Privacy in the Digital Age: States, Private Actors and Hybrid Arrangements

Revised Version, November 2003

Henry Farrell
Assistant Professor
University of Toronto
Email: farrell@utsc.utoronto.ca

.

Section I - Introduction

Privacy has emerged as a key regulatory issue in the wake of the information and communications revolution. New technologies have brought new problems; they have made it more difficult for individuals to maintain their privacy (or for other actors to protect it on their behalf), while also giving rise to complex issues of global regulation.

The right to privacy, however it is defined, rests on the individual's ability to control information about himself or herself, and how that information is disseminated and used. Advances in information and communications technology have had profound consequences for individuals' ability to exercise that right. New technologies, including, but not limited to, the World Wide Web (WWW) make it far easier for third parties to gather information about behavior, and potentially to link this information to specific individuals. Data mining and information sifting techniques, together with access to computing power, make it easier to analyze that information and make it useful. These new technologies make it far more difficult for individuals who value their privacy to maintain it. The sheer volume of information, and of uses to which information can be put, also make it more difficult for specialized agencies (such as data protection commissioners) to protect individual privacy.

Not only has communication technology made it more difficult to protect privacy in and of itself, but the vast increase in cross-border data flows has generated new problems of international governance. Different countries have adopted very different approaches to privacy protection. For example, the member states of the European Union

(EU) have adopted increasingly stringent legal measures to protect privacy,[1] most notably the EU-level Data Protection Directive (discussed below). Many other states, such as the US, have either opted for an approach that privileges voluntary forms of self regulation, or have not adopted any substantial measures at all. In states within the developing world, privacy legislation is typically a low priority, compared to more pressing, material needs. These radical differences of approach are increasingly the source of international disagreement, as communications technologies such as the Internet lead to increased interdependence between countries.[2] States may reasonably be concerned that their particular approach to privacy protection may be undermined if firms or individuals export data outside their jurisdiction and process it there. Thus, for example, the European Union has introduced measures in its Data Protection Directive that threaten to block data flows to countries that do not provide "adequate" privacy protections. However, countries that have different or no means for privacy protection may for their part feel threatened by the efforts of other countries to create a high international threshold for privacy.

What explains this varying pattern of privacy regulation? In this chapter, I argue that privacy regulation has always had a strong international component. To adapt Peter Gourevitch's famous analysis, domestic privacy regulation is best captured through the "second image reversed;" that is, through examining how international factors may translate into domestic outcomes. However, the causal impact of international factors is likely to depend on two key intervening variables. First of these is existing national institutional traditions, which affect whether individual states do, or do not, take up

[1] Although, as this chapter discusses later, some of these protections are being quietly watered down and abandoned.
[2] Farrell (2003).

specific modes of protecting privacy. Second is state bargaining power; stronger states may be able to force weaker states to reform their domestic policy, regardless of these weaker states' underlying preferences. While I do not propose an explicit model with hypotheses about the circumstances under which the one, or the other factor will be most important, I do show how these factors in combination provide a very considerable degree of insight into the development of institutions governing privacy at different instances over the last thirty years. I also show the relevance of these factors for policy, and for the viability of different policy recommendations in the current international context.

How have the institutions protecting privacy developed over the last thirty years? In a first phase of development, an "epistemic community" of policy experts developed a set of fair information practices that served as a template for comprehensive domestic laws in many domestic contexts. However, one key actor – the United States – was unwilling to accept a comprehensive privacy law based on fair information principles. Because of US bargaining strength, the US was able to go it alone, without acceding to external pressures.

In a second phase, states sought to create international instruments to protect privacy on the basis of their existing domestic institutions and preferences. However, irresolvable divergences of interest among powerful states led to stalemate, and the creation of two international instruments, one of which is non-binding, but which commanded assent among advanced industrialized democracies, and the other of which involved strong binding commitments, but was not acceded to by the US and other non-European states.

In the current phase of development increased pressures from interdependence are again leading to changes in the privacy agenda. On the one hand, European Union strong-arming is leading many countries to converge on an EU model of data protection law. EU pressure has further induced the US to enter into an international arrangement that allows US firms to comply to privacy standards that have been set in negotiations with the European Commission. On the other, new pressures (especially in the wake of September 11) are leading to a downgrading of privacy standards in many countries, including EU member states which had previously pushed for strong privacy standards.

Section II – Evolution of the Privacy Debate and International Institutions

Current controversies over privacy have their roots in debates on privacy that began in the late 1960's and early 1970's, and in states' differential response to these debates. These began in worries about how state administrations might use mainframe computers.[3] The demand of state bureaucracies for technical means to collate and analyse individual-level information seemed insatiable, and there were few legal safeguards to protect privacy.[4]

Concerns over privacy were especially strong in continental Europe, which had recent memories of how personal information had been abused during the era of National Socialism. They were also present in the US, with its strongly individualistic political

[3] See further, Bennett (1992).
[4] See further, Flaherty (1979).

tradition. In due course, they were manifested in formal legislation across a large number of industrialized countries, intended to provide formal protections for individual privacy.[5]

Experts in the field soon began to reach a rough consensus about how privacy might best be protected through "fair information principles." This cross-national "epistemic community" played an important role in realigning domestic debates within various countries, and in encouraging states to adopt laws which instantiated appropriate principles of privacy protection.[6] The fair information principles that these experts promulgated laid down basic guidelines about how information ought to be treated, in order best to protect individual privacy. Although different countries legislated for privacy at different times, and formulated their legislation through quite different processes, there was a remarkable degree of convergence across states at the level of principle.[7] However, there were notable differences in states' enthusiasm for privacy protection. In some states, such as the United Kingdom, privacy legislation was as much motivated by the fear of external difficulties as by enthusiastic debate of the ideas put forward by privacy experts.[8] In other contexts, most notably the United States, fair information principles exerted a weaker influence on policy debates than elsewhere.

These differences began to manifest themselves in clear policy divergences, as the debate over privacy shifted to include commercial as well as governmental uses of personal information. As firms began to develop their own computerized databases, and to use them for commercial purposes, it became clear that state administrations were not the only potential invaders of privacy. Even where there was rough consensus about

---

[5] Bennett (1992).
[6] Bennett (1992).
[7] Ibid; Mayer-Schönberger (1997).
[8] Bennett (1992).

appropriate principles of privacy protection, there were stark disagreements among states about how and where these principles should be implemented. Many mainland European countries began to develop comprehensive data protection laws that sought to provide broad legal protection to privacy across a variety of social and economic arenas. In contrast, the US (and, at a later juncture, Japan and North Korea) introduced legislation that applied privacy standards to the federal government, but failed to extend comprehensive legal protections to the private sphere, instead relying on a patchwork of self-regulation and narrowly based laws. In the US case at least, this failure to adapt a comprehensive approach can be traced back to a different constellation of state-private actor relations, and to the hostility of influential business actors to new legislation that would curtail their ability to use personal information. Instead, business actors suggested self-regulation as a viable means to privacy protection, and in some cases went so far as to introduce self-regulatory schemes which were rather more notable for rhetoric than for substantial consumer protections.

