I begin by discussing whether privacy can be defined as a common good, and the different forms of governance through which it might be provided. I then go on to examine the different approaches to privacy which have arisen in the two arenas under discussion; the European Union and the United States. Next, I describe the different actors involved both indirectly and directly in the negotiations, their preferences, and their power to achieve those preferences given prevailing circumstances. I go on to examine how these positions played out in three interlinked arenas, and conclude by discussing the implications of the Safe Harbor negotiations for common good provision in multi-arena settings.

Privacy as a Common Good

Privacy is an ambiguous concept, with multiple meanings, according both to its context, and the philosophical orientations of those discussing it. It is thus difficult precisely to characterize privacy as a common good, given that there is disagreement as to what precisely it involves. One can nonetheless examine how privacy has been discussed and implemented in policy terms, and the extent to which this has involved collective action problems. Since the early 1970's, policy makers have typically conceived of privacy in terms of principles of data

protection.[2] Indeed, the 1970's and 1980's saw a substantial degree of policy convergence among industrialized Western democracies as to what such principles should involve (Bennett 1992, 1997). This convergence was marked on the international level by the OECD's non-binding guidelines on data protection and the Council of Europe's Convention, and on the national level by the adoption of data protection laws in most OECD countries. These principles impose real burdens on the collectors of data: in other words, they are not self-enforcing. Data collectors, if they are guided by rational self-interest, and do not believe they will be punished for failing to abide by these principles, will tend to ignore them.

The observance of fair information principles is a public good problem (Ostrom, this volume). There is non-rivalness of consumption; my observation of privacy principles is unlikely to detract from your observation of privacy principles in most circumstances, but it is difficult to exclude those who seek to free ride on the general perception that fair information principles are observed. Like other public goods, it is likely to be underprovided. Take, for example, privacy on the World Wide Web (WWW).[3] There is substantial opinion poll evidence suggesting that many consumers are unwilling to make purchases or carry out other activities on the WWW, because of privacy concerns.[4] The WWW allows new forms of data collection which are often difficult for consumers to detect; furthermore there have been several widely-reported cases in which consumers' privacy has indeed been invaded. However, consumers face a serious collective action problem if they wish to mobilize against those firms that do invade their privacy. "Exit" on its own may be insufficient to change firm policy, especially for firms such as profiling firms, which the consumer does not necessarily deal with directly, but which are pervasive on the WWW, and which gather detailed information on consumers' websurfing. But organized collective action may prove difficult given the vast number of consumers involved. The unwillingness of political decision makers (at least in the US) to become involved in regulation of e-commerce makes it unlikely that government will serve as a "multiplier" for collective action (Hardin 1982).

Firms, as well as consumers face a collective action problem. Given the lack of consumer confidence in the WWW, firms may have a common interest in buoying up consumer confidence, and encouraging them to make purchases, through adhering to fair information practices and pressuring other firms to do so too. But this interest is precisely a *collective* one. Insofar as individual firms are unlikely to benefit very much from their own, particular contribution to the common good of consumer confidence in the Web, they will have an incentive to free ride on the efforts of others. In the words of Robert Litan,

> In principle, the privacy problem on the Net is a classic "collective action" problem: that is, because all actual and potential Net users would be better off if they were comfortable that the information they provided over the Net was absolutely safe and private, no single firm can capture all of the benefits of guaranteeing that its particular Web site has these characteristics.[5]

This collective action problem might be resolved in various ways. First, reputational incentives alone might encourage firms to adhere to a stringent privacy policy. Insofar as it is the *particular* reputation of a firm which suffers from privacy violations, rather than the *general* reputation of WWW commercial actors as a group, the firm may have an incentive to adhere to privacy practices, even if they are not formally required.[6] Many business representative organizations argue that these reputational effects are sufficient to guarantee consumer privacy: market forces will drive firms with bad reputations out of business, or force them to improve their behaviour.

A second possible solution is that business self-regulate through its representative organizations, through adherence to uniform privacy standards, through third party bodies, or through some mixture of these three. Knill and Lehmkuhl (this volume) discuss the capacity of private actors to provide common goods, distinguishing between the "strength" of a business organization vis-a-vis its members, and the "degree" to which a particular set of business actors is organized, and willing to contribute to the provision of a common good. If self-regulatory schemes are sufficiently "strong," and provide a broad "degree" of coverage, they may be capable of enforcing common good provision.[7]

A third solution is state action; formal regulations which mandate that actors adhere to a certain set of standards. In privacy, one may identify two broad approaches to state regulation. First is the approach of the member states of the European Union and some other OECD states. These states have both omnibus cross-sectoral laws, which lay out privacy practices in detail and independent, specialized agencies - data protection commissions - which seek to ensure that those laws are enforced. Second is the US approach, with a patchwork of laws and regulations, which differ widely between sectors. In many sectors, there is no legal coverage beyond self-regulation, or firms' own commitments. However, there is a mechanism to ensure that firms do at least live up to any promises they may have made to consumers about the privacy of their information. The Federal Trade Commission (FTC), under Section 5 of the FTC Act, can issue "cease and desist" orders to firms who are violating their stated commitments, and impose substantial fines. It has taken action against firms such as Geocities, which have violated their privacy statements. One should note that the FTC cannot either force firms to issue a privacy policy, or dictate what the terms of any privacy policy should involve; it can merely police those commitments that firms have voluntarily made.

I do not wish to discuss the respective strengths and weaknesses of these approaches in this chapter; instead, I wish to repeat the suggestion that the mode (or mix of modes) which prevails in a particular policy setting is likely to be the end-result of struggles between different actors with competing end-goals. Most firms would ideally prefer a situation in which privacy protection is left to them, either through pure market mechanisms, or through some form of self-regulation in which they set the rules. Equally, other actors such as consumer organizations or data protection authorities may prefer an end-result in which privacy is protected through legally binding rules mandating fair information practices.

