THE TRANS-ATLANTIC INFORMATION PRIVACY DISPUTE AND REGULATORY SPILLOVER

Stephen J. Kobrin
Department of Management
The Wharton School
University of Pennsylvania
kobrins@wharton.upenn.edu

For presentation at the Annual Conference of the European International Business Academy
Athens Greece, December 2002

The U.S.- European Union dispute the protection of information privacy, an individual's control over the processing of personally identifiable or name-linked data (Kang 1998), raises difficult questions about territorial jurisdiction and democratic governance, indeed about how political "space" and a political community are defined in the digital age. It illustrates the emerging *geographic incongruity* between the reach and domain of the territorially defined Westphalian state -- as legal jurisdiction, political authority, and self-governing democratic community -- and the deep and dense network of transnational economic relations that constitutes the early 21st century world economy.

There certainly are examples of markedly different regulatory approaches to problems in the Europe and the United States: Germany's strict control of retail store opening hours and limits on promotional or discount activity, for example. Given the modern political system's norm of mutually exclusive jurisdiction one would expect differences in law and regulation to be the rule rather than the exception: they are definitional at the most basic level.

Regulatory differences become problematic and conflictual when there is cross-border "spill over" into other jurisdictions. That occurs when 1) the impact of the regulation is not limited to the geographic territory of the originating jurisdiction and 2) state capabilities and authority in other affected jurisdictions are constrained to the point where impacts cannot be mitigated. Under conditions where the intensity of transborder relations is such that both conditions become general, the system norm of mutually exclusive territorial jurisdiction becomes questionable.

In the trans-Atlantic context, regulatory spill-over is becoming more common. EU competition authorities' objections derailed the merger of Honeywell and General

Electric, two "American" companies, and the head of the U.S. Anti-Trust Division felt it necessary to remind European authorities that *their* concerns about Microsoft's use of market power had not held up in American courts. In fact, given the size of the EU's economy and its relative preference for regulation, its policies have had a significant impact within the United States. As a *Wall Street Journal* article noted, "Americans may not realize it, but rules governing the food they eat, the software they use and the cars they drive, are increasingly set in Brussels…" (Mitchener 2002, p. 1).

Electronic integration increases dramatically the potential for regulatory spill-over. While electronic networks may not be borderless, cross-border transactions are effortless; in an electronically interconnected world the effects of any given action – posting an article on a website, for example -- can be felt elsewhere (and everywhere) with no relationship to geography and territorial jurisdiction whatsoever (Berman 2002).

The European Data Directive assumes the existence of cross-border data flows and attempts to protect the data privacy rights of Europeans regardless of where data are transferred and processed. Article 25 (of which much more below) prohibits transfer of personally identifiable data to any third country that does not provide "adequate" protection, which includes the United States.

As cutting-off trans-Atlantic data flows would have catastrophic impacts, bilateral negotiations were undertaken resulting in the "Safe Harbor" agreement which attempts to bridge the gap by providing protection for personal information deemed adequate by the Europeans without unduly compromising American beliefs in self-regulation and the marketplace. As will be seen, Safe Harbor does not appear to be a success and both

Europeans and Americans find themselves subject to data protection regimes that are not of their making and to which they resist complying.

I will proceed by first discussing the general issue of data or information privacy (the terms are used interchangeably here) and its protection and then turn to a detailed examination of differences in American and European data protection norms and review implementation in each region. I will then review the progress of Safe Harbor to date and discuss implications for territorial jurisdiction and global governance.

Data Privacy

Data privacy involves standards for the treatment of personal information (Reidenberg 1995), the terms under which information identifiable to an individual is acquired, disclosed and used (Privacy Working Group 1995). The information revolution and the ubiquity of Cyberspace have significantly increased the risks to data privacy.

Using the Information Infrastructure to communicate, order goods and services, or obtain information produces electronic data that can easily and inexpensively be stored, retrieved, analyzed, and reused (Privacy Working Group 1995). Furthermore, rapidly developing technologies (data mining) are providing new and very powerful means to sort, combine and analyze data. Last and critically, these data exist in a *networked environment*: personal information collected, created and processed on any computer on the Net is, at least in theory, accessible by every computer on the Net (Reidenberg 2000).

Protecting Personal Information

The protection of personal information entails complex benefit/cost trade-offs for both society and individuals. As Fromholz (2000) notes, privacy is not an absolute good: while it results in unquestioned benefits, it also "imposes real costs on society." While

privacy may protect some individuals, it may result in economic and social costs by preventing others from making fully informed decisions. Frumholz cites instances such as a babysitter who was convicted of child abuse or a physician with a history of malpractice.

