Review of International Studies (2004), 30, 111–131
DOI: 10.1017/S0260210504005856

Safe harbours are hard to find: the trans-Atlantic data privacy dispute, territorial jurisdiction and global governance

STEPHEN J. KOBRIN*

Abstract. The trans-Atlantic dispute over application of the European Union's Data Directive (1995) is discussed as a case study of an emerging geographic incongruity between the reach and domain of the territorially-defined Westphalian state and the deep and dense network of economic relations. The article reviews significant EU-US differences about the meaning of privacy and the means to protect it, the history of attempts to apply its provisions to information transferred to the US, and the less than satisfactory attempt at resolution – the Safe Harbor agreement. It then argues that attempting to apply the Directive to transactions on the Internet raises fundamental questions about the meaning of borders, territorial sovereignty and political space and explores the implications for territorial jurisdiction and global governance at some length.

> The spatial scope of social and political organization is not set for all time. The territorial state is not a sacred unit beyond historical time.[1]

Given the Westphalian state system's norm of mutually exclusive geographic jurisdiction – of borders and territorial sovereignty – one would expect differences in law and regulation to be the rule: they are definitional at the most basic level. Germany's strict control of retail store opening hours and limits on promotional or discount activity, compared with the absence of virtually any limits on either in the United States, provide an example.

Regulatory differences become problematic when there is cross-border 'spillover' into other jurisdictions. That occurs when (1) the impact of the regulation is not (or cannot be) 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.

Regulatory spillover is becoming more common in the trans-Atlantic context. EU competition authorities' objections derailed the merger of Honeywell and General Electric, two 'American' companies, and the head of the US Anti-Trust Division felt

* Stephen Brooks, Craig Eisendrath, Henry Farrell, Dan Hunter, Ed Mansfield, David Post and Joel Reidenberg provided comments on a previous draft.

[1] John A. Agnew. Timeless Space and State-Centrism: The Geographical Assumptions of International Relations Theory. In S. J. Rostow, N. Inayatullah and M. Rupert (eds.), *The Global Economy as Political Space* (Boulder, CO: Lynne Reinner, 1994).

it necessary to remind European authorities that *their* concerns about Microsoft's use of market power had not held up in American courts. 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 . . .'[2]

The European Union's (1995) Data Directive was designed to protect *Europeans'* data privacy – an individual's control over the processing of personally identifiable or name-linked data.[3] However, in a world where (electronic) cross-border data flows are inevitable, that regulation *must* reach beyond the EU if it is to be meaningful, it must apply wherever the data are transferred and processed. Cross-border spillover is necessary if the Data Directive is to be effective; in this case, 'domestic' legislation has a transnational footprint.

Neither cross-border transactions nor jurisdictional conflict are new: both are inherent in an international system rooted in geography, in the 'institutionalization of public authority within mutually exclusive territorial domains'.[4] The structure of the Westphalian international system, however, assumes that jurisdictional conflict and extra-territorial reach are the exception rather than the rule; that states accept geographic limits to claims to their authority to allow both their coexistence in defined territorial spaces and extensive cross-border interactions.[5] It is reasonable to ask whether the exception could become the rule: whether the increasing intensity, depth, and geographic ambiguity of transnational economic transactions will compromise the assumptions underlying an interstate system rooted in geographic sovereignty.

The dispute arising from the European Union's attempts to protect data privacy raises difficult questions about both territorial jurisdiction and democratic governance, about how political 'space' and political community are defined in the digital age. These two themes, which will be explored in this article, are closely related.

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.[6] To the extent that transactions on the Internet are location-independent, or occur in multiple locations simultaneously, the idea of political space as a bounded geographic construct loses meaning. If that is the case, territorial sovereignty, as mutually exclusive geographic jurisdiction based upon discrete and effective borders, becomes problematic. As Berman observes, '. . . the issue of jurisdiction is deeply enmeshed with precisely the fixed conception of territorial boundaries that contemporary events are challenging'.[7]

[2] Brandon Mitchener, 'Rules, Regulations of the Global Economy are Increasingly Being Set in Brussels', *Wall Street Journal On Line*, 23 April, 2002, p. 1.

[3] Jerry Kang, 'Information Privacy in Cyberspace Transactions', *Stanford Law Review*, 50 (1998), pp. 1193–294.

[4] John Gerard Ruggie, 'Territoriality and Beyond: Problematizing Modernity in International Relations', *International Organization*, 47:1 (1993), pp. 139–74.

[5] Hendrik Spruyt, *The Sovereign State and Its Competitors* (Princeton, NJ: Princeton University Press, 1994).

[6] Paul Schiff Berman, 'The Globalization of Jurisdiction', *The University of Pennsylvania Law Review*, 151 (2002).

[7] Berman, 'The Globalization of Jurisdiction', p. 318.

The dispute over the Data Directive illustrates an asymmetry between politics and markets in terms of both their scope or extent and their mode of organisation, between an integrated trans-Atlantic economy and fragmented governance structures – political authorities and political communities still contained within national (or regional) borders. More generally, there is an 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 constitute the early twenty-first century world economy.

Article 25 of the Data Directive (of which much more below) prohibits the 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 had catastrophic impacts, bilateral negotiations were undertaken resulting in the 'Safe Harbor' agreement which attempts to provide protection for personal information deemed adequate by the Europeans without unduly compromising American beliefs in self-regulation and the marketplace. Safe Harbor, however, 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.

Political conceptions of jurisdiction and community are not naturally defined, but socially constructed. In a world where spill-over and inter-jurisdictional conflict are becoming the norm and political space as a bounded geographic construct is losing meaning, establishing effective governance structures which retain some sense of democratic legitimacy may require reconceptualising both jurisdiction and political community. It may require some means of restoring the symmetry or congruity between economics and politics.

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 their implementation. I will then review the progress of Safe Harbor to date and conclude by discussing the implications of the data privacy dispute for territorial jurisdiction and global governance at some length.