State actors will have their own interests and objectives, which may vary between different policy areas within the state apparatus. The question of which set of preferences prevails is an empirical one, which will depend in part on the prevailing institutional setting, and its effect on the relative bargaining positions of the relevant actors.[8]

Thus, in summary, it is clear that privacy, or, more precisely, data protection) may give rise to collective action issues. Adherence to data protection principles is a public good. Consumers face a linked collective action problem if they wish to ensure that these principles are lived up to. There exist different mechanisms through which these common good problems might be resolved - reputation and market forces, self-regulation by firms, and government regulation. Each of these different modes has different implications and possibility conditions. These different mechanisms reflect the interests and objectives of different actors within those governance systems. As discussed in the next section, globalization and the advent of e-commerce are resulting in problems of governance, as common good problems become internationalised. But insofar as these problems must be resolved in a multi-arena setting, there are new opportunities for actors strategically to act across arenas in order to attain their goals.

Privacy and Data Protection in Europe and the US: the Background

Europe and the US have very different approaches to data protection and privacy. The US as discussed above, has eschewed an omnibus approach to privacy protection, and in many areas, most notably e-commerce, there is little substantial legal protection.[9] Furthermore, legislation in the area of e-commerce is a highly sensitive topic. The US administration has concluded that regulation is inappropriate, given how swiftly e-commerce is evolving, and has instead sought to encourage self-regulation in areas such as privacy, in the belief that self-regulation would be more flexible and responsive. In Europe, in contrast, data protection legislation has been enacted in a number of waves (Mayer-Schönberger (1997), culminating in the European Union's *Directive on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data*; the so-called "Data Protection Directive," which came into effect in October 1998. This Directive was intended to prevent differences in how member states protected data from impeding the integration of the Single Market. The Directive thus provided a framework for omnibus protection for privacy across different sectors, the specifics of which were to be implemented in national law.

The US and EU approaches came into conflict because of overspill between the two arenas; modern communications technology made it relatively easy to transfer information from the EU to third party states such as the US. This could potentially have undermined the EU's attempts to provide data protection for its citizens, if it were possible to transfer personal data outside the jurisdiction of

the EU, and then to process it without fulfilling the requirements of the Directive. Accordingly, the Directive only allowed the export of data (with some tightly worded exceptions) under two circumstances; where the data was contractually protected, or the jurisdiction to which it was being exported had "adequate" protection.[10] Contractual protection was more suited for some forms of data transfer (such as personnel records) than for others, and there was furthermore some doubt as to what contractual forms were necessary: the EU has only very recently finalized a set of model contractual clauses.[11]

The Data Protection Directive describes in some detail the process by which adequacy or non-adequacy is to be determined. The Commission, under Article 25.6 of the Directive, may find that a third country gives an adequate level of protection "by reason of its domestic law or of the international commitments it has entered into." Where the Commission finds that a third country provides an inadequate level of protection, member states are enjoined to prevent data transfers to that third country (Article 25, 4). At the same time, the Commission is instructed to enter into negotiations as appropriate with the third country (Article 25, 5). The "international commitments" provided by a third country may result directly from these negotiations; indeed the language of the relevant clause seems to suggest that this is the primary sense of the term as employed in the Directive.

In its negotiations with a third country, the Commission must also consult with the Article 31 Committee which is composed of representatives of the member states and chaired by the Commission.[12] This Committee is a comitology procedure which votes by qualified majority on measures to be taken with regard to adequacy. If the Committee votes against the proposed measure, the Commission must defer application of the measure for three months, and communicate this to the Council forthwith. The Council may act under qualified majority to take a different decision during that three month period. The European Parliament has procedural oversight, in order to ensure that neither Commission nor Council has overstepped its competences.

It was clear from an early stage that the US was unlikely to be considered an "adequate" jurisdiction as matters stood. However, US experts hoped that some sectors, with specific legal protections, could be considered "adequate," and that the EU might consider certain self-regulatory codes of conduct sufficient for an adequacy finding. The importance of EU-US trade in services meant that the Commission had to seek some mutually tolerable modus vivendi. Structured EU-US discussions over adequacy started in early 1998, some six months before the Directive was due to come into effect. Initially, these discussions were not especially fruitful. Prominent US decision-makers viewed the Directive as a fundamental threat to US commercial interests, and to the expansion of e-commerce, and they sought to force the European Union to back down. Other figures in the Department of Commerce were aware of how unlikely an EU climbdown was, and engaged in serious discussions with the European Union as to how adequacy might be reached. Ambassador David Aaron, the Undersecretary for International Trade in the Department of Commerce had been briefed by US businesses about the possible consequences

of the Directive, and began discussions with John Mogg, the Director General for the Internal Market. The EU-US discussions were initially frustrating. The European Union maintained that it was interested only in legislation drafted to provide adequate protection to the data of European citizens which had been exported, while the US sought to postpone the implementation of the Directive, and to gain a recognition of adequacy for the US system as it then stood. In this early stage of discussions, negotiators were pessimistic: the best likely outcome was some form of damage limitation. However, a suggestion by Aaron that the adequacy judgement need not extend to the entire US system, but rather to a set of firms which had voluntarily agreed to embrace a set of privacy principles, proved to be the basis for a potential compromise. EU negotiators found the approach interesting enough to merit further negotiations, and the EU undertook to be as flexible as possible in its interpretation of the Directive (i.e. to avoid data blockages unless absolutely necessary) while discussions were still under way. On November 4, 1998, Aaron wrote a public letter to US businesses, setting out draft principles for a so-called "Safe Harbor" for US firms: the intention was that firms which would not be subject to EU action as long as they adhered to these principles. In summarized form, the principles were

Notice – organisations must inform individuals about what type of personal information were collected, how it was collected, whom it was disclosed to, and the choices individuals had for limiting this disclosure.

Choice – Organisations must give individuals the opportunity to opt out when information was used for purposes unrelated to the use for which they originally disclosed it. Individuals must be given opt in choice with regard to certain sorts of sensitive information.

Onward transfer – Individuals must be able to choose whether and how a third party uses the information they provide. When information is transferred to third parties, these parties must provide at least the same level of privacy protection originally chosen.

Security – Organisations must take reasonable measures to assure the reliability of information, and prevent loss or misuse.

Data integrity – Personal data must be kept accurate, complete, current, and used only for the purposes for which it is gathered.

Access – Individuals must have reasonable access to data about them, and be able to correct it when it is inaccurate, subject to the sensitivity of the information and its dependent uses.