Thus, in this first phase, it is clear that international factors – the creation of a transnational epistemic community of privacy experts – did have an important influence on domestic outcomes. As Colin Bennett demonstrates, these experts succeeded in creating a rough consensus around "fair information principles" that then played an important part in guiding the creation of national legislation in many advanced industrialized democracies. However, the influence of this epistemic community was itself limited by domestic factors. In some national contexts – most notably many of the countries of mainland Europe – it proved possible to adopt comprehensive laws applying fair information principles. In other contexts, such as the UK, governmental actors were

less enthusiastic to adopt comprehensive new laws but recognized that it was probably in the interests of the UK to introduce legislation, given the increasingly close economic and political connections between the UK and mainland Europe. In the US, in contrast, both existing institutional frameworks and the opposition of powerful domestic actors meant that the US government was disinclined to introduce comprehensive laws. Furthermore, in contrast to the UK, the US was not deeply embedded in a dense web of relations with countries that were introducing comprehensive privacy protections, and was indeed in a strong bargaining position vis-à-vis other industrialized democracies. US governmental actors thus had neither strong internal nor external motivations to adopt comprehensive privacy legislation.

These disparities led to considerable disagreements among advanced industrialized democracies in a second stage of debate – when states sought to build upon their pre-existing national legislation to create international institutions in the sphere of privacy. The international debate on privacy came to the fore as the result of increasing interdependence; as firms began increasingly to move data over national borders, international commercial transfers of data became the subject of controversy. Over the late 1970's and early 1980's, many states began to worry that Transborder Data Flows (TDF) threatened their ability successfully to exercise their sovereign authority.[9] More specifically, even though the level of cross-border data flows was still relatively limited at this point,[10] some states were concerned that their domestic privacy legislation would be undermined if firms were able to transfer personal data to a laxer jurisdiction. This led to disagreement between the United States, which had weak to non-existent legal

[9] For a jaundiced but convincing account of the burgeoning and collapse of the TDF debate, see Drake (1993).
[10] Bennett (1992).

protections for privacy in the commercial arena, and those European states which had enacted comprehensive data protection laws. The latter pushed for strong international instruments to protect privacy, while the US sought to water down these proposals, which some US commentators perceived as barely masked protectionism.[11]

These disagreements led to arguments over whether binding international standards on privacy were appropriate. Debates were conducted in two main fora; the Council of Europe, and the Organization for Economic Cooperation and Development. The Council of Europe, a broadly based organization has a membership consisting of European states with the Vatican, the United States, Canada, Japan and Mexico as observers. States within the Council of Europe adopted the 1981 *Convention for the Protection of Individuals With Regard to the Automatic Processing of Personal Data*. This Convention laid out rules for information privacy that reflected fair information principles. It also forbade parties to the Convention from stopping data flows to other such parties for the sole purpose of protecting privacy, except when the other party did not protect certain kinds of data that were protected in the originating country. The Convention did however allow adhering countries to block data flows to third party jurisdictions that had not signed up to it.

The OECD also reached agreement in 1980 on the so-called *OECD Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data*. In contrast to the Convention, the Guidelines were not substantively binding on the states that had agreed to them. The Guidelines may best be interpreted as an effort to woo the United States by stages into signing up to an international arrangement on privacy.[12]

---

[11] See further Drake (1993), Bennett (1992).
[12] Drake (1993).

However, the OECD Guidelines had few teeth in terms of enforcement, precisely because of the desire of other states to persuade the US to agree to them, and because of US bargaining power (which was rather stronger in the OECD than in the Council of Europe). The result was predictable. While the US was a signatory to the Guidelines, its efforts to implement them were limited to (short-lived and largely ineffective) exhortations to US firms to abide by them.[13]

By the mid-1980's, the international policy debate on transborder data flows was, for all intents and purposes, over. The US, and large multinational corporations had successfully clamped down debate on multilateral measures to control data flows.[14] However, these data flows themselves continued to increase in volume, especially between advanced industrialized economies. The continued differences in approach to privacy protection led to important policy dilemmas, which non-binding statements of intent, like the OECD Guidelines, did little to address. Countries which placed a high premium on formal laws to protect privacy, such as Germany and France, legitimately feared that cross-border data transfers could undermine their laws, by allowing actors to transfer personal data to jurisdictions with weak or non-existent privacy protection, and processing it there. However, any efforts by these countries to control data flows would in turn have consequences for third party countries with different approaches to privacy.[15]

Thus, at the end of this second phase, disagreements between advanced industrialized democracies had led to the creation of two international instruments in privacy protection. One of these instruments, the Council of Europe Convention provided for comprehensive – and binding – rules protecting privacy. The countries adhering to

[13] Ibid.
[14] Ibid.
[15] See further, Farrell (2003).

this Convention were thus willing to accede to strong international rules. The second international instrument, the OECD Guidelines, was non-binding, and thus of uncertain consequence. This allowed states such as the US to sign up to the Guidelines, which they perceived as aspirational, if not indeed a complete dead letter. Again, because of the US's disproportionate bargaining power, American negotiators were able to avoid signing up to real commitments that would have obliged domestic change. The OECD Guidelines, rather than resolving disputes among industrialized democracies over privacy protection, papered over them.

The third – and current – phase of privacy regulation began in the early 1990's. It is a product of the wave towards comprehensive privacy protection in many industrialized democracies in the first phase, and the failure of these democracies to create a binding agreement that would include countries such as the US in the second. In order to cement, harmonize and rationalize national data protection laws, the European Union conducted discussions throughout the early 1990s on a comprehensive EU level framework. This culminated in the EU's *Directive on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data*, more tersely and conveniently dubbed the Data Protection Directive, which took effect in late 1998. This Directive had its origins in European worries that the EU's creation of a single Internal Market was being hampered by differences in data protection regulations; some EU member states were using data protection law to block data transfers to other member states that had weaker privacy protection. The Directive was drafted to ensure that all member states had broadly similar privacy standards in their domestic legislation,

and thus to remove any justification for blockages of data flows within the EU.[16] However, the Directive is more than just an intra-European house-cleaning exercise; it has also had important consequences for actors outside the European Union. The Directive mandated the European Commission to decide, under the strictures of a comitology procedure,[17] whether third countries had "adequate" protection for personal data or not. In cases where the Commission found that a country did not have adequate protection, member states were enjoined to prevent data transfers to that country, except under highly specific circumstances laid out in the Directive.