The issue is more subtle, and more general, than hiding a disreputable past. In an information-based economy, protection of name-linked data involves weighing individual rights to privacy on the one hand and economic efficiency on the other; the right of a business to record transaction generated information and consumers' demands that they be informed about the gathering and use of this data are often in tension with one another (Milberg, Smith, and Burke 2000). How that trade-off is evaluated is a function culture, social norms, political and economic philosophy and historical experience; there are marked differences in preferences between the United States and the European Union in this regard.

A number of authors have argued that there has been a tendency towards convergence around a set of generally accepted "fair information principles" including standards relating to data quality, transparency in processing, treatment of sensitive data, and enforcement mechanisms (Bennett 1997; Reidenberg 2000). While there may be agreement about the broad scope of fair information practices there is considerable disagreement about how these principles are actually interpreted and their execution or implementation (Reidenberg 2000).

Data privacy is never considered in a vacuum, but rather in a specific social, political, economic, cultural and historical *context.* In the modern political system, that context is the territorial state, the "physical container of society." As will be discussed

below, significant variation in the context directly affects interpretation of data privacy *norms*, whether information privacy is a considered a basic human right or a property right for example. These norms, in turn, affect what the fair information *principles* actually mean in practice. Last, given differences in context and norms there is considerable variance in *implementation* and execution.

Context and norms

Fundamental differences in the American and European contexts have led to very different norms. Two distinct visions of democratic governance -- views about the responsibility of the state to protect the rights of its citizens and the effectiveness and equity of markets (Reidenberg 2000) – are reflected in deep-seated differences in normative and positive beliefs about markets versus regulatory solutions to social problems, faith in technology, the relative weight put on individual rights and economic efficiency, and individual versus collective societal responsibility for one's welfare.

In the United States, rights are generally, if not uncontroversially, seen as rights against the government.[1] Thus, the U.S. approach to data privacy reflects a basic distrust of government; markets rather than law shape information privacy in the U.S. and as a result the legislation that does exist is reactive and issue specific (George, Lynch, and Marsnik 2001; Reidenberg 2000). Protection tends to be tort based and market oriented rather than political: a "patchwork of rules" that deal with specific sectors and problems in a haphazard manner (Banisar and Davies 1999; Frumholz 2000; Kang 1998; Reidenberg 2000; Roch 1996; Swire and Litan 1998). As privacy is seen as an alienable commodity disputes about personal information are often cast in economic terms:

[1] This tends not to be the case in Europe. I owe this point to David Post.

questions about property rights and rents, who "owns" the data collected in a commercial transaction.

In contrast, the European approach to privacy protection reflects a greater emphasis on society than the individual. Privacy is considered a fundamental human right and comprehensive systems of protection take the form of explicit statutes accompanied by regulatory agencies to oversee and insure enforcement. Europeans are more likely to have questions about the efficacy and equity of markets and to believe that legislation is the appropriate solution to societal concerns about commercial activity (Frumholz 2000).

The introduction to the EU Data Directive begins by referencing the objectives of the Community including "…promoting democracy on the basis of the fundamental rights recognized in the constitutions and laws of the Member States and in the European Convention for the Protection of Human Rights and Fundamental Freedoms." It goes on to state "(W)hereas data-processing systems are designed to serve man…they must…respect the fundamental freedoms and rights of individuals, notable the right to privacy, and contribute to economic and social progress…" (The Council 1995, pp 2 and 10).

Differences in both context and norms affect how Europeans and Americans evaluate trade-offs between data privacy, on the one hand, and other social goods on the other. As would be expected, Europeans are more like to privilege data protection "rights" at the expense of public access to information and/or economic efficiency. Americans would be likely to put much less weight on the former and more on the latter (George, Lynch, and Marsnik 2001).

In summary, trans-Atlantic differences with regards to data privacy and its protection reflect deeply rooted differences in historical experience, cultural values, beliefs about the organization of the polity, economy and society, and the importance of free speech versus other societal ends. Ambassador Aaron, who negotiated Safe Harbor, notes that in Europe "privacy protection is an obligation of the state towards its citizens. In America we believe that privacy is a right that inheres in the individual. We can trade our private information for some benefit. In many instances Europeans cannot" (2001).