Data privacy

Data privacy involves the terms under which information identifiable to an individual is acquired, disclosed and used.[8] Concern about information privacy is not

[8] Privacy Working Group, *Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information*, Information Infrastructure Task Force (11 January, 1995 [cited 2002]). Available from <http://www.iitf.nist.gov/ipc/ipc-pubs/niiprivprin_final.html>. 'Identifiable to an individual' has been defined in terms of an authorship relation, descriptive relation, or an instrumental relation. Kang, 'Information Privacy in Cyberspace Transactions'. The EU Data Directive defines an identifiable person is one who can be identified directly or indirectly, by reference either to an identification number or 'one or more factors specific to his physical, physiological, mental, economic, cultural or social identity'. The Council: Common Position (EC) no. 95. Adopted by the Council with a View to Adopting Directive 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 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (Brussels: European Union, 1995).

new; the New York Police Department 'tapped' their first telephone call in 1895[9] and party-line telephones were notorious in rural areas.

That being said, the information revolution and the ubiquity of Cyberspace have significantly increased the threats 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, analysed, and reused.[10] Rapidly developing technologies (data mining) are providing new and very powerful means to sort, combine and analyse data. Last and critically, these data exist in a *networked environment*: personal information collected and processed on any computer on the Net is, at least in theory, accessible by every computer on the Net.[11]

In fact, the gathering of personal information and profiling are part and parcel of electronic commerce. A January 2000 US Federal Trade Commission survey reveals that between 97 and 99 per cent of all websites collect personal identifying information from and about consumers.[12]

Protecting personal information

The protection of personal information entails complex benefit/cost trade-offs for both society and individuals. *The Economist*[13] argues that 'the end of privacy' will result from the cumulative effect of a series of bargains where each benefit offered by the information economy, such as cheaper communications, more entertainment, better government services or a wider selection of products, seems worth the surrender of a bit more personal information.

As Fromholz notes, privacy is not an absolute good: it results in unquestioned benefits, but also 'imposes real costs on society'.[14] 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'

[9] Eli M. Noam, 'Privacy and Self-Regulation: Markets for Electronic Privacy'. In *Privacy and Self-Regulation in the Information Age*, edited by National Telecommunications and Information Adminstration (Washington, DC: US Department of Commerce, 1997).

[10] Privacy Working Group, *Privacy and the National Information Infrastructure*.

[11] Joel R. Reidenberg, 'Resolving Conflicting International Data Privacy Rules in Cyberspace'. *Stanford Law Review*, 52 (2000), pp. 1315–71.

[12] The FTC concludes that 'Most of the sites surveyed, therefore, are capable of creating personal profiles of online consumers by tying any demographic, interest, purchasing behavior, or surfing behavior information they collect to personal identifying information'. Bureau of Consumer Protection, *Privacy Online: Fair Information Practices in the Electronic Marketplace* (Washington, DC: Federal Trade Commission, 2000).

[13] 'The End of Privacy', *The Economist*, 1 May 1999, pp. 15–16.

[14] Julia M. Frumholz, 'The European Data Privacy Directive', *Berkeley Technology Law Journal*, 15 (2000), pp. 461–84.

demands that they be informed about the gathering and use of this data are often in tension.[15] The constant struggle between the information needs of a credit-driven economy and protection of individual privacy provide an example.

How this benefit/cost trade-off is evaluated is a function of culture, social norms, political and economic philosophy and historical experience. The very idea of what information privacy represents, its relative importance *versus* other social 'goods' such as free speech, who is responsible for protecting it, and how it should be protected vary dramatically across countries and cultures, even those as close as Europe and America.

Data privacy is always considered 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'.[16] There is considerable cross-border variation in data privacy *norms*, whether information privacy is a considered a basic human right or a property right for example. These differences in context and norms lead to a good deal of variance in *implementation* and execution. I now turn to a comparison of the context of protection and privacy in the US and EU.

Context and norms

Fundamental differences in the American and European contexts have led to very different data privacy 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[17] – are reflected in deep-seated differences in 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 universally, seen as rights against the government.[18] Thus, the US approach to data privacy reflects a basic distrust of government; markets and self-regulation rather than government oversight shape information privacy in the US and as a result the legislation that does exist is reactive and issue-specific.[19] Protection tends to be tort-based and market oriented rather than legislative or regulatory: a 'patchwork of rules' that deal with specific sectors and problems in a haphazard manner.[20]

[15] Sandra J.Milberg, H. Jeff Smith, and Sandra J. Burke, 'Information Privacy: Corporate Management and National Regulation', *Organization Science*, 11: 1 (2000), pp. 35–57.

[16] Agnew, 'Timeless Space and State-Centrism'.

[17] Reidenberg, 'Resolving Data Privacy Rules'.

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

[19] Barbara Crutchfield George, Patricia Lynch, and Susan J. Marsnik, 'US Multinational Employers: Navigating Throught the "Safe Harbor" Principles to Comply with the EU Data Privacy Directive'. *American Business Law Journal*, 38 (2001), pp. 735–83; Reidenberg, 'Resolving Data Privacy Rules'.

[20] Kang, 'Information Privacy in Cyberspace'; David Banisar and Simon Davies, '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 (1999), pp. 1–111; Frumholz, 'The European Data Privacy Directive'; Reidenberg, 'Resolving Data Privacy Rules'; Michael P. Roch, 'Filling the Void of Data Protection in the United States: Following the European Example', *Santa Clara Computer and High Technology Law Journal*, 12 (1996), pp. 71–96; Peter P. Swire and Robert E. Litan, *None of Your Business* (Washington, DC: Brookings Institution Press, 1998).

In America privacy is seen as an alienable commodity subject to the market. Disputes about personal information as well as mechanisms for its protection are cast in economic terms: questions about property rights; who 'owns' the data collected in a commercial transaction; and who has the right to the rents flowing from its exploitation.[21]

The American emphasis on the market is evident even in the context of regulation. Senator Hollings cast the need for The Online Personal Privacy Act (S.2201) in terms of strong pre-emption (to give business the certainty it needs in the face of conflicting state standards), promoting consumer confidence and bolstering online commerce, and preventing consumer fears from stifling the Internet as a consumer medium.[22]

In contrast, the European approach to privacy puts the burden of protection on society rather than the individual. Privacy is considered to be a fundamental or natural right which is inalienable, and comprehensive systems of social or communitarian protection take the form of explicit statutes accompanied by regulatory agencies to oversee enforcement. It is the protection of the rights of citizens or 'data subjects' rather than consumers or users that is of concern.[23]

The introduction to the EU Data Directive states, '(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 . . .' Article 1.1 of the Directive is clear: 'Member states shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data'.[24] It is not accidental that privacy as a right precedes its contribution to economic and social progress in the text.