This led immediately to controversies with countries such as the US, which did not have data protection laws, or which had data protection laws that were likely to be judged inadequate by the Commission. This controversy was especially acrid because of the potential knock-on consequences of the Directive for the regulation of e-commerce. The prevailing wisdom in the US, and, to a lesser extent, in other advanced industrialized economies, was that e-commerce should only be regulated by government insofar as was absolutely necessary.[18] The Data Protection Directive, even though it had been conceived and drafted before the e-commerce revolution, was perceived by US business and policy makers as an EU effort to re-impose government control over e-commerce, and thus as setting a potentially dangerous precedent. While US firms and others successfully lobbied to weaken the Directive's requirements (originally, the Directive had required that third party jurisdictions have "equivalent" rather than merely "adequate" protections),[19] it was

[16] Regan (1999).
[17] For discussion of the comitology system, see Bergström, Farrell and Héritier (unpublished).
[18] Farrell (2003).
[19] Regan (1999).

still clear that the Directive could have quite substantial consequences for third party jurisdictions.

Between 1998 and today, the European Union has negotiated with various non-EU states over the circumstances under which the Commission would be prepared to find their systems of data protection "adequate" and thus obviate the threat of data flow blockages. Negotiations with the US received the most attention; the US administration initially argued strongly against the Directive, and sought to encourage an alternative approach based on self-regulation and so-called "privacy seal" organizations, such as TRUSTe and BBBOnline.[20] The US also expressed itself willing to use its bargaining strength to prevent the EU from imposing a solution upon it, and EU negotiators recognized that they were unlikely to bring through major domestic reforms within the US. However, the EU still refused to accept pure self-regulation as sufficient. EU-US negotiations culminated in the so-called "Safe Harbor" arrangement, in which the EU withheld a general adequacy judgment from the US, but announced that specific US firms, which voluntarily signed up to an agreed set of privacy principles, would be considered to have satisfied the requirements for adequacy.[21] Enforcement of these principles involved a mixture of public and private actors; self-regulatory organizations such as TRUSTe and BBBOnline could provide an initial line of defense, while the US Federal Trade Commission and EU's Data Protection Commissioners also played an important role.[22]

[20] I discuss privacy seal or web seal organizations in greater detail below.
[21] See Farrell (2002, 2003), Heisenberg and Fandel (2002) and Kobrin (unpublished), Long and Quek (2002) and Shaffer (2000), for discussion of the Safe Harbor negotiations.
[22] For a more detailed discussion of Safe Harbor, see Farrell (2003).

The EU has been much less inclined to make concessions in its discussions with weaker trading partners.[23] The consequence has been that countries in the developed world, and increasingly within the developing world, are seeking to implement legislation that reflects EU priorities, in order to be declared adequate.

However, even while the EU has been pushing other countries to implement stronger data protection laws, it has been weakening its own protections, as have other countries, in the wake of the events of September 11, 2001. Policymakers' perception of the relationship between security and privacy have shifted so that measures which would previously have been unthinkable, because of their negative consequences for privacy, have been implemented with little debate. Many of these measures have little, if anything to do, with the prevention of terrorism. State security and policing services are succeeding in getting privacy-intrusive measures passed that they have advocated for years, regardless or not of whether these measures address terrorism directly.[24] Even those states which have had comprehensive privacy legislation in the past are substantially weakening their protections. In particular, new battles are beginning to develop over traffic data retention; government requirements that telecommunications companies and Internet service providers (ISPs) retain information on their clients' communications traffic, and make that information available to the state for law enforcement and anti-terrorist purposes.

As of yet, these new pressures have not led to the creation of extensive multilateral arrangements, with the partial exception of the Council of Europe's Convention on Cybercrime (which was, however, drafted before September 11; see

[23] See below.
[24] I owe this point to Maria Farrell with whom I hope to address these problems in later collaborative work.

further, Hosein, this volume). However, more worryingly, they have led to the creation of transgovernmental regulatory networks[25] which increasingly seem to be driving privacy policy – and not in a privacy-friendly direction. If an epistemic community of privacy experts helped drive the international convergence on data protection principles at an earlier juncture, officials in justice, home affairs, and security ministries and agencies seem to be playing a similar role in many pertinent areas of policy. Furthermore, one may tentatively predict that these officials will likely play a more important policy role than privacy experts over the medium term, precisely insofar as they play a more direct and important role in policy-setting. More generally, privacy advocates face a very substantial challenge if they wish to develop new instruments to hold state actors accountable for privacy violations, especially in the current political climate, where privacy intrusive security measures are perceived by many as legitimate.[26]

Section III-1 – Current Debates on Privacy

As discussed above, privacy questions are being debated at a variety of levels, both domestically and internationally. While these levels intersect, they do so in somewhat confusing ways. Accordingly, in this section, I set out to describe the two key arenas in which the privacy debate is playing out at the moment; international relations among states (which may further be subdivided into relations among advanced industrialized democracies, and relations between advanced industrialized democracies and countries in the former Eastern bloc or developing world); and domestic relations

[25] Slaughter (2003).
[26] See further, Hosein (this volume).

within advanced industrial democracies between the state, commercial actors and citizens.

Section III-2 – Relations among States

International relations among states in the sphere of privacy involves two main subsets of relations, each of which has a quite different logic. Relations *among* advanced industrialized states receive the most attention in the literature, and generate the most public disputes, but relations *between* these states and states in the developing world have the potential to generate substantial policy problems in the future.

As described in the previous section, advanced industrial democracies have frequently disagreed over privacy regulation. Important differences in how these states regulate privacy have led increasingly to international disagreement. In some cases, there are substantial divergences; for example, differences between countries which have comprehensive privacy laws based on fair information principles and associated formal mechanisms of protection (data protection commissioners), and countries which do not. In other cases, differences are less pronounced (specific differences, for example, in how fair information principles are applied in the legislation of different countries). In both instances there are pressures for convergence.

Currently, the main motor force for convergence is rather different than it was at previous junctures. The key factor is not a community of policy experts, or agreed multilateral instruments, but the European Union's Data Protection Directive, and its

external consequences.[27] Since the Directive has come into force, third party jurisdictions have increasingly found themselves forced to adapt privacy standards along European lines.[28] In the eyes of some, this is leading to the creation of a new international privacy regime.[29]

Even given the notorious elasticity of the concept of regime,[30] this may be overstating the case. The end result is an array of bilateral negotiations; the EU's requirement of "adequacy" still permits a considerable degree of variation across different systems.[31] However, the EU's demands upon its trading partners are still resulting in an upward ratcheting of privacy standards across the developed world, even if this is not leading to general convergence upon a regulatory endpoint.