The Implementation of Privacy Protection

The word "privacy" is never mentioned in the American Constitution, indeed neither that document nor the Bill of Rights deal with the issue explicitly (Gellman 1997; George, Lynch, and Marsnik 2001; Reidenberg 1995; Roch 1996). As late as 1890 when Samuel Warren and Louis Brandeis published their famous *Harvard Law Review* article dealing with privacy, "there existed no coherent notion of privacy at all in American law" (Gormley 1992, p. 1343, 1344).[2]

The development of privacy protection in America has been sporadic, inchoate, sectorially specific and reactive. The first U.S. attempt at legislating information privacy protection in the private sector was The Fair Credit Reporting Act of 1970 (Caudill and Murphy 2000). Subsequent legislation has dealt has dealt with specific problems as deemed necessary. For example, the "Bork Bill" (1988) protects data on video tape rentals, the Cable Television Consumer Protection Act (1992) regulates the disclosure of name-linked data for cable subscribers, and the Children's Online Privacy Protection Act limits the personal information that can be collected from children (Frumholz 2000).

[2] It is of interest that Ken Gromley ascribes Warren and Brandeis' motivation to the rise of "yellow journalism" in the Boston tabloids which was, itself, a function of technological changes which allowed the production of cheap mass circulation newspapers. Also see (Reidenberg 1995).

While there are a number of bills being considered by Congress at this point, especially in the medical and financial services areas, regulatory protection of data privacy in the United States is still quite limited. In the main, the American privacy protection regime relies on market mechanisms and self-regulation.

The history of European data protection is grounded in the attempts of European countries, particularly the Federal Republic of Germany, to "curb the threat of the improper use of personal data" (Roch 1996, p.72). The right to privacy is specifically mentioned in a number of constitutions (e.g., Germany and Spain) and in the Council of Europe's "Convention for the Protection of Human Rights and Fundamental Freedoms" (George, Lynch, and Marsnik 2001).[3]

Sweden established the first data protection law in 1973 (The Swedish Data Bank Statue), followed by Germany in 1977 (based on a law passed by the state of Hesse in 1973) (Roch 1996). With the increasing integration of Europe regional efforts followed. In 1980, the OECD issued voluntary *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (which was signed by the United Sates) and a year later the Council of Europe issued a convention *For the Protection of Individual with Regard to Automatic Processing of Personal Data* (Swire and Litan 1998).

As barriers to full economic and financial integration fell within the EU, differences in national data protection legislation became increasingly important. The EU Data Directive was proposed in the early 1990s to harmonize data protection laws of the fifteen member states. Directive 95/46/EC of the European Parliament and of the Council. The Directive does not apply directly, but requires each member state to enact

[3] Article 8 of the Convention is entitled "Right to respect for private and family life" and it states that "Everyone has the *right* to respect for his private and family life, his home and his correspondence" (emphasis added). (Council of the Europe 1950)

legislation which meets minimum standards for the protection of personal information. (George, Lynch, and Marsnik 2001; Reidenberg 2001b; Roch 1996; Swire and Litan 1998). The primary provisions of the Directive require that:

- Data collected must be adequate, relevant and not excessive in relation to the purposes for which they are collected and processed.
- Data may not be further processed in ways incompatible with the purposes for which they are collected.
- Recipients of information are entitled to know where the information comes from, how it was collected, whether responses were voluntary, and the like.
- Individuals have full access to all data linked to their name and the right to correct any inaccurate data. Individuals also have the right to "opt out" of further processing or transmission of personal data.
- Processing of sensitive data containing information about individuals racial or ethnic origins, religious beliefs, union memberships, political opinions, sexual preferences and the like can not be processed without permission. In some cases, it cannot be processed even with the individual's permission.
- Each country must have one or more public authorities responsible for monitoring and enforcing the Directive.

The Data Directive recognized that as "cross-border flows of personal data are necessary to the expansion of international trade," transfers of personal data outside of the territory of the EU were inevitable. Article 25.1 states that the transfer of personal data which "are undergoing processing or are intended for processing after the transfer" can only take place if the "third country in question ensures an adequate level of protection" (The Council 1995).

Article 26 contains a number of "derogations" which allow data transfer to countries where protection has not been deemed adequate under certain conditions. These include, for example: unambiguous consent of the data subject; performance of a

contract; important public interest grounds; and the need to protect the "vital interests" of the data subject. It was assumed that many "everyday" transfers would be covered by Article 26 provisions of consent and contract including making hotel reservations, inter-bank transfers of funds, and booking travel (Smitis 1996).

The Safe Harbor Agreement

Once it became clear that trans-Atlantic data flows would not be assured on the basis of Article 26 exemptions alone and that adequacy would be an issue, negotiations began between the U.S. and the EU Commission (Long and Quek 2001).[4] Farrell (forthcoming) notes that it was a suggestion by Aaron that adequacy could be judged on an organization by organization basis which proved critical. Firms could enter a "Safe Harbor" by agreeing to a privacy protection regime acceptable to the EU, "Each organization subscribing to the safe harbor principles would be presumed to be providing adequate privacy protections" (Aaron 1999, p. 4).