In summary, trans-Atlantic differences with regards to data privacy and its protection reflect deeply rooted differences in historical experience, cultural values, and beliefs about the organisation of the polity, economy and society. Ambassador

[21] See Robert W. Hahn and Anne Layne-Farrar, *The Benefits and Costs of Privacy Regulation*. (Washington, DC, AEI-Brookings Joint Center for Regulatory Studies, 2001); Lessig, Lawrence, 'Internet: The Architecture of Privacy', Vanderbilt *Journal of Entertainment Law and Practice*, 1 (1999), pp. 55–65; Jessica Litman, 'Information Privacy/Information Property', *Stanford Law Review*, 52 (2000), pp. 1283–304; James Rule and Lawrence Hunter, 'Towards Property Rights in Personal Data', in C. J. Bennett and R. Grant (eds.), *Visions of Privacy: Policy Choices for the Digital Age* (Toronto: University of Toronto Press, 1999); Paul Sholtz, 'Transaction Costs and the Social Costs of Online Privacy', *First Monday*, 6:5 (2001), for examples.

[22] US Senate Committee on Commerce, Science, and Transportation, 2002. Statement by Senator Ernest F. Hollings. The Online Personal Privacy Act is an attempt to regulate the collection, use or disclosure or personally identifiable information by Internet service providers, website operators, and certain third parties that use these entities to collect information. *Tech. Law Journal* at <http://www.techlawjournal.com/cong107/privacy/hollings/20020418summary.asp> Accessed 5 May, 2003.

[23] Frumholz, 'The European Data Privacy Directive'; George, Lynch, and Marsnik, 'US Multinational Employers and "Safe Harbor" Principles': Directive; Reidenberg, 'Resolving Data Privacy Rules'. European concern about data privacy may be, to some extent, historically driven. The Third Reich's use of private data (and the thought of what that regime might have accomplished with access to modern data bases) and more recent experience with repressive regimes to the East have made Europeans all too aware of the consequences of the accumulation and transfer of personal information for an individual's safety, integrity and privacy. As detailed in Edwin Black, *IBM and the Holocaust* (New York: Crown Publishers, 2001), the Third Reich made full use of punch-card sorting machines, primitive technology by today's standards.

[24] The Council: Common Position (EC) no. 95. See n. 8 above.

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.'[25]

One caveat is important; it is difficult to generalise about European and American data privacy norms. Data privacy in Europe may well be an elite concern and it is not clear how widespread concern is among the mass of Europeans at large. Furthermore, much of the privacy rhetoric in the United Sates flows from interest groups: business lobbies on the one hand and privacy advocates on the other. Survey data indicates that the American public is concerned about personal privacy and is, to some degree, ambivalent about the capacity of the market or self-regulatory solutions to solve the problem.

The implementation of privacy protection

The United States. The word 'privacy' is never mentioned in the Constitution, neither that document nor the Bill of Rights deal with the issue explicitly.[26] As late as 1890 when Samuel Warren and Louis Brandeis published their famous *Harvard Law Review* article defining privacy as 'the right to be left alone', a coherent notion of privacy did not exist in American law.[27]

The extension of the Fourth Amendment's guarantees against unreasonable searches and seizures to deal with privacy issues took the better part of another century. Even then, the Supreme Court was clear that Fourth Amendment protection only applies to 'certain kinds of governmental intrusion' and not to the private sector; it protects citizens against the government rather than one another.[28]

The development of protection has been sporadic, inchoate, sectorially specific and reactive. The Fair Credit Reporting Act of 1970 was the first US attempt at protecting information privacy in the private sector.[29] Subsequent legislation has dealt with specific problems as deemed necessary; 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.[30]

[25] David L.Aaron, Testimony – European Union and Electronic Privacy (Washington, DC: House Committee on Energy and Commerce, 2001).

[26] Robert Gellman, 'Does Privacy Law Work?' In P. E. Agree and M. Rotenberg (eds.), *Technology and Privacy: The New Landscape* (Cambridge, MA: The MIT Press, 1997); George, Lynch, and Marsnik. 'US Multinational Employers and 'Safe Harbor' Principles; Roch, 'Filling the Void of Data Protection'; Joel R. Reidenberg, 'Setting Standards for Fair Information Practice in the US Private Sector', *Iowa Law Review*, 80: 3 (1995), pp. 497–551.

[27] Ken Gormley, 'One Hundred Years of Privacy', *Wisconsin Law Review* (1992), pp. 1335–441. It is of interest that 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, 'Setting Standards'.

[28] Gellman, 'Does Privacy Law Work?'; Gormley, 'One Hundred Years of Privacy'; Reidenberg, 'Setting Standards'.

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

[30] Frumholz, 'The European Data Privacy Directive'.

After reviewing results of its 2000 survey of the privacy practices of Websites, the Federal Trade Commission reversed its previous opinion and argued that self-regulation alone was not sufficient and recommended that Congress enact legislation to ensure adequate protection of consumer privacy online.[31] However, although there are a number of bills being considered by Congress, regulatory protection of data privacy in the United States is still quite limited.