The precise consequences of the Data Protection Directive for third countries vary according to (a) the fit between the country's existing privacy protections and EU demands, and (b) the country's bargaining strength vis-à-vis the EU. The Safe Harbor arrangement, discussed in the previous section, reflects the unique bargaining strength of the US, as well as that country's profound unwillingness to introduce comprehensive privacy legislation along EU lines. Thus, the Safe Harbor serves as a kind of "interface solution,"[32] minimizing conflict between the EU's emphasis on formal enforcement, and the US self-regulatory approach. It remains to be seen whether Safe Harbor will provide a

---

[27] The Data Protection Directive is, of course, itself an international instrument, but the EU is typically considered by international relations scholars as a single actor in its external aspects, rather than a multilateral forum.

[28] Bennett (1992) argues that Britain introduced data protection legislation largely in consequence of perceive external pressures, but argues that it was the exception rather than the rule at this phase of development.

[29] Heisenberg and Fandel (2002).

[30] Haggard and Simmons (1987).

[31] Indeed, there is still some divergence of implementation within the European Union; EU Directives, unlike Regulations, tend to set general principles which may be applied in different

[32] Scharpf (1994), Farrell (2002, 2003).

long term solution to EU-US disagreements over privacy; to date, relatively few US firms have signed up to the arrangement. However, it is significant as an exemplar of a new trend towards mixtures of state and private enforcement as a solution to international policy problems.[33]

Countries with less bargaining leverage than the US have had difficulty in reaching compromises that allow them to maintain their existing approach to privacy. This has led to some disgruntlement, especially where the EU asks countries to make substantial changes to their existing system. Australia, for example, has a federal Privacy Commissioner, and has introduced recent legislation enhancing privacy protections, which in part seeks to respond to European demands. Australia's Internet Industry Association has furthermore sought to implement a code of privacy practice based on the Safe Harbor Principles. However, European data commissioners[34] and Commission officials still find Australian protections to fall considerably short of adequacy, and clearly believe that they can wring further concessions from the Australian government. Australian officials have responded that they are being held to a higher standard than the US,[35] with the implication that they have grounds for a WTO action.[36] Other countries have had less difficulty in conforming to EU requirements. Canada and Switzerland have received positive adequacy judgments from the Commission, while New Zealand's

---

[33] See Dryden, John. "The Work of the OECD on Electronic Commerce." Available at http://www.oecd.org/subject/e_commerce/Ottowa_speech.pdf (checked October 10, 2000).

[34] See Data Protection Working Party, Opinion 3/2001 on the Level of Protection of the Australian Privacy Amendment (Private Sector) Act 2000, Available at http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp40en.htm (checked February 15, 2003).

[35] See Peter Ford, "Implementing the Data Protection Directive: An Outside Perspective," available at http://www.europa.eu.int/comm/internal_market/en/dataprot/lawreport/speeches/ford_en.pdf (checked February 15, 2003).

[36] The General Agreement on Trade in Services (GATS) has an exception for measures taken to further data protection, but requires that these measures not be applied in a discriminatory fashion. See further Shaffer (2000), Swire and Litan (1998). Thus, if the EU were to block data flows to Australia, the Australian government would have a *prima facie* case for WTO action.

privacy laws are close enough to EU requirements to require only minor legislative changes. There still remain some states where EU pressures do not seem likely to result in legislative changes in the near future. It is possible, but not certain by any means that there may be an upward ratchet effect that may eventually lead to changes in such states; multinational firms that have to obey EU rules in any event may acquiesce, or even actively press for changes in these countries over the longer term.[37] In the shorter term, efforts to use EU standards to provide internal leverage within these systems, as well as efforts to use existing programs (such as Safe Harbor in the US) may have at least a palliative effect.

In some respects, relationships between industrialized states, and middle income states within the developing world resemble relations among industrialized states themselves. The same is true of the new democracies of Central and Eastern Europe. However, there are clear differences. Most obviously, there are disparities of power. Even where developing countries have relatively substantial markets (as, for example, India), they still tend to have less clout in bilateral or multilateral negotiations than their size would suggest. But there are also differences as well in the extent to which they are concerned with privacy as a policy issue. Colin Bennett's judgment in 1992, that privacy is primarily a concern for industrialized countries, still has some force.[38] Most countries in the developing world have little interest in formal protections for privacy as such. Authoritarian regimes have little more interest in promoting privacy than in promoting other political rights that might have destabilizing implications for their rule, while poorer democracies usually have more pressing material needs to address, and limited

[37] Shaffer (2000).
[38] Bennett (1992).

resources with which to address them. There are some notable exceptions to this generalization. The Republic of South Africa, for example, does enshrine the right to privacy in its constitution, although it has yet to enact a data protection law; there is vigorous political debate over the extent to which the state should be able to monitor private communications. Hong Kong, insofar as it can be considered to be part of the developing world, has strong and comprehensive legislation protecting privacy, as well as a Privacy Commissioner. However, these are among the few exceptions to a more general pattern.

Even if developing and middle-income states have historically had little interest in privacy policy, they are increasingly finding that such an interest is forced upon them, for external reasons. Again, the European Union's Data Protection Directive is a key factor. Countries that wish to maintain good trade relations with the European Union, and encourage inward investment, are finding themselves obliged to conform to Europe's external requirements. Argentina, for example has introduced comprehensive legislation along European lines, while Peru has introduced specific sectoral legislation following the European model, and has established a Commission to draft more comprehensive reforms.[39] Other countries, such as India, face increasing pressure to enact legislation from their own firms, which are fearful of losing important markets.[40]

Nowhere is EU influence more marked than in the former states of the Eastern bloc, most of which are prospective EU members. Candidate countries must enact comprehensive privacy legislation along the lines laid out in the Directive as part of the *acquis communautaire*; the set of formal obligations associated with EU membership.

---

[39] Andrews and Privacy International (2002)
[40] See ibid, for discussion of the nascent debate in India.

Thus, they are not only enacting laws that reach the less onerous standard of adequacy, but laws that closely approximate the laws of existing EU members (or, more precisely, those EU members that have implemented the Directive in their domestic legislation; a few have yet to do so).