The objective was to "bridge the gap," to find a solution which would ensure the "adequacy" of protection of European data consistent with American preferences for reliance on self-regulation and market mechanisms. The Department of Commerce proposed a first set of Safe Harbor principles in November 1998 and after eighteen months of negotiations, the European Commission's final approval was attained in the spring of 2000 with the understanding they would come into effect the following November 1st (Farrell 2002; Long and Quek 2001; Shimanek 2001). (The European Parliament, which had the authority to advise but not to consent to the agreement,

[4] Writing in 1995 Simitis argued that "most transfer cases are, in fact, covered by the long list of exceptions found in Article 26…" (1996, p. vii). See (Farrell 2002; Farrell forthcoming) for a detailed discussion of the Safe Harbor negotiations.

rejected the finding of adequacy due to a complex combination of substantive, procedural and political factors.)

Safe Harbor includes the principles, a set of FAQs (Frequently Asked Questions) which explore the provisions in more detail and enforcement mechanisms. Safe Harbor is neither a treaty nor an international agreement but rather two unilateral actions: the U.S. issued the principles and the Commission issued an Article accepting them (Aaron 2001, statement of Barbara Wellberry, Councilor to the Under Secretary).[5]

At present, only companies which fall under the jurisdiction of the Federal Trade Commission or the Department of Transportation (air carriers and ticket agents) are eligible for Safe Harbor. Thus, major sectors of the economy, such as financial services and telecommunications, must rely on the Data Directive's Article 26 provisions for exemptions from the requirement of adequate protection, including situations where the data subject gives his or her informed consent to a specific transfer and where the transfer is necessary for the performance of a contract.[6]

It is fair to say that Safe Harbor has not been seen as an overwhelming success on either side of the Atlantic. As of October 23, 2002 only 254 companies had enrolled, few of them major multinationals.[7] The relatively low number of firms which have signed up reflects concerns about Safe Harbor combined with a sense that, at lease at this point, the penalties for non-compliance are not very obvious.

---

[5] The EU agreed to Safe Harbor with the understanding that the arrangement would be reviewed the following year. It is important to note that given that Safe Harbor represents a unilateral determination of adequacy from the EU's point of view rather than a treaty, that determination can revoked if it becomes apparent that the agreement is not working as intended (Farrell forthcoming).

[6] Article 27.1 of the Directive provides that "Member States and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of national provisions adopted by the Member States pursuant to this directive…" (The Council 1995).

[7] The list of organizations enrolled in Safe Harbor can be accessed from www.exports.gov/safeharbor/

In general, American firms believe that Safe Harbor goes too far, that implementing it will be too costly, that it might stimulate pressure for similar legislation in the U.S. and that it might subject them to unforeseen liabilities in Europe (Gruenwald 2000). In contrast, American privacy advocates believe that Safe Harbor does not go nearly far enough, that it is a weak and ineffective substitute for legislation. Reidenberg (2001a, pp. 719 and 739), for example, argues that Safe Harbor is a "weak, seriously flawed solution for e-commerce" and that Safe Harbor is no more than a mechanism to "delay facing tough decision about international privacy."

Safe Harbor was controversial in Europe from the start with serious questions raised by both national data authorities and in the Parliament about the adequacy of data protection. The European Commission Staff Working Paper on the effectiveness of Safe Harbor issued in early 2002 (summarizing a 2001 review) was diplomatic, but clearly expressed concern about both implementation and the adequacy of data protection. It notes that the number of organizations self-certifying under Safe Harbor is "lower than expected," and that many of those do not really satisfy the requirements of the agreement. It found that a substantial number of organizations do not meet the requirement that they publish a compliant privacy policy and indicate publicly their adherence to Safe Harbor (European Commission Staff 2002).

Territorial Jurisdiction and the Internet

The objective of the Data Directive is to protect the fundamental privacy rights of individuals, regardless of where their data is processed. As data collection has become common in cyberspace implementation of that objective has become much more complicated, both conceptually and practically; a recent Working Party Document

concluded that when processing operations involve a "controller" in a third country, "the country of origin principle…can no longer serve the purpose of determining the applicable law" (Article 29 - Data Protection Working Party 2002, p.7).