The European Union. 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'.[32] The right to privacy is specifically mentioned in a number of constitutions (for example, Germany and Spain) and in the Council of Europe's 'Convention for the Protection of Human Rights and Fundamental Freedoms'.[33]

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).[34] 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 Individuals with Regard to Automatic Processing of Personal Data.*[35]

The Council of Europe's 1981 Convention was based on the OECD guidelines and called for national implementation of data privacy laws by individual European states. It is important to note that both the OECD guidelines and the Council's Convention call for explicit privacy legislation and support curbs of transborder data flows if protection in the recipient country is not sufficient.[36]

By the early 1990s many of the EU member states had enacted data privacy laws based on the Council's Convention and as barriers to full economic and financial integration fell, differences in national data protection legislation became a concern. The Data Directive was proposed as a means to harmonise data protection laws; Directive 95/46/EC of the European Parliament and of the Council 'on the protection of individuals with regard to the processing of personal data and the free movement of such data' was enacted in 1995 and came into force in 1998. The Directive does not apply directly, but requires each member state to enact legislation which meets minimum standards for the protection of personal information.[37] The primary provisions of the Directive require that:

[31] Bureau of Consumer Protection, *Privacy Online: Fair Information Practices*.

[32] Roch, 'Filling the Void of Data Protection'.

[33] George, Lynch, and Marsnik, 'US Multinational Employers and "Safe Harbor" Principles'. 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). Convention for the Protection of Human Rights and Fundamental Freedoms (Council of Europe. 1950).

[34] Roch, 'Filling the Void of Data Protection'.

[35] Swire and Litan, *None of Your Business*.

[36] George, Lynch, and Marsnik, 'US Multinational Employers and "Safe Harbor" Principles'; Roch, 'Filling the Void of Data Protection'.

[37] George, Lynch, and Marsnik, 'US Multinational Employers and "Safe Harbor" Principles'; Joel R. Reidenberg, Testimony before Subcommittee on Commerce, Trade, and Consumer Protection (Washington, DC: Federal Document Clearing House, 2001b); Roch, 'Filling the Void of Data Protection'; Swire and Litan, *None of Your Business*.

- 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.

As noted above, effective implementation of the Directive's provisions required recognition of the reality of cross-border data flows. Simitis[38] argues that a regulation which 'ignored international transfers could hardly be reconciled with the direct relationship repeatedly stressed with the Union's commitment to human rights. . . . The Community's duty to respect and guarantee human rights does not cease at the Union's borders.' Concern about data being processed beyond the reach of European Authorities resulted in Articles 25 and 26 of the Directive which contain provisions for controlling transfer to third countries.

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 issue of adequacy is to be assessed in 'light of all of the circumstances surrounding the data transfer operation' (25.2) and if the Commission finds that a third country does not ensure an adequate level of protection, member states should take the necessary measures to prevent the data transfer (25.4).[39]

Article 26 contains a number of 'derogations' which allow data transfer to countries where protection has not been deemed adequate given 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.[40]

The derogations aside, as standards of data protection in the US were unlikely to meet the EU's criteria for adequacy, the provisions of Article 25 represented a serious threat to trans-Atlantic data flows. However, Article 25 also contains a provision (25.5) which instructs the Commission to enter into negotiations with third countries when there has been a finding that data protection levels are not

[38] Spiros Smitis, 'Foreword', in P. M. Schwartz and J. R. Reidenberg (eds.), *Data Privacy Law* (Charlottesville, VA: Michie, 1996).
[39] The Council: Common Position (EC) no. 95. See n. 8 above.
[40] Smitis, 'Foreword'.

adequate 'with a view to remedying the situation.'[41] That led directly to the Safe Harbor negotiations with the United States.

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 US and the EU Commission.[42] Initial discussions were frustrated by a lack of common ground until Washington realised that the Commission was not going to accept the existing American self-regulatory regime as adequate. Negotiations then began in earnest between David Aaron, the Undersecretary for Trade in the Department of Commerce, and John Mogg, the Director General for the Internal Market.[43]

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. A suggestion by Aaron that adequacy should be judged on an organisation by organisation basis proved critical;[44] 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'.[45]

The Department of Commerce proposed a first set of Safe Harbor principles in November 1998 and after eighteen months of negotiation, 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.[46] (The European Parliament, which had the authority to advise but not to consent to the agreement, 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. The Principles, which are consistent with both the 1980 OECD Data Protection Guidelines and the Data Directive, require organisations to provide for notice about the

[41] The Council, 1995. Common Position (EC) no. 95. See n. 8 above.

[42] William J. Long, and Mark Pang Quek, *Personal Data Privacy Protection in an Age of Globalization: The US – EU Safe Harbor Compromise* (Atlanta, GA: Sam Nunn School of International Affairs, Georgia Institute of Technology, 2001). Writing in 1995, Simitis argued that 'most transfer cases are, in fact, covered by the long list of exceptions found in Article 26…', Smitis, 'Foreword'. See Henry Farrell, 'Constructing the International Foundations of E-Commerce – The EU-US Safe Harbor Arrangement,' *International Organization*, 57 (Spring 2003); and Henry Farrell, 'Negotiating Privacy Across Arenas – The EU-US Safe Harbor Discussions', in A. Heritier (ed.), *Common Goods: Reinventing European and International Governance* (Rowman and Littlefield, forthcoming) for a detailed discussion of the Safe Harbor negotiations.

[43] Farrell, 'Negotiating Privacy Across Arenas'.

[44] Ibid.

[45] David L. Aaron, 'Remarks before the Information Technology Session of America, Fourth Annual IT Policy Summit' (1999), p. 4.

[46] Farrell, 'Constructing the International Foundations of E-Commerce'. Long and Quek, 'Personal Data Privacy Protection'; Anna E. Shimanek, 'Do You Want Milk with Those Cookies? Complying with the Safe Harbor Privacy Principles'. *The Journal of Corporation Law* (Winter 2001), pp. 456–77.

collection and use of information, choice or the opportunity to 'opt out', controls over onward transfer, access by individuals to personal information, security of name-linked data, data integrity and compliance. Enforcement of Safe Harbor relies on prosecution for unfair or deceptive advertising or promises by the Federal Trade Commission.[47] An organisation may enter the Safe Harbor by either joining an approved self-regulatory programme or developing its own compliant privacy policy and certifying it annually to the Department of Commerce.[48]

Safe Harbor is neither a treaty nor an international agreement but rather two unilateral actions: the US issued the principles and the Commission issued an Article accepting them. [49] In keeping with the American tradition of privacy protection, Safe Harbor was a reactive response to the threat of an interruption of data transfers between the EU and US.[50] It is an attempt to harmonise the effects of data protection schemes, rather than to reach agreement on principles or methods. Farrell describes Safe Harbor as an 'interface' between the European system of formal regulation and the American system of self-regulation which is qualitatively different from either.[51]

It is fair to say that Safe Harbor has not been seen as an overwhelming success on either side of the Atlantic. As of 7 May, 2003 only 338 companies had enrolled, few of them major multinationals.[52] The relatively low number of firms which have signed up reflects concern about Safe Harbor combined with a sense that, at least at this point, the penalties for non-compliance are not very obvious. (The dispute and Safe Harbor negotiations have increased awareness of data privacy as an issue on both sides of the Atlantic.)