Enforcement – There must be mechanisms for assuring compliance with the principles, recourse for individuals, and consequences for the organisation when the principles are not followed. Enforcement could take place through

compliance with private sector privacy programmes, through compliance with legal or regulatory authorities, or by committing to cooperate with the data protection authorities in Europe.

The US hoped that the EU would accept these principles relatively swiftly; instead, negotiations were to last over eighteen months. When the Commission presented the US proposal, certain member states expressed their difficulties with the package, in particular on the questions of access and enforcement. Lengthy negotiations followed, which only reached a final resolution in June 2000. The Safe Harbor principles themselves saw very significant amendment, mostly in response to European demands that they be tightened and made more workable. In addition to the Principles themselves, a series of Frequently Asked Questions (FAQs) were negotiated, which provided authoritative interpretation of the principles in specific instances.

The final agreement reached on Safe Harbor involves both the principles themselves, and enforcement mechanisms designed to back them up. Enforcement is provided on three levels. The first line of enforcement is intended to handle complaints about possible breaches of their privacy. Organizations may sign up to third party dispute resolution bodies, which should fulfil certain stated criteria, or commit to cooperate with data protection authorities within the European Union member states; in future they may also be able to commit to work together with appropriate US regulatory authorities.

The second line of enforcement is intended to ensure both that organizations do not fail to fulfil their Safe Harbor commitments, and that third party dispute resolution mechanisms work as they are supposed to. The FTC has oversight powers under the FTC Act: signing up to Safe Harbor is a public commitment, and firms which fail to abide by such commitments can be penalized.[13] The same is true of third party dispute resolution bodies, insofar as they act on behalf of for-profit bodies. The FTC has undertaken to deal with complaints from third party dispute resolution bodies and from European data protection authorities on an accelerated basis.

The third line of enforcement is provided by the European Union itself. Under certain restricted circumstances, European data protection authorities can still block the flow of data. Further, the Safe Harbor arrangement itself is a unilateral determination of adequacy on the part of the European Union rather than an international agreement, which means that it can be suspended or abrogated unilaterally if it is clear that it is not working.

At the time of writing (June 2001), the Safe Harbor has come into effect, but so far has attracted some sixty firms. Interviews suggest that firms are behaving cautiously: Safe Harbor involves serious obligations, which many firms are reluctant to take on without fully considering alternatives. While involved actors suggest that Safe Harbor will play a substantial role for US firms, this is still uncertain.

Privacy and Data Protection: Arenas and Actors

The process leading up to Safe Harbor can be characterized in terms of three interlinked arenas, or, in Tsebelis' term "nested games" (Tsebelis 1990). The first of these arenas is the obvious one: the EU-US negotiations. But the second of these arenas was more important for many of the US actors involved: domestic politics within the US itself. Privacy had suddenly become an important policy issue, in part because of the publicity surrounding the EU's Data Protection Directive and its external effect, but mostly because of consumer concern both about privacy on the WWW, and new technologies allowing the offline gathering and use of personal information. Further, these two arenas potentially intersected: many actors who sought to influence developments in the first arena (EU-US negotiations) were motivated by goals that they were pursuing in the second (the domestic US debate). In particular, actors who were less powerful in the second sought to use their influence in the first to increase their bargaining strength. Finally, there was a third arena, that within the European Union itself, where any adequacy arrangement would have to receive approval in terms of its substance (Article 31 Committee/Council) and process (European Parliament).

To develop this argument, it is first necessary to describe actors involved in the negotiation process in greater detail. The remainder of this section describes these actors and their goals. The subsequent three sections will look in closer detail at each of the three games - first, the EU-US negotiations, next the domestic policy debate within the US, and finally the debate within the EU institutions.

On the European side, four main actors (or sets of actors) can be identified - the Commission, the member states, the European Parliament, and the data protection commissioners of the individual member states.[15]

The *Commission* did not have unified preferences on Safe Harbor, but internal critics of its negotiating stance did not play a major role in determining its policy. The Commission negotiators' primary concern was to resolve what they saw as a potentially dangerous situation for the implementation of the Directive. Officials believed that many firms were ignoring the Directive, and transmitting personal information to the United States, because it was necessary to their business, and because the benefits outweighed the risks of being caught. The Commission effectively had three alternatives. First was to ignore what was happening, which would have undercut the intent and credibility of the Directive. Second was to encourage a harsher attitude to enforcement, which might have prompted more compliance on the part of firms, but which also might have led to US retaliation, as well as domestic difficulties. Third was to negotiate with the United States in order to try to reach an adequacy finding which would allow firms to comply with the Directive. The third of these was the most attractive to the Commission, which retained the option of more stringent enforcement as a bargaining tool.

The *member states* differed in their attitudes to data protection, and to the kinds of compromise that would be necessary to reach an agreed solution with

the United States. Some member states, most prominently the UK and Ireland, had no difficulties in principle with a self-regulated, non legislative compromise of the sort that finally emerged. Germany and France, in contrast were more sceptical about self-regulation and more difficult to persuade. In the absence of formal legal protections, they preferred not to grant adequacy to the US, and instead to oblige firms to provide contractual protections to information transfers outside the US. Member states were represented in the process through the Article 31 Committee.

The *European Parliament* did not become formally involved until after the Commission and Article 31 Committee had decided to grant adequacy. The Parliament was politically split on the merits and drawbacks of a compromise solution with the US. This split cut across party lines. On the one hand, many Parliament members were distrustful of self-regulation, and were influenced by the jaundiced view of data protection commissioners. Furthermore, because the process of determining adequacy did not involve an international agreement as such, the Parliament's role was limited to procedural oversight, which rankled for some MEPs, who felt that they should have a more direct say. On the other hand, other Parliament members viewed the process as a political opportunity to demonstrate that a more flexible approach to consumer protection issues could work, and thus to influence ongoing policy debates within Europe. Throughout the negotiations, Commission officials sought to keep MEPs on both sides of the debate informed of developments.

The *data protection commissioners* were formally represented in the policy discussions surrounding the negotiations through the so-called Article 29 Working Party. This body was constituted of representatives of the data protection commissions, one from each member state. Votes took place on the basis of a simple majority procedure. The Working Party's role, however, was purely advisory; while the Commission was obliged to inform the Working Party about how it had responded to the Party's proposals and suggestions, it was under no obligation to implement them. The Working Party was deeply sceptical of the proposition that the "patchwork of narrowly-focussed sectoral laws and voluntary self-regulation" (Data Protection 1998) that characterized the US could provide comprehensive protection to the data of European citizens.