Article 4.1, which deals with the applicability of law, states that national provisions adopted by each Member State to comply with the Directive shall apply to the processing of personal data where: (4.1c) "the controller is not established on Community territory and, for purposes of processing personal data *makes use of equipment*, automated or otherwise, *situated on the territory* of said Member State, unless such equipment is used only for purposes of transit…" (The Council 1995, emphasis added).[8]

A recent attempt to apply Article 4.1 to the Internet argues that the "place of establishment" is neither the place where the technology supporting a web site is located nor the place at which the web site is accessible, but rather the place where it pursues its *activity* (Article 29 - Data Protection Working Party 2002). The question then, is whether the web site (data controller) makes use of equipment situated in the EU in pursuing its activity. If it does, it appears that the "place" where it pursues its activity is deemed to be within the territory of a Member State and the Data Directive applies.

Two "concrete examples" are provided. If a "cookie" is placed on the hard drive of a computer located within the EU and data is sent back to the originating web site, the user's PC is viewed as equipment in the sense of Article 4 and the provisions of the Data Directive apply. The same argument applies if Java Script or banners are used to collect personal data.

[8] In fact, Reidenberg and Schwartz note that the French text of the Directive uses the term *moyens* or means rather than *equipment* which might well imply a greater applicability of the Directive to interactions in Cyberspace (Reidenberg and Schwartz 1998).

Thus, if a user in Dortmund logs onto a Website in Dallas and provides personally identifiable information in exchange for access to a magazine article, or if the website places cookies on the computer's hard drive, the EU Data Directive would apply to the website in Texas. It is not unreasonable to argue that a Website which makes use of European equipment (or means) should be subject to its reach, "to insure that Europeans are not deprived of the protection to which they are entitled under this Directive" (Article 29 - Data Protection Working Party 2002, p. 10). That conclusion, however, is problematic in a world organized politically in terms of territorial sovereignty.

Many of the existing arguments about the Internet, whether it is "borderless" or whether computers and their users can be located in physical space for example, divert attention from more fundamental concerns such as the meaning of concepts such as borders and mutually exclusive jurisdiction in a digitally integrated world. In fact, one can question the viability of geography as the political system's organizing principle as Cyberspace and electronic networks gain in importance.

Borders are no longer significant in an economic or political sense when anyone with a computer connected to the Internet can cross them at will, and may not even know that they have done so, to exchange information in the form of articles, music, movies, books or digital cash. When in the terms of Goolsbee's metaphor, everyone lives in a virtual border town where crossing most borders is as easy as crossing the street (Goolsbee 2000).

The idea of borders as a barrier, which is necessary if they are to have substantive meaning, implies that physical or material goods cross them in geographic space and can be prevented from doing so at the will of the sovereign. A message transmitted on the

Internet between two individuals located in Munich and Muncie does not "cross" a border in any meaningful sense of the word; both sets of computers and their users remain fixed in place. While governments may be able to force entities at various points in the network to block transmission or receipt of the message, they cannot intercept it at the border and turn it back. When the user in Munich logs into a Website in Muncie it is more reasonable to argue that the interaction is taking place in both "locations" simultaneously than to think of it in terms of a transmission "sent" across physical space.

It is clear that the privacy rights of European citizens on the internet cannot be protected if the Data Directive does not have an extraterritorial reach. However, Article 4.1c implies that the EU (and by implication every jurisdiction) has the right to apply its regulation to any Website, regardless of where it is located, that can be accessed from and have an effect on its territory. By extension, that implies that every website or "data controller" is, at least potentially, subject to regulation emanating from every jurisdiction in the world. As Wrenn (2002) notes, that would turn the idea of a borderless internet into one in which the power of governments to regulate Cyberspace would be unrestrained, it would give rise to a world of "hyper-regulation."

That possibility would turn the idea of extraterritoriality on its head and corrupt fundamentally territoriality as the organizing principle of the modern interstate system. At some point quantity becomes quality; when "cross-border" transactions, regulatory spill-over and extraterritorial jurisdictional reach become the norm rather the exception, one has to question the meaning of both internal sovereignty in terms of the state as the ultimate domestic authority within its borders and external sovereignty in terms of the fundamental concept of mutually exclusive geographic jurisdiction.

If personal information can be transmitted instantaneously to multiple locations anyplace in the world, its location becomes ambiguous (Bennett 1997). Indeed the idea that it is "located" anywhere at any given time loses meaning conceptually. If that is the case, regulations which attempt to protect the data privacy of Europeans, or anyone else for that matter, must also ignore "location" as a constraint if they are to be effective. Extraterritorial reach not only becomes the norm rather than the exception, the concept itself looses meaning as the distinction between domestic and international affairs blurs to the point where it is no longer meaningful and territoriality becomes problematic as the organizing principle underlying the international political system.