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 US and that it might subject them to unforeseen liabilities in Europe.[53] Concern about the impact of Safe Harbor on the American data privacy regime shadowed

[47] The FTC's legal authority comes from Section 5 of the Federal Trade Commission Act which prohibits unfair or deceptive practices. Joel R. Reidenberg, 'E-Commerce and Trans-Atlantic Privacy', *Houston Law Review*, 38 (2001a), pp. 717–49, argues that the Constitutional basis for FTC oversight here is questionable. 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.

[48] A more complete description of Safe Harbor can be found at <www.export.gov/safeharbor/sh_overview.html>

[49] David L. Aaron, 'Testimony – European Union and Electronic Privacy'. The EU agreed to Safe Harbor on 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.

[50] A complete description of Safe Harbor and its provisions can be found on the Department of Commerce's Website at <http://www.export.gov/safeharbor/sh_overview.html>

[51] Farrell, 'Constructing the International Foundations of E-Commerce'.

[52] The list of organisations enrolled in Safe Harbor can be accessed from <www.export.gov/safeharbor/>

[53] Juliana Gruenwald, 'Safe Harbor, Stormy Waters', *Interactive Week* (30 October 2000 [cited 5 May 2001]). Available from <http://www.zdnet.com/zdnn>. A lawyer in a major international firm noted that most American companies find it difficult to enter into the contracts called for under the Safe Harbor agreement and would not do so on their own. Bob Sherwood, 'Inside Track Law & Business', *The Financial Times*, 21 October 2002, p. 20.

the entire process of negotiations: in a talk given to an industry group Ambassador Aaron took pains to make it clear that '. . . these safe harbor principles have been developed and are aimed at a specific situation – reassuring the Europeans that their privacy . . . will be protected. . . . In no way does the U.S. government intend for these safe harbor principles to be seen as precedents for any future changes in the U.S. privacy regime.'[54]

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,[55] 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 decisions about international privacy.'

Safe Harbor was controversial in Europe from the start with serious questions raised by both national data authorities and in the European Parliament about the adequacy of data protection. A European Commission Staff Working Paper issued in early 2002 was diplomatic, but expressed serious concern about both implementation and the adequacy of data protection. It notes that the number of organisations 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 organisations do not meet the requirement that they publish a compliant privacy policy and indicate publicly their adherence to Safe Harbor. Less than half of those organisations post privacy policies that reflect all seven Safe Harbor principles or inform individuals how they can proceed with complaints and a dispute resolution mechanism. It observes that no company has been prosecuted for making false statements.[56]

Territorial jurisdiction and the Internet

The European Data Directive emerged during the last moments before Cyberspace exploded; it envisions a world of mainframe computers and trans-border data flows.[57] It reflects a transitory state of affairs: data transferred electronically in a physical world where borders, geography and a sense of place dominate. Article 25 is phrased in terms of the 'transfer' of personal data to third countries and assumes a temporal sequence: that the data will either be transferred after processing or processed after transfer.[58]

[54] Aaron: Remarks before the Information Technology Session of America, Fourth Annual IT Policy Summit.

[55] Reidenberg. E-Commerce and Trans-Atlantic Privacy.

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

[57] Swire and Litan, *None of Your Business*.

[58] The European Data Directive descends from the data protection principles established in the OECD Guidelines of 1980 and the Council of Europe's Convention of 1981. Its immediate stimulus was the Single Market Initiative of the late 1980s; the initial data protection proposal was made by the Commission in 1990, a second draft was released in late 1992, and agreement was reached with the Member States in December 1994 prior to its adoption in February 1995 by the Council of Ministers. Priscilla M. Regan, American Business and the European Data Protection Directive: Lobbying Strategies and Tactics. In C. J. Bennett and R. Grant (eds.), *Visions of Privacy: Policy Choices for the Digital Age* (Toronto: University of Toronto Press, 1996); Swire and Litan, *None of Your Business*.

In this world of trans-border data flows or data 'exports',[59] the jurisdictional issues raised are relatively straightforward; the Directive uses the criterion of '*place of establishment of the controller*' or, in other words, the country of origin principle.[60] If the data are collected within the EU and processed within the borders of a member state (or 'exported' for processing), there is no question about the applicability of the Directive and Article 25 takes the form of a traditional 'at the border' control.

Transactions in the Internet's world of networked computers are much more ambiguous. 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 when: (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 . . .'[61] This clause has been interpreted broadly to mean that a website anywhere in the world accessed by a user whose computer is located within the EU can be seen as 'making use of equipment' situated on territory of a member state.[62]

A more 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 website is located nor the place at which the web site is accessible, but rather the place where it pursues its *activity*.[63] 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 are sent back to the originating website, 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.

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 reasonable 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'.[64] That conclusion, however, is problematic in a world organised politically in terms of territorial sovereignty.

[59] Schwartz and Reidenberg, *Data Privacy Law*.

[60] Article 29 – Data Protection Working Party. 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, 2002).

[61] The Council, 1995 (emphasis added). 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. Joel R. Reidenberg and Paul M Schwartz. Data Protection Law and On-line Services: Regulatory Responses (Brussels: European Commission, Directorate General XV, 1998).

[62] Reidenberg, 'E-Commerce and Trans-Atlantic Privacy'; Swire and Litan, *None of Your Business*.

[63] Article 29 – Data Protection Working Party.

[64] Ibid.