On the US side, the main actors were those within the administration (I include independent agencies in this category), concerned businesses and business organizations, and consumer groups. While some figures in Congress maintained a strong interest in privacy, and a watching brief, they did not play a direct role.

The *administration* was relatively slow to react to the Data Protection Directive, and initially was internally divided about how best to respond. Many figures in the administration saw the Directive in terms of the ongoing policy debate about the regulation of privacy on the WWW, and the regulation of e-commerce more generally. The White House had sought to forestall government regulation of the Internet, and saw the Data Protection Directive as an antithetical approach, which involved an extensive role for government in e-commerce, and a heavy regulatory burden for firms. Thus, it advocated a

hardline position which would seek to force the EU to back down. Another body of opinion shared the basic presumption that self-regulation was the best way to regulate e-commerce, but did not believe that the EU or its member states could be pressured to put the Directive into abeyance. Negotiations would be necessary to find some mutually acceptable *modus vivendi*. This perspective was most clearly articulated by the Department of Commerce where the National Telecommunications and Information Administration had already sought to carve out a leadership role in the debate on self-regulation and e-commerce (Department of Commerce 1997). A third approach was embodied in the FTC, an independent agency. The FTC too had sought to shape the debate on privacy through a series of reports, and had strongly hinted that it wished to expand its ambit to include privacy issues. While the FTC moved back and forth on the issue of whether self-regulation was sufficient to protect privacy, tacking to the prevailing political winds, it saw privacy on the WWW as a consumer protection issue, which might eventually best be handled through formal legislation, and an enforcement role for the FTC itself.

Business, like the administration, was divided, but initially hostile to the Directive. US firms had lobbied heavily while the Directive was working its way through the EU decision-making process, and had been successful in persuading lawmakers to water down some of its requirements (Regan 1999). However, it still remained threatening to US business, especially in its extraterritorial aspects. Business had strong relationships with the US administration, and a direct voice in the EU-US relationship, through the TransAtlantic Business Dialogue (TABD), a process through which EU and US businesses could reach common positions on outstanding issues in the transatlantic relationship, and voice them to policymakers (Peterson and Green Cowles 1998). US firms had two, partially conflicting aims. On the one hand, they wished to see a regime which would allow stability in data transfers. On the other hand, they wished to firewall EU-US discussions from the nascent domestic debate about whether formal privacy standards should be implemented on the WWW. At the same time that the Directive's extraterritorial impact was becoming a political issue, businesses was having mixed success in creating credible self-regulatory schemes to forestall domestic privacy legislation. Firms feared that the two debates might become enmeshed, and that EU pressure might increase the leverage of groups lobbying for legislation on online privacy.

Finally, US *consumer organizations* favoured strong legislation to protect individual privacy, both in the online and offline worlds. A small group of privacy advocacy groups, most prominently the Electronic Privacy Information Center (EPIC) had successfully highlighted privacy problems within the US, and sought to persuade policymakers to take a more pro-active approach to privacy protection. More broadly-focussed consumer groups, including the Public Interest Research Group (PIRG), and the Consumer Project on Technology (CPTech) had also become involved in the issue. While these groups had succeeded in placing privacy on the policy agenda, consumer groups had relatively limited access to policymakers within the administration, who typically saw privacy as an issue of e-commerce confidence, and took their lead

from business. Like business, consumer groups had an official voice in the transatlantic relationship through the TransAtlantic Consumer Dialogue (TACD), initiated in 1998.

Arena I - the EU-US Negotiations

The EU-US negotiations had its start in a kind of confrontation that is analytically tractable: its structure resembled the "Chicken" game-form. Important figures within the United States wanted the European Union to back down and suspend application of the extraterritorial aspects of the Directive. Ira Magaziner, the White House information technology "czar" embarked on a series of speeches and briefings where he threatened WTO action should the EU stop data flows. He also suggested that the Directive was unpopular among member states, many of which had no previous data law of their own, and were relatively slow to adopt required legislation. The implication was that the Europeans should recognize that the US system as adequate under the Directive, if they did not indeed themselves embrace a self-regulatory approach. For their part, the Europeans wanted the US to back down and create a formal system of domestic data protection which would provide adequacy under the Directive. In the Chicken game, each player wants the other player to play Cooperate (to back down), while she plays Defect. The danger is that if both players play Defect, the result is mutually disastrous. And this seemed to be the most likely scenario[17] - the EU refusing to back down, but the US refusing to introduce formal legislative changes which would have provided adequacy.

Of course, neither side prevailed as such. There is some reason to believe that the US threat of WTO action was not a credible one. Legal scholarship[18] suggests that the European Union, provided it did not act in a discriminatory fashion in blocking data, would have had a good chance of prevailing in any WTO case. The relevant treaty, the General Agreement on Trade in Services (GATS), provides a specific exemption for the protection of personal information.[19] EU officials were confident that they would prevail in any action, and on the US side, the USTR appeared reluctant to become involved. Thus, the international institutional environment did not provide the US with sufficient leverage to force the EU to climb down. Further, the EU could credibly claim that its hands were tied by the Directive; the Commission was legally bound to make adequacy judgements on the basis of a more or less objective set of criteria.

Similarly, however, the US could credibly refuse to introduce formal federal legislation. The multitude of veto points in the US political system would have made it difficult for the US to introduce extensive omnibus legislation, even had it wanted to (Scharpf 2000). And it was clear that there was no political consensus within the administration to legislate on privacy, let alone at the behest of a foreign supranational entity.

The squaring of the circle came about through an imaginative US proposal to provide the kinds of adequacy that the EU was looking for, but through means that both (a) were closer to the current US approach of self-regulation, and (b) did not require formal legislation, and thus did not have to be shepherded through the numerous veto points. As described by a senior US negotiator, "the basic deal was we will accept your high standards, if you will accept our self-regulation."[20] But the package, as European negotiators stressed, was not standard self-regulation - it involved governmental officials negotiating the content of rules, and regulatory authorities ensuring that they were enforced. Rather than seeking to harmonize two radically different approaches to privacy regulation, Safe Harbor seeks to provide an interface between them.