Data Privacy and Global Governance

McGrew (1997, p. 5) argues that the bounded sovereign state provides a territorially delimited space in which "the struggles for democracy, the nurturing of social solidarities, and constitutional forms of government could develop within a framework of the rule of law." In fact, a geographically organized international system assumes not only that the territorial state is the primary container of politics, but that there is a geographic congruity between politics, economics and social relations, that geographic space has meaning as a political-economic construct.

While the EU-U.S. dispute over the Data Directive may yet be resolved though bi-lateral negotiations, it is more likely to be representative of an emerging set of issues which render territorial jurisdiction problematic and which pose difficulties for traditional bi-lateral or inter-jurisdictional negotiation. Effective governance may require a redefinition of both the scope or extent of political space and the meaning of space as a political construct.

In an interconnected world it is increasingly likely that the legitimate decisions made by states will affect people and areas outside of a state's sovereign domain, that there is "less and less congruence between the group of participants in a collective decision and the total of all of those affected by their decision" (Habermas 2001, p. 70). While the EU Commission did not intend to extend the reach of the Data Directive extraterritorially, it was clear that the information privacy rights of Europeans could not be protected if the effects of the legislation were limited to the geographic territory of the European Union. The footprint of the Data Directive is transnational and "the EU's 1995 Data Protection Directive now constitutes the rules of the road for the increasingly global character of data processing operations" (Bennett 1997, p. 103 and 111).

As discussed above, there are significant differences in belief systems between Europe and the U.S. These include the meaning of privacy, as a basic human right or an alienable commodity, the responsibility of society to protect individuals versus the responsibility of individuals to protect themselves, whether government regulation is a first choice or a last resort, reliance on and the proper scope of the market, and the relative importance of economic efficiency versus other social goods. While there are certainly Europeans who share American views and Americans who would prefer European regulatory solutions to data protection, belief systems relevant to the data privacy issue map reasonably well on political geography. Although there may a degree of convergence on data protection principles, I believe that very significant differences exist once one crosses the Atlantic in terms of the context, norms and meanings ascribed to data privacy, and certainly appropriate modes of implementing protection.

We are thus left with democratic political institutions and belief systems which remain contained within the national space, the transnational footprint of data privacy regulation and transnational political activity both gradually expanding "political space" beyond national borders, and the "space" occupied by the global world economy and networked data systems encompassing at least most of the major markets. This marked geographic incongruity affects our ability to govern effectively.

Global Governance

Albrow (1997, p. 58) argues that the shift to the new epoch, the break with modern forms of organization, comes "when the social takes on a meaning outside the frame of reference set by the nation-state." Others talk about a space economy that extends beyond the regulatory capacity of the nation-state (Sassen 2000) or denationalization as the extension of social spaces beyond national borders (Zurn 2000). Unless one has traditional regional economic integration in mind (e.g., the EU or NAFTA), once one transcends the borders of the territorial state the concept of space leaves its geographic frame of reference behind and takes on a meaning that only makes sense metaphorically.

Political space is socially constructed. The geographic organization of the Westphalian system would not have been possible before the rediscovery of Ptolemaic geography, the ability to conceive of external space in material rather than mythical or cosmological terms, and the emergence of single point perspective (Harvey 1990; Ruggie 1993). A digital networked world economy entails a transition from spatial to relational modes of organization and in that sense "space" can only be seen as a metaphor for one or more multidimensional networks. I would certainly agree with Anderson (1996, p.

142) that "(T)he medieval-to-modern political transformation was associated with a transformation in how space and time were experienced, conceptualized and represented. With contemporary globalization we may now be experiencing a similarly radical modern-to-postmodern transformation, with similarly radical consequences for existing territoriality."

As our modes of thought are trapped in the modern state system which is geographic to its core, we can only express our concepts of political and economic authority in terms of borders and territorial jurisdiction. Globalization, however, is relational rather than geographic; the new political space from which effective and legitimate governance must emerge takes the form of relational networks rather than territory, a "space of flows" versus a "space of spaces" (Castells 2000).

The trans-Atlantic dispute over data privacy is unfolding in a non-territorial political space that both transcends the borders of European Union and the United Sates and is difficult to conceive of in purely geographic terms. The transnational reach of "domestic" legislation, the difficulty of reaching a negotiated solution perceived as democratically legitimate and the emergence of significant transnational political activity all indicate the problematic nature of territorial jurisdiction in this issue area and argue for a multidimensional reconceptualization of political space, including identities and affiliates as well as territoriality (Rosenau 1997) and perhaps other constructs as well.