It should be noted that the data privacy dispute is only one of a number of recent Internet cases which have raised difficult questions about the extent and meaning of territorial jurisdiction. In November of 2000, a French Court held that Yahoo! must block Internet users located in France from accessing auctions of Nazi memorabilia on its US website, even though the sales were perfectly legal in the United States, indeed protected by the First Amendment. Australia's highest court held (in December, 2002) that Dow Jones could be sued for libel in Australia for an article that appeared on the Baron's American website.[65] Both cases rest on an assumption that a virtual presence provides a basis for jurisdiction.

There is a large and well developed legal literature dealing with questions of jurisdiction and the Internet.[66] Much of the 'early' argument revolved around the question of whether or not Cyberspace is *borderless*; whether geographic jurisdiction can be mapped on a virtual network. In a well known article that set the parameters of the discussion for some time, Johnson and Post argued that Cyberspace breaks down the correspondence between physical boundaries and 'law space', that 'Cyberspace radically undermines the relationship between legally significant (online) phenomena and physical location.'[67]

In response, Goldsmith[68] and others dismissed 'Cyberanarchy', arguing that all of the equipment connected to the Net and all of the people who use it are located in a specific physical place and that sceptics underestimate the power of traditional legal tools to deal with multi-jurisdictional regulatory problems. They argue that the Net is not borderless, but subject to traditional political and legal jurisdiction. The fundamental question at hand, however, is not whether the Internet is 'borderless', but whether the meaning of borders, mutually exclusive jurisdiction, and territoriality as political constructs will erode as Cyberspace and electronic networks gain in importance.

Borders are not, and never have been, impenetrable barriers to flows of people, goods, currency and information. However, it is reasonable to ask if they will continue to be 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.[69]

In Cyberspace the term 'crossing borders' may be no more than a metaphor and an inappropriate one at that. In an interesting paper, Hunter[70] argues that the

[65] See Joel Reidenberg 'Yahoo! and Democracy on the Internet', *Jurimetrics*, 42 (Spring 2002) and 'An Aussie Can Sue Over Online Story', *Wired News*, 10 December 2002, at <www.wired.com/new/business/0,1367,56793,00.html> Access 7 May, 2003.

[66] See Michael A Geist, 'Is There a There There? Toward Greater Certainty for Internet Jurisdiction'. *Berkeley Technology Law Journal*, 16 (2001), pp. 1345–407.

[67] David Johnson and David Post, 'Law and Borders: The Rise of Law in Cyberspace'. *Stanford Law Review*, 48: 5 (1996), pp. 1367–402.

[68] Jack L. Goldsmith, 'Against Cyberanarchy'. *University of Chicago Law Review*, 65 (1998), pp. 1199–250.

[69] Austan Goolsbee,. 'In a World Without Borders: The Impact of Taxes on Internet Commerce'. *The Quarterly Journal of Economics*, 115 (2000), pp. 561–76.

[70] Dan Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons* (Philadelphia, PA: The Wharton School, 2002).

construct of 'Cyberspace as place' is a cognitive physical metaphor that leads to a view of Cyberspace as physical property which is dysfunctional in terms of attempts to develop a legal or regulatory framework for the Internet. 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. Cyberspace is characterised by a 'non-vectorial simultaneity', the possibility that interactions or transactions can take place in multiple 'places' at a single time.[71]

The concept of mutually exclusive jurisdiction and territorial sovereignty gives any state the right to apply its law and regulation within its borders and to its citizens abroad; attempts to apply law and regulation *extra-territorially*, to non-nationals who are outside the state's borders, violates system norms. That term has been used to describe application of the EU's Data Directive to third countries;[72] indeed a recent EU Commission Working Party Report concerned with the question of the international implications of the Data Directive, uses examples such as competition law and consumer protection to argue explicitly that extra-territorial application may be necessary to protect the rights and interests of EU citizens.[73]

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. Taken to its logical limit, that implies that every website or 'data controller' is, at least potentially, subject to regulation emanating from every jurisdiction in the world, a situation that has been described as 'hyper-regulation'.[74]

That possibility would turn the idea of extra-territoriality on its head and corrupt fundamentally geography or territoriality as the organising principle of the modern interstate system. At some point quantity becomes quality; if 'cross-border' transactions, regulatory spill-over and extra-territorial jurisdictional reach become the norm rather the exception, one would have to question the meaning of both internal sovereignty in terms of the state as the ultimate domestic authority within its borders

[71] Stephen J. Kobrin, Territoriality and the Governance of Cyberspace. *Journal of International Business Studies*, 32: 4 (2001), pp. 687–704.

[72] George, Lynch, and Marsnik, 'US Multinational Employers and "Safe Harbor" Principles'.

[73] Article 29 – Data Protection Working Party. Working Document on Determining the International Application of EU Data Protection Law to Personal Data Processing on the Internet by Non-EU Based Websites.

[74] Gegory J. Wrenn, '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 (2002), pp. 97–106. Goldsmith, 'Against Cyberanarchy', argues that given the unenforceability of most extra-territorial judgments, this possibility is not an issue in practice. While that may be true at present, the problem is still conceptually important and it is far from clear that the threat of hyper-regulation is merely ephemeral.

and external sovereignty in terms of the fundamental concept of mutually exclusive geographic jurisdiction.

If personal information can be transmitted instantaneously to multiple locations anywhere in the world, its location becomes ambiguous.[75] 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. Extra-territoriality not only becomes the norm, the concept itself loses 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 organising principle underlying the international political system.

Data privacy and democratic governance

As discussed above, there are significant differences in belief systems between Europe and the US. 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 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.

McGrew 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'.[76] In fact, a geographically organised 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, and that geographic space has meaning as a political-economic construct.

In the case at hand, we are left with democratic political institutions and belief systems which remain contained within the national space, 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 is affecting our ability to govern effectively.

On the one hand, given the level of 'cross-border' transfers data privacy cannot be protected though unilateral acts within the borders of a single territory. On the other, integration renders the cost of interrupting those 'cross-border' flows so high as to markedly constrain the freedom of action of each government to mitigate spillovers.[77]

[75] Bennett, 'Convergence Revisited: Toward a Global Policy for the Protection of Personal Data?'