In summary, the EU's Directive is having a substantial external effect on middle income countries within the developing world, and is substantially determining the privacy laws of candidate countries within the former Eastern bloc. Where its effects are more ambiguous are in the poorest developing countries, as well as some middle income countries (such as Russia) where the rule of law is at best imperfectly established. Some of these countries are seeking to respond to the EU's perceived demands. However, there is little substantial likelihood that they will receive adequacy judgments, which depend not only on the formal protections offered to privacy, but on the degree to which these protections are likely to be implemented in practice. Countries in which legal institutions are underfunded, or ineffective, will find it difficult to conform to EU requirements. On the one hand, they cannot credibly guarantee that comprehensive privacy laws will be enforced if they are enacted. On the other hand, they are ineligible for Safe Harbor style solutions, even if the EU adopted a more liberal approach to negotiating such solutions. Commission officials have made it clear that such solutions are only appropriate in well-functioning legal systems.[41]

If one leaves the problems of weak states to one side, the above might suggest that the long term international outlook for privacy is positive; a "ratcheting upwards" to Europe-set standards. However, an important set of complicating factors has recently begun to emerge, due to state initiatives to combat crime and terrorism. The Council of

[41] Author's interviews with Commission officials.

Europe's Convention on Cybercrime, which has yet to be ratified, requires participating states to legislate for new surveillance capabilities on the Internet and to use these capabilities where necessary to cooperate in criminal investigations.[42] This instrument was formulated in a poorly publicized series of negotiations in the period leading up to September 2001.

Since the events of September 11, pressures to curtail privacy in the fight against terrorism have increased dramatically. The US administration has demanded – and received – changes in European policy that have important knock-on consequences for the existing EU privacy regime. In a letter dated October 16, 2001, the US administration requested that the European Union "consider data protection issues in the context of law enforcement and counterterrorism imperatives," and that the EU institute a series of policy changes, including the modification of draft legislation so as to allow the retention of traffic data.[43] The EU has acquiesced to this request. EU-level legislation protecting the privacy of traffic data has been dramatically weakened, while European member states have agreed to a wide-ranging exchange of police and security information with the US through Europol. It is likely that over the next few years, the fight against terrorism will serve as a reason (or excuse) for new international, multilateral and bilateral initiatives that will substantially weaken privacy protections in "high" privacy countries such as those of Western Europe. Policy makers speak of a necessary tradeoff between privacy and security; while this grossly mischaracterizes the complex relationship between the two, it is likely to shape public debate and relevant public policy over the

[42] Hosein, this volume.
[43] Letter available at http://www.statewatch.org/news/2002/feb/useu.pdf (checked February 15, 2001).

coming decade. Thus, there are new international pressures for the weakening of privacy protections in many jurisdictions; I return to this point in the next section.

Section III-3 - Privacy Debates within Advanced Industrialized Democracies

The international disagreements over privacy that have been described above intersect with disagreements at the domestic level in many Western democracies.[44] The specific constellations of these disagreements vary according to political setting and issue area. Two sets of disputes are especially important. First are continuing arguments over the proper balance between law and private enforcement. Second are new disagreements over government's access to information on people's behavior on the Internet and other communication networks.

First, in domestic contexts where there are weak or nonexistent laws governing business's use of personal information, privacy advocates have sought comprehensive legislation to prevent privacy abuses by firms. Firms, in contrast, have typically lobbied against such legislation, claiming (with more fervor than credibility) that market forces and self-regulation suffice to protect consumer interests. Here, privacy advocates seek to defend the interests of citizens against abuses by firms, which in turn have tried to use their clout with the government to block change. A new set of battles is being fought over the appropriate mix between government and private enforcement, as industry groups and web seal organizations expand the range of self-regulatory privacy regimes.

Here again, the US is the key test case of a prominent state without effective and comprehensive privacy laws. In the late 1990's, US-based privacy advocates had hoped

[44] See further, Farrell (2002).

to use external pressures, especially the EU's Data Protection Directive, to press for domestic privacy laws that would meet international standards. However, they faced formidable obstacles. The US political system makes it notoriously difficult to enact major reforms, because of its many veto points,[45] and it furthermore privileges business over consumer interests to an extraordinary degree. The US administration, far from acceding to European demands, instead proposed an alternative vision of privacy protection on the WWW, which would rely on self-regulation.[46] In the short to medium term, the administration proposed reliance on self regulatory web seal organizations, which would award seals to web sites that adhered to certain privacy standards. US administration officials argued that this would provide consumer protection – consumers could choose only to do business with websites that had signed up to these seal programs. Ira Magaziner, the architect of the White Paper, argued that self-regulatory organizations would eventually be superceded by technological tools, which would give individuals control over precisely how they shared their information.[47] The administration's position reflected the views of key figures in the US information technology industry, who were vigorous proponents of a hands-off approach to the regulation of e-commerce.

US administration pressures, together with the desire of some businesses to garner garner favorable publicity, led firms to sign up with two privacy seal organizations, TrustE (originally called Etrust), and BBBOnline.[48] Industry associations such as the Direct Marketing Association (DMA) later set up their own schemes in order to make it easier for members to comply with Safe Harbor. However, privacy advocates viewed

---

[45] Tsebelis (2000).
[46] See the "White House Framework for Global Electronic Commerce," available at http://www.ta.doc.gov/digeconomy/framewrk.htm (checked February 15, 2001)
[47] Interview with Ira Magaziner, conducted September 21, 2000.
[48] See further, Farrell (2003).

these programs as an entirely unsatisfactory substitute for comprehensive laws; TrustE in particular came under heavy fire for perceived gaps in enforcement.[49] Advocates continued to press for federal legislation protecting consumer privacy in online (and, if possible, offline) business transactions. In mid-2001, they appeared to be making some progress; privacy issues occupied a prominent position on Congress's legislative agenda. Many observers predicted that comprehensive legislation would be passed, albeit with weaker protections than advocates would like, if only to pre-empt the possibility of legislation at the state level. However, in the wake of the events of September 2001, much of this momentum was lost; while privacy legislation in the medium term is still possible, it is by no means certain.

Both BBBOnline and TrustE have vigorously marketed themselves outside the US. The logic of this is clear; if the WWW is indeed a global phenomenon involving transnational commercial transactions, then the market for website privacy certification is also global. However, many countries are uncomfortable with the idea that foreign private entities should be guarantors of privacy standards, leading to renewed cross national discussions about the appropriate mix between public and private enforcement in privacy protection. This debate is complicated by differing notions of the relationship between public and private, and of the relationship between government regulation and self-regulation.

Many countries with strong traditions of privacy law devolve certain aspects of privacy protection to non-state actors. However, this practice is better described as "co-

[49] TrustE's credibility was badly damaged by its failure to punish member firms such as Microsoft and Real Networks for violations of their customers' privacy which fell outside TrustE's formal ambit of enforcement.

regulation" or "private interest government"[50] than self-regulation; it involves government specifically delegating certain public interest tasks (with accompanying procedures of oversight and responsibility) to private sector associations. Typically, governments exercise strong forms of oversight.[51] This differs markedly from the Anglo-American concept of self-regulation, in which business self-regulation is seen not as a means of implementing government regulation, but as a substitute for it.[52] Arrangements such as that prevailing in Australia, in which the Federal Privacy Commissioner may grant approval to industry codes that appear to embody appropriate principles, stand somewhere between co-regulation and self-regulation.