To say that the solution is an interface between the two systems is not to imply that there was not vigorous bargaining between the EU and US as to the form that this interface should take. The Safe Harbor Principles and accompanying FAQ's were submitted to detailed parsing and negotiation. Furthermore, the particular institutional arrangements of the adequacy procedure had implications for the respective bargaining strength of the EU and US. A recent body of literature in international relations has examined the effect of institutional arrangements on both the EU's bargaining strength, and the likelihood of agreement in international negotiations where the EU is involved (Jupille 1999, Meunier 2000). However, this literature focuses on trade negotiations, where the issues are more readily captured using simple spatial models; one of the key difficulties of the Safe Harbor negotiations was precisely that negotiators' bargaining positions could not be mapped onto a simple continuous issue space. In the words of an EU negotiator

> you can't negotiate very easily on these issues. First of all, because they are fundamental rights, that you can't just negotiate away. ... you've got access or you've got no access, you can't have half access. You really have to define very specifically when access has to be given, when access can be denied.[22]

Or as David Aaron described it, "the solution we're seeking is not a balance or a tradeoff. It's more like resolving simultaneous equations." (Aaron 1999). This said, as Meunier and Jupille have suggested, the institutional structures governing Safe Harbor did have an important effect on the bargaining power of the parties. In particular, the EU was able to use the complications of the adequacy procedure to wring concessions from their US counterparts. The European Union both had ultimate veto power, and some (more limited) power in agenda setting, through the Commission's role in the negotiations.

More specifically, if adequacy was to be granted, the Commission had to have the approval of the Article 31 Committee, or at the very least, the benign neglect of the Council. But key member states such as Germany and France had signalled their scepticism about the principles and enforcement aspects of Safe Harbor. These countries, together with other doubters, were capable of blocking approval of adequacy under the qualified majority procedure: thus, they held an implicit veto over the adequacy decision. And Commission negotiators used

these states' reluctance on certain issues as bargaining ammunition in their discussions with their US counterparts. By keeping the member states informed, and by reporting their doubts back to the Americans, Commission negotiators were able to secure important concessions. This continued until the Article 31 Committee finally issued an unanimous decision in favour of the Safe Harbor in June, 2000: the EU was successful in demanding some concessions even after an outline deal had been agreed in March of the same year. The scepticism of data protection commissioners also proved useful at times: the perception that US firms might face the unconstrained zeal of independent-minded data protection commissions in the absence of an agreement helped concentrate the minds of US negotiators. Finally, the European Parliament's doubts about the Safe Harbor had less influence in the negotiations because their formal role was less important: their oversight of the adequacy finding was supposed to be limited to its procedural aspects (although see below). But the approval of Parliament is important for the long-run political legitimacy of the arrangement, which may have important consequences for the continuation of Safe Harbor, especially if any scandals erupt about the misuse of EU citizens' data by US firms.

Thus, in summation, the possibility of EU-US confrontation over privacy was averted by an "interface" solution. In bargaining over the particular form of this solution, the European Union enjoyed a position of structural advantage. The adequacy procedure allowed it to accept or reject any US proposal. Furthermore, the European Commission was able to shuttle back and forth between the negotiations (Arena I) and the other actors within the European Union (Arena III). The obduracy of actors with veto power within the European Union strengthened its bargaining hand in negotiations with the Americans. If most of the changes made in subsequent drafts of Safe Harbor went the way of the EU rather than the US, this reflects the structural advantage which EU negotiators enjoyed given the institutional framework governing the adequacy finding, rather than any lack of skill on the part of the US negotiating team.[22]

Arena II - the Domestic Debate on Privacy within the US

Even before the Directive came into effect, it had already begun to have reverberations in the US debate over online and offline privacy. The game between the EU and US began at an early stage to intersect in complicated ways with the wider political battles within the US about how privacy should be protected in the information age. By mid 1998, when the Directive began to loom large, privacy had already become a charged issue in the US. Both those who argued in favour of formal legislation to protect privacy (privacy advocates), and those who argued for self-regulation (firms and the administration) had already taken cognizance of the EU adequacy ruling, and its possible consequences. Marc Rotenberg, the director of EPIC, perhaps the most important privacy advocacy group in the debate, spoke of the EU Directive in broadly positive terms in Congressional testimony, arguing that the EU's

Directive should alert the US to how far it lagged behind in privacy protection.[23] Business, unsurprisingly, had a different analysis of the Directive. The TABD initially criticized the Directive, warning that "Data protection standards should not be used to establish new trade barriers which could hinder the development of electronic commerce between the EU and the U.S" (Trans Atlantic Business Dialogue 1997). Within the US, industry groups had already mobilized both to lobby against possible legislation, and to argue that the adequacy requirements of the European Union would be perfectly well met by existing self-regulatory initiatives. The Online Privacy Alliance (OPA) was founded by a group of major firms following a meeting in April 1998, with the aim both of convincing EU and US regulators that self-regulation was providing adequate protection to individual privacy on the WWW, and of persuading other firms to sign up to self-regulatory schemes while there was still a chance of influencing the policy agenda. The administration too was eager to persuade businesses to sign up to self-regulation, in part because of longstanding policy, but also in part to strengthen its hand in negotiations with Brussels. If the US was successfully to persuade the EU that self-regulation could protect privacy, it had to be able to point to existing and relatively widespread mechanisms of self-regulation (Magaziner 1998). In mid-1998, the US administration was clearly disappointed at how slow businesses had been to respond to this challenge. One so-called "privacy seal organization," TrustE had commenced operation, but still had relatively few members. Administration pressure led a number of large firms to approach the Better Business Bureau (BBB) to set up a privacy seal programme, but this took time to launch; the BBB had ample experience in dispute resolution, but little to none in privacy related issues.