How then can political space "catch up" with economic space? I do not believe that a solution that is both effective and perceived as legitimate by all affected will result from bilateral negotiations. The "space" in which a solution must be found is both larger than either party's territory *and* fundamentally non-geographic. It is a space of flows, of

networks of multinational firms, internet users, electronic commerce websites, governments, and transnational civil society groups such as the TACD. An effective and legitimate resolution of the problem requires that this enlarged non-territorial space be occupied. That we think of communities in network terms and then "conceptualize legal jurisdiction in terms of social interactions that are fluid processes, not motionless demarcations, frozen in time and space" (Berman 2002, pp. 8-9).

It is difficult to imagine this larger political space emerging spontaneously. A governance regime will require effective international institutions that could provide a venue for discourse, for the development of interactive professional networks, and for public communications about the nature of the problem and the requirements for an effective solution. An international institution that makes it clear that all affected by political decisions are not located in a single jurisdiction and provide the ability for groups affected by decision to communicate publicly (Zurn 2000).

A very relevant example is provided by the OECD's efforts to find an international cooperative solution to the problems of taxation of electronic commerce transactions. The OECD brought together representatives of member governments, the private sector , civil society and professional groups for extensive discussions that dealt with the problems of taxing electronic transactions in the context of very different systems of taxation across regions. The discussions reinforced the need for a common solution, or at least harmonization of effects across regions, and helped establish a community of common interest in dealing with these issues. The discussion also helped insure that interested groups in various countries understood the parameters of the

problem in the sense of a common solution necessarily departing from *ex ante* preferences.

One can generalize from the trans-Atlantic data privacy dispute. A class of problems is emerging that are inherently international in the sense that their solution is beyond the capabilities of any single national government. Global warming, financial stability, drug trafficking, the AIDs epidemic, and poverty alleviation all serve as examples. While these issues are global in scope, the social and political institutions which deal with them are still predominately local and national. Any meaningful solution will require both enlarging political space by building the rudiments of a transnational social community and establishing more effective international institutions.

Bibliography

Aaron, David L. 1999. Remarks before the Information Technology Session of America, Fourth Annual IT Policy Summit.

Aaron, David L. 2001. Testimony -European Union and Electronic Privacy. Washington, D.C.: House Committee on Energy and Commerce.

Albrow, Martin. 1997. *The Global Age*. Stanford: Stanford University Press.

Anderson, James. 1996. The Shifting Stage of Politics: New Medieval and Postmodern Territorialities. *Environment and Planning D: Society and Space* 14:133-153.

Article 29 - Data Protection Working Party. 2002. Working Document on Determining the International Application of EU Data Protection Law to Personal Data Processing on the Internet by Non-EU Based Websites. Brussels: European Commission Internal Market DG.

Banisar, David, and Simon Davies. 1999. Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments. *John Marshall Journal of Computer and Information Law* 18:1-111.

Bennett, Colin J. 1997. Convergence Revisited: Toward a Global Policy for the Protection of Personal Data? In *Technology and Privacy: The New Landscapte*, edited by P. E. Agree and M. Rotenberg. Cambridge: The MIT Press.

Berman, Paul Schiff. 2002. The Globalization of Jurisdiction: Cyberspace, Nation States, and Community Definition. Harford, University of Connecticut School of Law.

Castells, Manuel. 2000. *The rise of the network society*. Edited by M. Castells. 2nd ed, *Information age ; v. 1*. Oxford ; Malden, Mass.: Blackwell Publishers.

Caudill, Eve M., and Patrick E. Murphy. 2000. Consumer Online Privacy: Legal and Ethical Issues. *Journal of Public Policy and Marketing* 19 (1):7-.

Council of the Europe. 1950. Convention for the Protection of Human Rights and Fundamental Freedoms.

European Commission Staff. 2002. The Application of Commission Decision 520/2000/EC of July 26 2000 Pursuant to Directive 95/46 of the European Parliament and the Council. Brussels: European Commission.

Farrell, Henry. 2002. Constructing the International Foundations of E-Commerce - The EU-US Safe Harbor Arrangement. Bonn: Max Panck Institute.

Farrell, Henry. forthcoming. Negotiating Privacy Across Arenas -- The EU-US Safe Harbor Discussions. In *Common Goods: Reinventing European and International Governance*, edited by A. Heritier: Rowman and Littlefield.

Frumholz, Julia M. 2000. The European Data Privacy Directive. *Berkeley Technology Law Journal* 15:461-484.

Gellman, Robert. 1997. Does Privacy Law Work. In *Technology and Privacy: The New Landscapte*, edited by P. E. Agree and M. Rotenberg. Cambridge: The MIT Press.