Differences between these models of public-private interaction have led to wide variation in officials' attitudes to international web seal organizations. Some national level privacy commissioners have cautiously welcomed web seal organizations as a possible means to protect individual privacy in international transactions, where it is difficult for national officials effectively to exercise their powers.[53] Others have vigorously disagreed. Many officials from non-Anglo American political systems have expressed considerable doubts about schemes such as TrustE, which they see as embodying weak principles, and providing inadequate enforcement with little opportunity for external oversight.

These disputes are likely to continue, and leave web seal organizations in an unenviable position between states and firms. On the one hand, these organizations must

---

[50] Streeck and Schmitter (1985).
[51] However, note that private interest government is strongly associated with corporatist forms of interest intermediation and policy making, which some democratic theorists find to be problematic.
[52] See further, Bach and Newman (unpublished).
[53] Interview with Malcolm Crompton, Federal Privacy Commissioner for Australia, September 8, 2000. For further discussion, see Cavoukian and Crompton (2000).

persuade state authorities that they present an effective means to protect privacy in order to protect and extend their limited realm of private authority. On the other, they face pressure not to administer principles too harshly, from the very firms on whom they rely on revenue. It appears that, at least in some instances, web seal organizations are finding themselves increasingly drawn into closer relationships with governments, as they become enmeshed in "hybrid arrangements," which mix state oversight with private enforcement.

The EU-US Safe Harbor arrangement is the best existing example of such an arrangement; it rests on principles that have been negotiated between the EU and US, but that are in part enforced by web seal organizations (or other providers of dispute resolution services).[54] Such arrangements offer states some advantages. They may make it easier to resolve regulatory clashes between states,[55] while providing states with increased leverage over private international commercial relations. However, as privacy advocates have been swift to point out, they may also lead to new problems of transparency and accountability. Lines of responsibility are typically blurred; it is hard to hold either private enforcers or government overseers liable for their actions. Furthermore, these arrangements are highly non-transparent with convoluted decision making procedures. Because they lie between politics and markets, they are only weakly subject to the democratic restraints of oversight associated with the one, and the pressures of market choice associated with the other.[56] The political consequences of these

[54] The EU's interest in Safe Harbor was in part spurred by its belief that the arrangement would allow it to influence the codes of web seal organizations. See Farrell (2003).
[55] See further, Scharpf (1994).
[56] I further note that market forces provide only poor protection for many kinds of individual and collective rights, even (and especially) when they work in an unconstrained manner.

arrangements (especially when they are international rather than national) are only beginning to receive attention from political scientists.

Second, there are emerging conflicts over the circumstances under which governments can access and use information on their citizens. These result less from worries about government use of its centralized databases (although such worries persist) than from new concerns about how governments may require private actors such as ISPs and telcos (telecommunications companies) to accede to surveillance technologies, to retain information on their customers and to provide it to government on request. These battles have received most debate in the US, where there is a highly active privacy community that has publicly excoriated initiatives such as the FBI's "Carnivore" and the administration's proposed Total Information Awareness project. However, the most important fights are taking place in other parts of the world (although they are in part the result of US government pressures in the "war on terrorism"). State security and law enforcement agencies across the developed world have used the events of September 11, and associated pressures from the US for increased intelligence, to press for new laws permitting them massively to expand their information gathering capacities. In particular, these agencies are pressing, often successfully, for the removal of restrictions on their ability to gather data about individuals' behavior on the Internet. Further, they are building on international instruments such as the Council of Europe Convention on Cybercrime, as a means to forestall domestic opposition.

Thus, for example, in Canada, the government has used the Convention on Cybercrime as a rationale for proposed new rules on "lawful access" to communications

data.[57] Current legislative developments in the European Union pose even more serious problems for individual privacy; complicated transnational procedures of law-making make it difficult to hold governments accountable for proposals to increase access to personal data. In the wake of September 11, the European Council (the body directly representing Member State interests within the European Union) has pushed successfully for the elimination of certain kinds of personal data, persuading both Commission and Parliament to abandon their earlier opposition to these changes.[58] Rules which previously mandated the destruction of traffic data held by European ISPs and telcos after 3 to 7 days, have been eliminated. This has made it possible under European law for EU member state governments to oblige ISPs and telcos to retain traffic data, and to make it available to law enforcement authorities and security services. Currently, the European Council is engaged in discussions on EU member states' differing approaches to traffic data retention.[59] Reports suggest that there are moves within the Council towards a harmonized European traffic data retention regime; again, these discussions are taking place in a venue that is secretive, and relatively impermeable to pressure from individual citizens and privacy advocacy groups. Decision making within the Council of Ministers is notoriously non-transparent, involving specialized committees of civil servants, and meetings between ministers behind closed doors. These problems are especially marked in Justice and Home Affairs, or "third pillar" issues, where neither national parliaments

---

[57] See http://www.canada.justice.gc.ca/en/cons/la_al/ (checked February 15, 2003).

[58] Increases in the power of Parliament (the extension and refinement of the so-called "codecision" procedure), were supposed to result in greater transparency and democratic accountability. In many cases, however, they have not had this effect, instead increasing the power of rapporteurs and of power-brokers within the two main parties to reach agreement with member states behind closed doors. See further, Farrell and Héritier (unpublished).

[59] See the leaked questionnaire on member state data retention policies at http://www.effi.org/sananvapaus/eu-2002-11-20.html (checked February 15, 2003).

nor the European Parliament have any effective voice.[60] Justice and Home Affairs is likely to see a substantial expansion in cooperation over the coming decade. Transgovernmental networks which deal with substantive political issues within the EU have negative consequences for democratic legitimacy; this is all the more so when these networks come to include external actors from interested parties in the US and elsewhere.

The impetus towards data traffic retention, in the EU and elsewhere, is one manifestation of a wider transformation in the relationship between states and ISPs. The latter are increasingly expected to act as agents on behalf of the state, in contexts such as copyright protection,[61] content regulation,[62] and the detection and prevention of crime. Such cooperation poses serious risks to individual privacy; in Ian Kerr's provocative description, ISP is coming to stand less for Internet Service Provider than Internet Secret Police.[63] Information on these relationships between states, ISPs and telcos, and what they involve, is difficult to come by. What safeguards there are appear to be minimal. Again, it can be seen that hybrid arrangements involving both states and private actors, pose new policy problems. Unlike Safe Harbor, these arrangements are designed to share information rather than to protect it, but they involve similar issues of accountability, transparency, and legitimacy.