The Safe Harbor Principles drew vigorous public and private comment. Aaron's covering letter for the draft principles had stressed that they were "not intended to govern or affect U.S. privacy regimes, which are being addressed by other government and private sector efforts," seeking to draw a line between the EU-US negotiations and the ongoing domestic privacy debate. It was clear, however from the comments of firms and business organizations that many of them disagreed. Most explicitly, TrustE and the Information Technology Association of America (ITAA) stressed in public comments that the Safe Harbor principles were likely to set the floor for domestic privacy practice, regardless of the intent of their negotiators, a fact which the ITAA urged Commerce to bear in mind during negotiations. The OPA vehemently opposed the Safe Harbor principles, implying that the Department of Commerce had almost entirely capitulated to their European counterparts in drafting the principles, and forcefully suggesting that Commerce rethink its whole approach and adopt the OPA's own (rather less demanding) privacy guidelines as a baseline for negotiation. Finally, American negotiators in practice were forced to recognize the intersection of the international and national debates. At one point in the negotiations, the US team had to deliberately slow-pedal discussions with the Europeans on the principle of onward transfer, for fear that any agreement would be seen as setting a precedent for debate over financial services reform in Congress.

US consumer advocates also objected strongly to the draft Safe Harbor standards, but from the opposite standpoint; they felt that the standards were too weak in many important aspects, and were in any event highly suspicious of the suggestion that privacy protection could be achieved through self-regulation. Privacy advocates had hoped that the external pressure of the Directive could increase pressure towards a more stringent legal approach to privacy protection in the US. In pressing their objections, the existence of TACD proved invaluable. Business interests remained more influential than consumer groups and better able to make themselves heard to policy-makers. But by the same token, TACD was more important to consumer groups than TABD was to firms, who usually had individual channels to important decision-makers. Many consumer advocates had difficulty in gaining access to a policy-making process that was almost entirely dominated by commercial interests (EPIC et al. 1998).[24] Consumer associations were also highly fragmented, making it more difficult for them to present a unified front to government; deep divisions had developed between consumer groups over the NAFTA agreement. TACD allowed these groups to overcome both hurdles in the Safe Harbor debate. First, these groups now had an official voice in the process, and opportunities to press their concerns in person on decision-makers in the administration. Second, they could reach common positions on issues such as the Safe Harbor, presenting a unified perspective. Finally, the TACD process allowed US consumer groups to exploit new channels to European officials and Members of the European Parliament (MEP's) as well as American ones. EU consumer groups, unlike their US counterparts, frequently had strong relationships with officials at the European level, thanks to the Commission's creation of policy networks on various consumer issues. US consumer and privacy groups could now use these relationships to press their concerns on EU officials involved in the Safe Harbor process, and thus seek indirectly to influence outcomes in Arena II (the US domestic debate) through acquiring leverage in Arena III (the internal EU debate) and consequently Arena I (the EU-US negotiations).

Thus, in short, the EU-US negotiations (Arena I) had an important impact on domestic US discussions on privacy (Arena II), despite the efforts of the Department of Commerce to firewall them from each other. Even before the Safe Harbor approach was articulated, privacy advocates sought to use the Directive's likely extraterritorial effects to push for formal legislation, while businesses were hostile to the Directive, in part just because they feared it would strengthen the argument for such legislation. Furthermore, actors in Arena II sought to influence negotiations in Arena I because these might in turn have knock-on effects in Arena II. Thus, businesses sought to persuade Commerce negotiators to maintain a tough line, while privacy advocates used the official channels of TACD and the unofficial channels between European consumer groups and European officials to press their case. More generally, the institutional framework of the transatlantic relationship clearly had a substantial impact on the capacity of consumer interests to make their case on privacy issues, even within the American context.

Arena III - the EU Approval Process

The granting of adequacy, as has been observed, involves a long and complicated procedure. The veto points in this procedure strengthened the Commission in its negotiations in Game I; the unwillingness of the member states and the suspicions of the Parliament and data protection commissioners were useful ammunition in its discussions with the Americans. But they were sometimes problematic for the Commission, forcing it to engage in a multi-sided set of discussions, representing the US position to European decision-makers, and vice-versa, in a process which consumed valuable time and resources. Indeed, when the Commission had finally reached an agreement with the US side that it thought was workable, the strengths turned into weaknesses. After having sold a deal to the Americans on the basis that this was the best available, given the intransigence of member states and other actors, it now had to turn around and sell the deal to those self-same intransigent actors. The Commission's adequacy decision had to meet the approval of the member states and the procedural approval of the Parliament if it was to hold.

The Commission, anticipating this, had been careful to prepare its ground. It had kept key figures in the Parliament briefed as to the state of negotiations. Even more importantly, it had sought to educate members of the Article 31 Committee as to the benefits of a deal. One key turning point in this process was a meeting in January 2000, where selected members of the Committee were ininvited to Washington DC for three days of consultations with US officials and representatives of self-regulatory organizations, most importantly TrustE and BBBOnline.

However the Parliament proved rather more difficult to persuade, even though Parliament's role was supposed to be limited to procedural oversight. The initial response to the adequacy finding came from the Parliament's Committee on Citizens' Freedoms and Rights, Justice and Home Affairs, where the rapporteur was an Italian MEP, Elena Paciotti. Paciotti was influenced in her report by the Article 29 Working Party's largely negative appraisal of the arrangement, as well as by the critical comments of the FTC, which had recently issued a harsh assessment of the effectiveness of self-regulation in providing online privacy. Further, the efforts of American privacy and consumer groups to argue against Safe Harbor in Brussels had borne fruit; the Committee "took on board the concerns of the representatives of American consumers regarding the inadequacy of the American protection system" in its discussions.[25] In referring to these, and to other principled objections, the report went considerably beyond procedural oversight, demanding that the Commission renegotiate the substance of the Safe Harbor, which it saw as insufficient in several important aspects.