George, Barbara Crutchfield, Patricia Lynch, and Susan J. Marsnik. 2001. U.S. Multinational Employers: Navigating Throught the "Safe Harbor" Principles to Comply with the EU Data Privacy Directive. *American Business Law Journal* 38:735-783.

Goolsbee, Austan. 2000. "In a World Without Border: The Impact of Taxes on Internet Commerce". *The Quarterly Journal of Economics* 115:561-76.

Gormley, Ken. 1992. One Hundred Years of Privacy. *Wisconsin Law Review*:1335-1441.
Gruenwald, Juliana. 2001. *Safe Harbor, Stormy Waters* Interactive Week, October 30 2000 [cited May 5 2001]. Available from http://www.zdnet.com/zdnn.
Habermas, Jurgen. 2001. *The Postnational Coalition: Political Essays*. Cambridge: MIT Press.
Harvey, David. 1990. *The Condition of Postmodernity*. Cambridge, MA: Blackwell Publishers.
Kang, Jerry. 1998. Information Privacy in Cyberspace Transactions. *Stanford Law Review* 50:1193-1294.
Long, William J., and Mark Pang Quek. 2001. Personal Data Privacy Protection in an Age of Globalization: The U.S. - EU Safe Harbor Compromise. Atlanta: Sam Nunn School of International Affairs, Georgia Institute of Technology.
McGrew, Anthony. 1997. Globalization and Territorial Democracy: An Introduction. In *The Transformation of Democracy*, edited by A. McGrew. London: Polity Press.
Milberg, Sandra J., H. Jeff Smith, and Sandra J. Burke. 2000. Information Privacy: Corporate Management and National Regulation. *Organization Science* 11 (1):35-57.
Mitchener, Brandon. 2002. Rules, Regulations of the Global Economy are Increasingly Being Set in Brussels. *Wall Street Journal On Line*, April 23, 1.
Privacy Working Group. 2002. *Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information* (January 11) Information Infrastructure Task Force, 1995 [cited 2002]. Available from http://www.iitf.nist.gov/ipc/ipc-pubs/niiprivprin_final.html.
Reidenberg, Joel R. 1995. Setting Standards for Fair Information Practice in the U.S. Private Sector. *Iowa Law Review* 80 (3):497-551.
Reidenberg, Joel R. 2000. Resolving Conflicting International Data Privacy Rules in Cyberspace. *Stanford Law Review* 52:1315-1371.
Reidenberg, Joel R. 2001a. E-Commerce and Trans-Atlantic Privacy. *Houston Law Review* 38:717-749.
Reidenberg, Joel R. 2001b. Testimony before Subcommittee on Commerce, Trade, and Consumer Protection. Washington, D.C.: Federal Document Clearing House.
Reidenberg, Joel R., and Paul M Schwartz. 1998. Data Protection Law and On-line Services: Regulatory Responses. Brussels: European Commission, Directorate General XV.
Roch, Michael P. 1996. Filling the Void of Data Protection in the United Sates: Following the European Example. *Santa Clara Computer and High Technology Law Journal* 12:71-96.
Rosenau, James N. 1997. *Along the domestic-foreign frontier : exploring governance in a turbulent world*, *Cambridge studies in international relations ; 53*. Cambridge, U.K. ; New York, NY: Cambridge University Press.
Ruggie, John Gerard. 1993. Territoriality and Beyond: Problematizing Modernity in International Relations. *International Organization* 47 (1, Winter):139-174.
Sassen, Saskia. 2000. Territory and Territoriality in the Global Economy. *International Sociology* 15 (2):372-393.

Shimanek, Anna E. 2001. Do You Want Milk with Those Cookies? Complying with the Safe Harbor Privacy Principles. *The Journal of Corporation Law* (Winter):456-477.

Smitis, Spiros. 1996. Foreward. In *Data Privacy Law*, edited by P. M. Schwartz and J. R. Reidenberg. Charlottesville, VA: Michie.

Swire, Peter P., and Robert E. Litan. 1998. *None of Your Business*. Washington, D.C.: Brookings Institution Press.

The Council. 1995. Common Position (EC) No /95 Adopted by the Council with a View to Adopting Diective 94/EC of the European Parliament and of the Council on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data, Directive 95/EC of the European Parliament and of the Council of On The Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movment of Such Data. Brussels: European Union.

Wrenn, Gegory J. 2002. Cyberspace is Real, Borders are Fiction: The Protection of Expressive Rights Online Through Recognition of National Borders in Cyberspace. *Stanford Journal of International Law* 38:97-106.

Zurn, Michael. 2000. Democratic Governance Beyond the Nation-State: The EU and Other International Institutions. *European Journal of International Relations* 6 (2):183-221.