[76] Anthony McGrew, Globalization and Territorial Democracy: An Introduction. In A. McGrew (ed.), *The Transformation of Democracy* (London: Polity Press, 1997).

[77] The trans-Atlantic economy is deeply integrated. Sales of American firms' subsidiaries in the EU total over $117 bn (1998) and those of European firms in the US almost $107 bn (1999). The vast majority of those firms transfer financial, credit and marketing data and personnel records among subsidiaries and between subsidiaries and headquarters electronically: their viability depends on their electronic data networks.

This asymmetry between the political space necessary for the effective implementation of the Data Directive – or any effective data privacy regime – and the actual scope of existing territorial jurisdictions (or political communities) is manifest in number of ways in the data privacy dispute. It has generated considerable transnational political activity on the part of interested groups;[78] the Directive resulted in what has been called a 'firestorm' of criticism in the US because of concerns that its requirements would prevent the extensive data transfers necessary for effective integrated multinational operations.[79] As a result American business firms lobbied directly in Brussels, and worked in conjunction with their European counterparts through organisations such as the International Chamber of Commerce and the Trans-Atlantic Business Dialogue.[80]

American privacy advocates, who saw the Safe Harbor discussions as a unique opportunity to argue for stronger domestic data protection laws,[81] also established formal linkages with interested European groups. The Trans Atlantic Consumer Dialogue (TACD) is a forum comprised of 45 EU and 20 US consumer groups formed in 1998.[82] While privacy advocates' attempts to influence the process have not yet resulted in legislation in the US, the TACD process allowed consumer groups to work together to influence both officials and Members of the European Parliament in Europe and the legislative process in the US.[83]

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'.[84] That being said, it is difficult to envision an effective solution to the data privacy problem resulting from either (1) regulatory efforts in either jurisdiction or (2) negotiations between the two jurisdictions *qua* jurisdictions. There are two major issues here: democratic legitimacy and the meaning of 'political space' and/or 'political community.'

There is an incongruence between the space where the Data Directive represents the 'self-expression' of a political constituency and where it takes effect: between the actual 'political space' encompassed by the Data Directive and the political space where it reflects the 'common interests' of a distinct constituency.[85] Scharpf decom-

[78] More complete descriptions of the involvement of business and consumer groups in the process can be found in Farrell, 'Negotiating Privacy Across Arenas'; Regan, 'American Business and the European Data Protection Directive: Lobbying Strategies and Tactics'.

[79] Regan, 'American Business and the European Data Protection Directive'.

[80] Farrell, 'Negotiating Privacy Across Arenas'.

[81] Long and Quek, 'Personal Data Privacy Protection'.

[82] Trans Atlantic Consumer Dialogue, *Letter to David Aaron* (3 December 1999 [cited 29 May 2002]). Available from <http://www.tacd.org>

[83] Farrell, 'Negotiating Privacy Across Arenas'. In a letter to Ambassador Aaron during the negotiations the TACD argued that the Safe Harbor proposal 'fails to provide adequate privacy protection for consumers in the United Sates and Europe' and that the lack of adequate protection in the US leaves the country increasingly isolated in the world marketplace. In comments attached to the letter they argued strongly that 'Rather than eroding the principles of the Directive, Safe Harbor should seek to reinforce data protection for all individuals'. Trans Atlantic Consumer Dialogue, *Letter to David Aaron* (3 December 1999 [cited 29 May 2002]). Available from <http://www.tacd.org>

[84] Jurgen Habermas, *The Postnational Coalition: Political Essays* (Cambridge, MA: MIT Press, 2001), p. 70.

[85] Fritz W. Scharpf, 'Interdependence and Democratic Legitimation', in S. J. Pharr and R. D. Putnam (eds.), *Disaffected Democracies: What's Troubling the Trilateral Countries* (Princeton, NJ: Princeton University Press, 2000).

poses legitimacy into two components. Input legitimacy implies that 'collectively binding decisions' flow from the self-expression of the constituency in question; laws should be self-determined rather than imposed exogenously. Output legitimacy implies that collectively binding decisions serve the common interests of the constituency, including those who may oppose the specific decision in question. It assumes that a strong collective identity and a pervasive sense of a common fate will override divergent preferences and interests.

American business firms' have expressed objection to being 'subject' to European law and there is concern among both businesses and the Administration about European law becoming the *de facto* standard for data privacy in the US. On the other hand, Europeans have expressed concern about the lack of adequate protection in the US and the hollowness of the Safe Harbor regime. To the extent interdependence makes the cost of not dealing with American 'data controllers' and US Websites prohibitive, Europeans find themselves subject to a privacy regime that is not of their making and certainly does not reflect their common interests. I suspect that it is fair to say that there is no sense of input legitimacy on either side and both the reluctance of American organisations to submit to Safe Harbor and of Data Regulators in individual European countries to accept its protection as adequate are indications of a lack of output legitimacy, an unwillingness to accept the decision as binding.

The problems with Safe Harbor exemplify the difficulty of negotiating when there is deep-seated disagreement on basic values and beliefs about both the nature of the problem and appropriate solutions. An acceptable middle ground between privacy as an inalienable right and privacy as an alienable commodity, or a belief in the responsibility of society to protect citizens or data subjects and a belief in the individual responsibility of consumers to protect themselves is far from self-evident. It is difficult to conceive of a negotiated solution to the data privacy problem that would be both effective and perceived as legitimate. In the absence of some sense of a political community which transcends the boundaries of either jurisdiction, it is likely that any solution optimal for the larger political space would be rejected as illegitimate by both polities.

Conclusions

The problems raised by the trans-Atlantic data privacy dispute flow from the incongruity between economic and political 'space'. The scope of the global economy and global information networks is considerably broader than that of national territories, the domestic – international 'frontier' is blurred if not erased in both contexts, and both are organised in terms of networks or flows rather than geography. In contrast, politics – jurisdiction, political communities and democratic governance – remains, to a large extent, bounded by national borders and organised geographically. If this incongruity is to be resolved, then in Habermas' terms, politics has to catch up with economics, with global markets.[86]

[86] Jurgen Habermas, *The Postnational Coalition: Political Essays* (Cambridge, MA: MIT Press, 2001).