The plenary debate in Parliament on the adequacy finding, which followed the rapporteur's report and its adoption in committee, showed that many parliamentarians held the hope that the Safe Harbor could be re-negotiated, and that withholding an adequacy judgement would encourage the US to adopt

formal legislation. Commissioner Fritz Bolkestein, seeking to undermine this analysis argued that

> To make approval of the determination of adequacy conditional on these changes is more likely to end up sinking the safe harbour than achieving hoped-for improvements. I would like to leave you in absolutely no doubt about this. The United States has no desire to revisit the discussions again and the Commission also takes the view that the talks are over.[26]

The Commission adopted precisely the opposite tactic to that which it had adopted in the negotiations. Now, rather than using inflexibilities in Arena III (the EU approval process) in order to improve its bargaining position in Arena I (the EU-US negotiations), the Commission sought to use inflexibilities in Arena I to improve its bargaining position in Arena III. The Commission sought to represent reality as it saw it: it was convinced that it had exhausted the concessions that the US side might have to offer, and believed that the EU could essentially take or leave the deal.[27] In the event, it was successful, but only just. Parliament passed the report by an extremely narrow majority, but without an amendment that would have made it clear that the Commission had overstepped its authority in making the adequacy decision. This could have caused a major institutional crisis between the Commission and Parliament: as MEP Palacio Vallelersundi noted in plenary, the Parliament was substantially overstepping its legal powers in seeking to require the Commission to re-negotiate the substance of the arrangement.[28] Bolkestein, who was well aware that Parliament was split over the Safe Harbor, took the position that since the Parliament had not explicitly stated that the Commission had overstepped its powers, it had exercised its powers of oversight, and not judged against the adequacy decision, which therefore stood. Parliament, not willing to start institutional warfare, tacitly acquiesced.

Thus, the approval process within the European Union was deeply interconnected with the other two arenas of decision-making. Not only did institutional inflexibilities in the process of determining adequacy (Arena III) strengthen the Commission's hand in its negotiations with the US (Arena I), but the opposite also was true; inflexibilities in the deal reached with the US (Arena I) helped the Commission to make its case in Parliament that the arrangement could not be renegotiated (Arena III). Furthermore, US privacy advocates, in their efforts to win formal privacy legislation in the US (Arena II) had sought to make their objections to the Safe Harbor deal heard in Brussels (Arena III), in order to keep the US administration under pressure. They were successful, in that they influenced Parliamentary debate against Safe Harbor, and helped ensure that Parliament remains vigilant for cracks and flaws that might appear in the Safe Harbor process over time.

Conclusions

In this chapter, I have sought to examine the processes leading up to the provision of one common good - privacy – across multiple arenas. I have suggested that these processes are inherently *political*; that is, that they involve conflict between actors with different perceptions of how the good in question is best provided, and even of whether the good should be provided at all.

This suggests a mode of analysis that does not examine common good provision in functionalist terms; rather, it sees common good provision as the possible result of political conflict. This clearly implies that common good provision in multiple arenas involves at least two different sorts of inter-relationships. The first is that which is most frequently discussed in the literature; that is, the extent to which multiple arenas make it more or less possible for certain kinds of common good to be provided (Cerny 1995). Thus, in the case at hand, the ease of data exchange between the EU and US meant that it was impossible for the EU to enforce a Directive with strong legislative protections for personal data without somehow preventing the external misuse of that data.

Yet there is a second kind of inter-relationship too, which is the one that I have emphasized in this chapter. Not only does the increasing importance of multi-arena governance pose policy *problems* but it provides political *opportunities* for various actors. To the extent that one arena of decision-making intersects with another, it may allow actors to find new ways of achieving goals that might otherwise have been impossible. More generally, through its effects on the relative bargaining power of actors, it has substantial (and differential) effects on the political constellations of the various arenas that have become related to each other. This is clearly demonstrated in the case studied in this chapter. Actors in one game may seek to use leverage in another in order to pursue their goals. Safe Harbor is a continuing process; at this point it is difficult to predict its final outcome. Debate continues over the efficacy (or lack of same) of hybrid institutions, which rely in part on private actors for enforcement. What is clear from the history of Safe Harbor is that the intersections between policy arenas have had an important influence on the relative power of actors on both sides of that debate to make their voices heard, and to strive for policy results close to their preferred outcome.

Notes

1. This chapter is one of three linked papers discussing Safe Harbor. The second links the negotiations into broader discussions of change in the EU-US relationship. The third will examine the solution reached in terms of broader arguments in international relations theory about regime formation.
2. Many privacy advocates believe that such data protection principles do not either capture the concept of privacy, or protect it in practical terms. See Davies (1997). In my argument, I bracket this debate, as I seek to examine the policy implications of privacy rather than its normative dimensions.
3. I use the example of firms on the WWW, both because it highlights many of these issues, and because it is highly relevant both to the main topic of this chapter and to

policy discussions on privacy more generally. Many, and perhaps most, of the arguments that I make can be extended to non-WWW firms.

4. See, for example, a poll carried out by Odyssey, cited in the New York Times, which finds that a massive 92% of respondents agreed, or agreed strongly with the statement ""I don't trust companies to keep personal information about me confidential, no matter what they promise." Cited in "Survey Shows Few Trust Promises on Online Privacy," *New York Times*, April 17, 2000. There have been a number of widely publicized privacy breaches or potential privacy breaches by major e-commerce firms and technology firms, including Geocities, Real Networks, Doubleclick, Intel and Microsoft.

5. Robert E. Litan, Testimony: The European Union Privacy Directive, given before the House Committee on International Affairs, May 7, 1998.

6. For a reputation-based account of the persistence of firms, see Kreps (1990).

7. On compliance, see Tanja Börzel, this volume.

8. I note that ideational factors also play an extremely important role, so that "simple" institutional arguments have only limited explanatory power. I explore ideational factors in greater detail in forthcoming work.

9. There are however safeguards for the online privacy of children in the Children's Online Privacy Protection Act (1999).

10. The term "adequate" had been substituted after heavy lobbying from business interests for the term "equivalent", which was used in the original draft of the Directive. See Regan (1999). Adequacy clearly pre-supposed a lower standard than equivalency, and a wider variety in the approaches that could be considered to meet the requirements of the Directive.

11. Discussions have been ongoing between the European Union and the International Chamber of Commerce on the subject of model contracts. At the time of writing, a draft set of clauses has been issued for public discussion; business has indicated its dissatisfaction with them.

12. The Article 31 Committee should not be confused with the Article 29 Working Party, which I describe below.

13. The FTC act does not cover firms in certain sectors (although in air-transport, for example, there is an equivalent set of obligations and enforcement mechanisms), leading to serious worries among privacy advocates.

14. I limit my remarks here to Safe Harbor's *direct* effects, as measured in terms of the number of firms adhering to it. As I hope to elaborate in later work, Safe Harbor's *indirect* effects appear to be substantial, and may in the long run be more important.