Section IV – Policy Recommendations

---

[60] The European Parliament will assume a greater role in 2004.
[61] This is a key issue in ongoing legal battles between the US music industry and ISPs over whether the US Digital Millenium Copyright Act obliges ISPs to hand over the names of customers who are suspected of downloading illegal music. ISPs argue that this would effectively oblige them to police the behavior of their customers, and breach customer privacy on a massive scale.
[62] See Frydman and Rorive (2002).
[63] See http://www.cacr.math.uwaterloo.ca/conferences/2002/isw-eleventh/kerr.ppt (checked February 15, 2003).

In the above discussion, I have sought to describe the complex relationship between technology and privacy as it has evolved over the last thirty years. I have examined how both power relations among states, and existing institutional trajectories within them, have influenced domestic and international outcomes. In this section, I turn to policy recommendations; given the realities of international politics, what means may we best use to protect privacy?

Policy Recommendation I – Extending Privacy Protections Internationally

As long as some states have lax or non-existent privacy standards, there exists the risk of a lowest common denominator effect. The EU Data Protection Directive - despite its flaws - has had a significant positive effect in raising the international bar of best practice. Safe Harbor is inadequate when judged against the standards of the Directive itself, but it is a significant improvement on the domestic *status quo ante* that participating US firms observed, and it may help build up pressures for change over the medium term. Thus, Safe Harbor type solutions should be encouraged for jurisdictions such as the US, South Korea and Japan that are unwilling or unable to introduce strong, comprehensive formal legislation.

A second problem is less directly pressing, but may have significant long term consequences. Privacy issues may lead to non-tariff barriers, which hamper the exchange of services with less-developed countries that have weak privacy laws or poor enforcement. This is increasingly relevant as more data processing services are contracted out to countries in the developing world. Two possible arrangements might prevent this if

they are accepted as valid means to ensure privacy – Safe Harbor style arrangements or contracts. Here, the paper will provisionally recommend a reliance on contracts[64] – Safe Harbor style arrangements require an impartially functioning legal system – which may not be present in some developing countries. Contracts, which may be enforced in other jurisdictions than the third country in question, are more flexible, and provide firms in these countries with a means of complying with higher requirements, without making demands for institutional change that are unrealistic in the short term.

Policy Recommendation 2 – Strengthening of International Mechanisms of Privacy Protection

There is a clear and urgent need for mechanisms to protect privacy at the international level. As should be clear from the above discussion, the national and international arenas intersect in ways that make it increasingly difficult for national level actors to protect privacy without reference to international politics.

Privacy advocates, and the EU-US consumer interest umbrella group, the Trans-Atlantic Consumer Dialogue (TACD), have advocated an international Privacy Convention, which would embody strong and enforceable privacy standards.[65] While this remains a laudable long term objective, it is impossible to achieve under current configurations of power and interest. A more practical response might be the strengthening of democratic oversight and consumer representatives' voice at the international level; this expansion must be accompanied by expanded oversight, to ensure

[64] Model contracts have been approved by the European Commission for various forms of data exchange.
[65] See http://www.tacd.org/cgi-bin/db.cgi?page=view&config=admin/docs.cfg&id=97 (checked February 15, 2003).

that international meetings do not short-circuit democratic accountability. Such oversight would ideally involve a mixture of strengthening of accountability at the national level (through national parliamentary committees.

More broadly, the international role of consumer representative organizations should be greatly strengthened. The TACD serves as an excellent and successful example of how consumer organizations may articulate a common position on international issues of e-commerce regulation, but its membership is limited to EU and US organizations that wish to address the EU-US relationship. Public Voice is underfunded, only partially representative, and lacks the formal "status" of the TACD. A wider partnership would address consumer and privacy issues across a variety of multilateral settings, serving both as an "official" voice for consumer interests, and as a counterpart to the Global Business Dialogue (GBDe) and similar organizations. It would also provide an opportunity for consumer interests from developing countries to have their voice heard in international fora. As discussed already, the developing world is likely to have a different set of priorities regarding privacy, at least in the short term – these priorities are currently given short shrift.

Policy Recommendation 3 – Increased Accountability Requirements for Public-Private Actor Relationships (Hybrid Arrangements)

As discussed above, many of the new policy issues on the privacy agenda involve emerging, hybrid relationships between public and private actors. Such relationships have

diffuse lines of responsibility; they weaken democratic accountability by devolving important functions to private actors.

The Safe Harbor arrangement, in its first two years of operation, illustrates this problem. There is remarkably little information available on what procedures are followed in evaluating and adjudicating complaints under Safe Harbor, and some evidence to suggest that the European Commission (the relevant European administrative body) has not made serious efforts to monitor day-to-day enforcement of the arrangement.[66] Problems of transparency and accountability are likely to be worse still in situations involving security or police investigations.

Thus, this chapter makes the following recommendations. First, there should be strong reporting requirements when international public-private partnerships are used to achieve important policy goals. There should be regular reports detailing both general procedures and specific actions. These reports should be published, and the relevant actors should be explicitly accountable to democratic assemblies (such as, in the case of Safe Harbor, the European Parliament).

Second, public-private cooperation in the sphere of security and policing should only be mandated where absolutely necessary. These public functions of the state are, quite simply, too important to be delegated to private actors, except where there is a burning and immediate need. In instances where they are necessary, they should be limited, targeted and proportional to the need at hand. They should not involve generalized and diffuse increases in the policy aegis of security services, and/or the responsibilities of private actors. Further, they should be subject, insofar as is compatible

[66] This is representative of a more general set of problems that the Commission faces; while it is responsible for enforcement across a wide variety of EU policy areas, it must delegate many aspects of implementation to third parties, and has scanty resources to monitor how these third parties behave.

with any legitimate need for secrecy and confidentiality, with the reporting requirements outlined above. In any event, regular reports should be published, indicating the general patterns of enforcement. Furthermore, there should be strong oversight mechanisms, involving independent third parties, to ensure that public-private cooperation does not invade privacy more than is absolutely necessary for specific and legitimate purposes.

Conclusions

The regulation of privacy involves both international and national dimensions. In this chapter, I have argued that the relationship between the two in different conjunctures is best understood by concentrating on two key factors – existing institutional traditions and power relations among states. Existing institutional traditions in various countries help explain their initial preferences, and their relative willingness to adopt comprehensive privacy laws that were proposed by a cross-national policy community of privacy experts. Countries in mainland Europe, which had previously existing traditions of extensive business regulation, and which had recent experience of Nazi abuses of privacy were relatively willing to regulate. Countries such as the US, which had weak traditions of business regulation, and a different constellation of state-private actor relations, were not.