Berman notes that the two primary issues raised in this article, territoriality or political jurisdiction and governance or political community, are intertwined. Jurisdiction is '. . . the locus for debates about community definition, sovereignty and legitimacy . . . the idea of legal jurisdiction both reflects and reinforces social conceptions of space, distance and identity.'[87] While no definitive resolution of the issues raised in this article is possible – indeed, the outlines of the problem are barely visible at this point – I will suggest briefly three *related* issue areas which represent first steps in that direction: the emergence of multiple and overlapping political authorities, non-territorial forms of jurisdiction, and harmonisation through international institutions.

The geographic organisation 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.[88] I would certainly agree with Anderson that '(T)he medieval-to-modern political transformation was associated with a transformation in how space and time were experienced, conceptualised and represented. With contemporary globalisation we may now be experiencing a similarly radical modern-to-postmodern transformation, with similarly radical consequences for existing territoriality'.[89]

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. The 'space' in which a solution to the data privacy dispute will be found, however, is fundamentally relational and non-geographic. It is a 'space of flows' rather than a 'space of spaces',[90] occupied by networks of multinational firms, internet users, electronic commerce websites, governments, and transnational civil society groups such as the TACD.

It is a space filled with multiple and overlapping political communities and authorities, of individuals who are Americans, members of the TACD and operate websites all at the same time. In a sense then, we have already moved beyond the confines of the Westphalian system of singular national authorities delimited through discrete borders. With the emergence of multiple political actors and communities the foundation for an enlarged, non-territorial political space may be in place.

The transnational reach of 'domestic' data privacy 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 multi-dimensional reconceptualisation of political space, including identities and affiliates as well as territoriality.[91] As an example, Berman argues for a 'cosmopolitan pluralist' concep-

[87] Berman, 'The Globalization of Jurisdiction', p. 319.

[88] Ruggie, 'Territoriality and Beyond'; David Harvey, *The Condition of Postmodernity* (Cambridge, MA: Blackwell Publishers, 1990).

[89] James Anderson, 'The Shifting Stage of Politics: New Medieval and Postmodern Territorialities'. *Environment and Planning D: Society and Space*, 14 (1996), pp. 133–53.

[90] Manuel Castells, *The Rise of the Network Society*, in M. Castells (ed.), *Information Age*, vol. 1 (Malden, MA: Blackwell, 2000).

[91] James N. Rosenau, *Along the Domestic-Foreign Frontier: Exploring Governance in a Turbulent World*, *Cambridge Studies in International Relations* (Cambridge & New York: Cambridge University Press, 1997).

tion of jurisdiction. 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'.[92]

The Westphalian world order of sovereign, territorial states has been the norm for a very long time and it is difficult even to imagine what a shift to non-territorial modes of jurisdiction might entail. Furthermore, jurisdiction is a manifestation of an order grounded in sovereign territoriality and any change in that order's fundamental organising principle will compromise both internal and external sovereignty; the state as supreme domestically and mutually exclusive territoriality. However, as the data privacy dispute illustrates, both territorial jurisdiction and territorial sovereignty are compromised when extra-territoriality and regulatory spillover become the norm rather than the exception; it then makes sense to begin to think about restoring isomorphism between the basis for law and regulation and what is being regulated.

A larger political space will not emerge spontaneously. Furthermore, reconceptualising political space and political jurisdiction are both means to achieve effective and democratic global governance. An effective governance regime will require robust 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. International institutions that make it clear that all affected by political decisions are not located in a single national jurisdiction and which provide the ability for groups affected by a decision to communicate publicly.[93] At a minimum, an expanded sense of political community that provides a basis for harmonisation of national law and regulation that is perceived as democratically legitimate will lay the groundwork for a more general global governance scheme.

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 multiple communities, 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 harmonisation of effects across regions, and helped establish a community of common interest in dealing with these issues. The discussion also helped ensure 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.[94]

Can one can generalise from the trans-Atlantic dispute over the Data Directive? That depends on the extent to which other issues share its critical characteristics. First, cross-border spillover is inherent in that any effective attempt to protect data privacy will have to have an extra-territorial reach. Second, there are deep-seated

[92] Berman, 'The Globalization of Jurisdiction', p. 321.

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

[94] It is important to note that even after extensive discussion at OECD, taxation of purely digital transactions – an exchange of an electronic book for electronic cash, for example – remains problematic. Thus, the analogy to some of the issues raised in this article, while relevant, is imperfect.

differences in beliefs about both the phenomenon itself and appropriate remedies across jurisdictions. Last, concerns about data privacy are increasingly centred in Cyberspace which in itself raises difficult issues about the relevance of borders, geography and the meaning of political space.

There are certainly a number of issues which are inherently international in the sense that their solution is beyond the capabilities of any single national government. Global warming, financial stability, human rights, the AIDS epidemic, and poverty alleviation all serve as examples. An effective remedy for any of these problems will have to have a multi-jurisdictional reach. Several of these issues are also characterised by significant cross-national differences in normative and positive beliefs: the question of patent protection for anti-AIDS drugs and what constitutes a human rights violation (as well as whether international intervention is appropriate) come immediately to mind.

In one sense these issues are similar to data privacy in that effective solutions which are perceived as legitimate will require an expansion of political space, the emergence of a political community which transcends national borders. While far from complete or universally accepted, there are international political communities made up of civil society groups, international organisations, multinational firms, and at least some states which have emerged to deal with human rights and the environment.

To a very large extent, however, these issues play out in physical rather than Cyberspace. That is, in a context where physical borders are meaningful and flows across them can be controlled – at least in theory – by states (global warming may be an exception here). That may limit our ability to generalise from the data privacy dispute, but it is a matter of degree and not kind. To the extent that regulatory spillover becomes the norm rather than the exception, borders, territorial jurisdiction, and geography as the mode of organisation of the political system will become problematic. The data privacy dispute is illustrative of issues which are global in scope while 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.