15. Consumer groups were not directly involved to the same extent as their US counterparts.

16. See Department of Commerce (1997). Reidenberg (1999) has a useful short discussion of policy debates on privacy within the US administration during this period.

17. More accurately I should say "disastrous for some." A stand-off between the EU and US would have had substantial negative implications for commercial exchange, and consequently for state actors responsive to the needs of commerce. But it may well have had advantages for players in other games. Some US privacy advocates, for example, might well have preferred a continuing and volatile stalemate on the international level: this would have helped increase the pressures on domestic legislators to introduce formal privacy protection.

18. Shaffer (2000). For a somewhat different emphasis, see Reidenberg (1999), and Swire and Litan (1998).

19. Magaziner's threat of WTO action may interpreted in another way though, as a signalling device to show that the US viewed this issue seriously, and was prepared to make life highly uncomfortable for the EU if it actually blocked data flows. Interview

with Ira Magaziner, conducted September 21, 2000. Certainly, EU negotiators were highly worried about how the administration would respond to substantial blockages in data flow between US companies and their European subsidiaries.
20. Interview with US negotiator.
21. Interview with Commission negotiator.
22. Of course, the Europeans could not persuade the US to move further than its minimum acceptable position. Further, the US side did have substantial agenda-setting power, which it used - the fact that it persuaded the EU side finally to accept a solution with substantial self-regulatory elements is evidence of this.
23. Marc Rotenberg, Testimony given before the House Committee on International Relations, May 7, 1998.
24. See, for example, the complaints in the "Letter Regarding a Proposed White House Conference on Privacy" sent to the Secretary for Commerce by various advocates, scholars and experts in the field of privacy on February 26, 1998. <http://www.epic.org/privacy/internet/daley_ltr_2_26_98.html >(checked Jan 14, 2001).
25. Available at http://www3.europarl.eu.int/omk/omnsapir.so/debats?FILE=00-07-03&LANGUE=EN&LEVEL=DOC&GCSELECTCHAP=8&GCSELECTPERS=92 (Checked Jan 14, 2001).
26. See the discussions in the Parliament's Plenary debate, July 3, 2000, available at http://www3.europarl.eu.int/omk/omnsapir.so/debats?FILE=00-07-03&LANGUE=EN&LEVEL=DOC&GCSELECTCHAP=8&GCSELECTPERS=94 (Jan 14, 2000).
27. Interviews with Commission negotiators.
28. Available at http://www3.europarl.eu.int/omk/omnsapir.so/debats?FILE=00-07-03&LANGUE=EN&LEVEL=DOC&GCSELECTCHAP=8&GCSELECTPERS=89 (Jan 14, 2000).

References

Aaron, D. 1999. Remarks of David L. Aaron, Under Secretary of Commerce for International Trade before the Information Technology Association of America Fourth Annual IT Policy Summit, March 15, 1999.

Bennett, C. 1992. *Regulating Privacy: Data Protection and Public Policy in Europe and the United States.* Ithaca, NY. Cornell University Press.

———. 1997. Convergence Revisited: Toward a Global Public Policy for the Protection of Personal Data?. In *Technology and Privacy: The New Landscape*. ed. Rotenberg, M. and P. Agre. Cambridge, Mass. The MIT Press.

Cerny, P. 1995. Globalization and the Changing Logic of Collective Action. *International Organization* 49: 595-625.

Data Protection Working Party. 1998. *Working Document: Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive*. Brussels. European Commission, Directorate General XV, D/5025/98.

Davies, S. 1997. Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity. In *Technology and Privacy: The New Landscape* ed. M. Rotenberg and P. Agre. Cambridge, Mass.

Department of Commerce. 1997. *Privacy and Self Regulation in the Information Age*. Washington DC. Department of Commerce NTIA.

Hardin, R. 1982. *Collective Action*. Baltimore, Md. Johns Hopkins University Press.

Jupille, J. 1999. The European Union and International Outcomes. *International Organization* 53: 403-425

Kreps, D. 1990. Corporate Culture and Economic Theory. In *Perspectives on Positive Political Economy*, ed. Alt, J. and K. Shepsle. Cambridge. Cambridge University Press.

Magaziner, I. 1998. Speech given in Context of IBM Privacy Symposium <http://www.ibm.com/iac/transcripts/internet_privacy_symp/iramagaziner.html> (checked October 10, 2000).

Mayer-Schönberger, V. 1997. Generational Development of Data Protection in Europe," in *Technology and Privacy: The New Landscape*. ed. Rotenberg, M. and P. Agre. Cambridge, Mass. The MIT Press.

Meunier, S. 2000. What Single Voice? European Institutions and EU-U.S. Trade Negotiations. *International Organization* 54: 103-135

Olson, M. 1965. *The Logic of Collective Action*. New York, NY. Schocken.

Peterson, J. and M. Green Cowles. 1998. Clinton, Europe and Economic Diplomacy: What Makes the EU Different?. *Governance* 11: 251-271.

Regan, P. 1999. American Business and the European Data Protection Directive: Lobbying Strategies and Tactics. In *Visions of Privacy,* ed. Bennett, C. and R.Grant. Toronto. University of Toronto Press, 1999.

Reidenberg, J. 1999. The Globalization of Privacy Solutions: The Movement towards Obligatory Standards for Fair Information Practice. In *Visions of Privacy,* ed. Bennett, C. and R.Grant. Toronto. University of Toronto Press.

Ronit, K. and V.Schneider. 1999. Global Governance through International Organizations. *Governance* 12: 243-266.

Scharpf, F. 1997. *Games Real Actors Play: Actor-Centered Institutionalism in Policy Research.* Boulder. Westview Press.

———. 2000. Institutions in Comparative Policy Research, *Comparative Political Studies*: 762-790

Shaffer, G. 2000. Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards. *Yale Journal of International Law* 25 :1-88

Swire, P. and R. Litan. 1998. *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive.* Washington DC. The Brookings Institution.

Trans Atlantic Business Dialogue. 1997. "TABD Priorities for the Mid-Year U.S.-EU Summit, May 13, 1997," < http://www.tabd.org/recom/97priority.html> (checked. Jan.13, 2001).

George Tsebelis. 1990. *Nested Games*. Berkeley, Ca. University of California Press.