Power relations – and the relative bargaining strength of states – help explain the circumstances under which states have accepted, or failed to accept, external privacy rules that do not accord with their previously existing traditions. Powerful states in strong bargaining positions, have little incentive to accept such rules, which would be

domestically costly and difficult to implement.[67] Weaker states may have little choice but to accept externally imposed constraints, even when they have little desire to do so, when they believe that more powerful states will retaliate against them if they do not.

This explains the persistent unwillingness of the US to accept externally imposed rules on privacy. Given the US relationship of dominance with most of its trading partners, it has few incentives to make domestic concessions, especially when such concessions would involve major institutional changes. While the EU has been successful in pressing the US to accept a "hybrid" solution, this solution does not formally involve any change to existing US institutions. Other countries, which are weaker vis-à-vis the EU than the US have had little success in winning Safe Harbor style concessions. Countries in weak bargaining positions – most especially EU applicant countries – have had little choice but to accept the EU's basic position on data protection.

These twin forces not only help explain the circumstances under which international pressures result in domestic change; they help explain the circumstances under which domestic preferences are (or are not) instantiated in substantial, binding political agreements. The failure of an epistemic community to produce complete convergence at a previous juncture meant that there was substantial divergence in goals between European states on the one hand, and the US and a few other countries on the other, over whether or not there should be binding international rules covering data transfer. The US, which had both different preferences from most other countries, and an impregnable bargaining position, refused to participate in any binding international agreements, resulting in two international arrangements, one which was inclusive and

[67] I do not take account here of more complex dynamics between arenas, which may allow underprivileged actors in one arena to use leverage in another. See further, Farrell (2002).

non-binding, the other of which was binding, but only involved a more limited club of states.

This analysis furthermore suggests clear limits to the expert-driven processes of policy convergence around strong privacy standards that Bennett observed at an earlier stage.[68] Epistemic communities are only likely to succeed in persuading countries to adopt comprehensive privacy legislation under relatively limited conditions – i.e. where such policy solutions instantiate previously-existing social goals, and are compatible with broad national institutional frameworks governing, for example, state-private actor interaction. Where such conditions do not apply, as, for example in the US, the advice of non-political experts will at best have limited political effect.

The current day politics of privacy are driven by two countervailing forces. On the one hand, the European Union has enjoyed some success in bringing countries that are in some way dependent on it to introduce comprehensive privacy laws. This suggests a gradual upward ratcheting in privacy regulation around the world. On the other hand, the events of September 11 have very considerably strengthened the hand of security elites in the various advanced industrialized democracies. These elites have successfully pressed for the introduction of new laws that limit personal privacy, both in their particular domestic contexts and through various transgovernmental policy networks. In many cases, emerging domestic and international security frameworks involve close – and perhaps sometimes incestuous – relations between states and private actors that have strongly negative implications for privacy. To use less academic language, it is arguable that these changes are eating out the heart of the emerging privacy framework, even as this framework is apparently being extended to new parts of the world. Unlike privacy

[68] Bennett (1992).

experts at an earlier juncture, security elites are at the very heart of the state apparatus; they thus seem to be enjoying more general success in altering domestic and international practices.

Bibliography

Andrews, Sarah, and Privacy International (2002), *Privacy and Human Rights 2002: An International Survey of Privacy Laws and Developments* (London: Privacy International).

Bach, David and Abe Newman (unpublished) *Self-Regulatory Trajectories in the Shadow of Public Power: Resolving Digital Dilemmas in Europe and the United States.*

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

Bergström, Karl-Fredrik, Henry Farrell and Adrienne Héritier (unpublished) *Legislate or Delegate?: Comitology and Delegated Powers in the European Union*.

Cavoukian, Ann, and Malcolm Crompton (2000), *Web Seals: A Review of Online Privacy Programs* (Canberra/Toronto: Office of the Federal Privacy Commissioner/Office of the Privacy Commissioner).

Drake, William J (1993), "Territoriality and Intangibility: Transborder Data Flows and National Sovereignty," in Kaarle Nordenstreng and Herbert I. Schiller, eds., *Beyond National Sovereignty: International Communications in the 1990s* (Norwood: Ablex).

Farrell, Henry (2002), "Negotiating Privacy across Arenas - The EU-US "Safe Harbor" Discussions," in *Common Goods: Reinventing European and International Governance*, ed. Adrienne Héritier (Lanham, MD: Rowman and Littlefield).

Farrell, Henry (2003), "Constructing the International Foundations of E-Commerce: The EU-US Safe Harbor Arrangement." *International Organization* (57) 2: 277-306.

Farrell, Henry and Adrienne Héritier (unpublished), *Interorganizational Cooperation and Intraorganizational Power: Early Agreements under Codecision and Their Impact on the Parliament and the Council*.

Flaherty, David (1979). *Privacy and Government Data Banks: An International Perspective* (London, Mansell: 1979).

Frydman, Benoît and Isabelle Rorive (2002), "Regulating Internet Content Through Intermediaries in Europe and in the United States," *Zeitschrift für Rechtssoziologie* (23) 1: 41-59

Haggard, Stephan and Beth Simmons (1987), "Theories of International Regimes," *International Organization* (41) 3: 491-517

Heisenberg, Dorothee and Fandel, Marie-Helene (2002). *Projecting EU Regimes Abroad: The EU Data Protection Directive as Global Standard.* Paper prepared for delivery at the 2002 Annual Meeting of the American Political Science Association, Boston, August 29-September 1, 2002.

Long, William J. and Marc Pang Quek (2002), "Personal data privacy protection in an age of globalization: the US-EU safe harbor compromise," *Journal of European Public Policy*. (9) 3: 325-344.

Kobrin, Stephen J. (unpublished), *The Trans-Atlantic Data Privacy Dispute: Territorial Jurisdiction and Global Governance*.

Mayer-Schönberger, Viktor (1997), "Generational development of Data Protection in Europe" in Philip E. Agre and Marc Rotenberg, eds., *Technology and Privacy: The New Landscape*, (Cambridge: MIT Press).

Regan, Priscilla (1999). "American Business and the European Data Protection Directive: Lobbying Strategies and Tactics," in Colin Bennett and Rebecca Grant eds., *Visions of Privacy* (Toronto: University of Toronto Press).

Scharpf, Fritz W. (1994), "Community and Autonomy. Multilevel Policy-making in the European Union," *Journal of European Public Policy* (1) 2: 219-242.

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

Slaughter, Anne-Marie (2001), "Global Government Networks, Global Information Agencies, and Disaggregated Democracy," unpublished paper.

Streeck, Wolfgang and Philippe C. Schmitter (1985), "Market, State, Community and Associations? The Prospective Contribution of Interest Governance to Social Order," *European Sociological Review* (1): 119-138

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

Tsebelis, George (2000), "Veto Players and Institutional Analysis," *Governance* (13) 4: 441-74.