INFORMATION POLICY AND INFORMATION PRIVACY: INTERNATIONAL ARENAS OF GOVERNANCE

Colin J. Bennett*

I. INTRODUCTION

This paper is based on remarks that I gave at an International Conference on Intellectual Property in Chicago in October, 2002.¹ The hosts very kindly flew me from my hometown to Chicago and showed great hospitality during my stay. They covered my expenses and paid a nice honorarium. For this latter purpose, I was informed by the organizers that reimbursement would be a lot easier if I had a U.S. Social Security Number ("SSN"). Did I have one? If not, could I apply for one? A number of lengthy forms were supplied in the latter eventuality. I inquired, in vain, whether my Canadian Social Insurance Number would suffice – after all, there is a Tax Treaty between the two countries. I also briefly considered making a number up. I recalled that some of the more radical privacy advocates have written about how to make up a valid and new SSN without, of course, jeopardizing the rights of others.

It so happens, however, that I was a student at the University of Illinois ("U of I") in the early 1980s; I completed a Ph.D. in Political Science. And I did, in those years, have a SSN. However, I could not remember it and seemed to have no documentation on which this number appeared. I realized that somewhere in the labyrinthine bureaucracy of the U of I, some record must exist which showed my number. So I contacted my old department (without success), as well as someone in the student transcript department. From the latter, I was informed that I had a SSN on file and that, yes, they could send it to the

* Professor, Department of Political Science, University of Victoria; cjb@uvic.ca; http://web.uvic.ca/~polisci/Bennett/index.htm.
conference organizers. And, so, my immediate problem was solved. However, I then asked the transcript department to send the SSN to me in case I needed it in the future. The response interested me because I was informed that although my SSN could be transferred within the U of I administration, they could not e-mail it to me. Indeed, the only way that I could receive that number would be to order an official copy of my transcript or my certification of degree. The former would cost five dollars, the latter four dollars. If I wished to order these documents, I would have to send, via facsimile, a letter with appropriate identification requesting either or both of these documents and supply a credit card number so that I could be billed. But I had better do this quickly because the transcript department was moving to a new database which would not be including the SSN.

My point in relaying this story is not to make fun of hard-working university employees at my alma mater, nor to highlight the absurdity of a situation in which personal information could be transferred easily to a third party but not back to me, the "data subject." The point is to reflect on the question of whether my SSN is worth five dollars. It is undoubtedly personal information and would be considered such under any privacy or data protection law in the world. On the other hand, I made no effort to create this number. It is not intrinsic to me in the sense that my blood type or genetic make-up is intrinsic. And it clearly is not my property; how could it be if the number itself was unknown to me? Like the thousands of other unique numbers, which may or may not be known to me, that are associated with the name Colin J. Bennett, it was created by a bureaucratic organization for a set of administrative purposes, which, unfortunately in the case of the SSN, have become more and more expansive. It has no value to me, except under the circumstances when a U.S. public agency requires it as an identifier. It is patently not worth five dollars. It is not worth one dollar. It is not worth five cents.

Just because no monetary value can be attached to this information does not mean that I do not have a clear interest in how this number may be used or disclosed. There are many horror stories where out-of-date or inaccurate SSNs have shown up in databases and led to the unjust denial of rights and services. For instance, the SSN is used by credit reporting agencies in the United States. If my number were confused with that of a bad credit risk and appeared in the files of a credit reporting agency, I may very well be denied credit. The SSN is also used as an identifier in many computer-matching programs between agencies at different levels of government, including, of course, the Internal Revenue Service. Maybe it is used as the identifier on U of I alumni records. This information is not my property, but it does relate to me. And there are plenty of actual circumstances when the illegitimate processing of correct
information, or the legitimate processing of incorrect information, can have severe consequences for individuals.  

Here, then, we reach an important distinction between the realm of intellectual property law and that of privacy or data protection law. The former assumes a property ownership of information, the latter does not. In the first part of this paper, I try to chart the intellectual history of that category of statutory law that comes under the title “privacy protection” or, to use the European nomenclature, “data protection.” I then demonstrate how the formation and implementation of information privacy rules have become inescapably international issues and describe the various arenas in which these international rules have been negotiated. The global governance of privacy protection is now a complex phenomenon that involves a plurality of actors and a variety of modes of coordination and operation.

II. INFORMATION PRIVACY

The concept of informational privacy arose in the 1960s and 1970s at about the same time that “data protection” (derived from the German, Datenschutz) entered the vocabulary of European experts. The value was inextricably connected to the information processing capabilities of computers and to the need to build protective safeguards at a time when large national data integration projects were being contemplated in different European, North American, and Australian states. These projects raised the fears of an omniscient “big brother” government with unprecedented surveillance power. Experts in different countries then turned their attention to what should be done. Study commissions were established, such as in Britain, the United States, Canada, Sweden, Australia, and elsewhere. These analytical efforts led to the world’s first “data protection” or “information privacy” statutes, which have spread around the world in a number of stages.

Although concerns differed among these states, a closely-knit group of experts in different countries coalesced, shared ideas, and generated a general consensus about the best way to solve the problem. The overall policy goal in every country was to give individuals greater control of the information that is collected, stored, processed, and disseminated about them by public, and in some cases, private organizations. This goal was

4. See id. at 45-94.
5. Id.
6. Id.
7. Id.
prominent in English-speaking countries as well as in continental Europe. The concept of Informationsselbstbestimmung (informational self-determination) was later developed and given constitutional status in Germany. By the 1980s, it was possible to discern the set of key assumptions upon which information privacy policy development has since rested. Those assumptions are as follows.

First, it is believed that it is generally impossible to define a priori those data that are inherently worthy of greater protection (sensitive data) because it is the context rather than the properties of the data that lead to privacy risks. The same information can take on very different sensitivity levels in different contexts. My name in the telephone directory may be insensitive; my name on a list of bad credit risks or sex offenders may be very sensitive. My SSN on my U of I transcript may be insensitive, but on a list of tax cheats, sensitive. For the most part, therefore, law cannot delineate between those types of data that are worthy of protection and those that are not, even though some have tried. Public policy generally cannot draw a line between those types of information that should remain private and those that may be in the public domain.

Second, privacy is a highly subjective value. Concerns about the protection of personal information vary over time, legal jurisdiction, ethnic subgroups, gender, and so on. For instance, a name and address in a telephone directory may be insensitive for most people but may be very sensitive for vulnerable persons who do not want to be monitored and tracked down. Examples of such people would be battered wives, doctors who perform abortions, celebrities, child protection staff, police officers, and so on. Consequently, public policy cannot second-guess the kinds of personal information about which a given population will be concerned at a given time. The most privacy protection policy can achieve is to give individuals the procedural rights to control their personal information, should they be so motivated. Thus, the content of privacy rights and interests has to be subjectively defined by individuals themselves according to context. Information privacy policy is based inevitably therefore on procedural, rather than substantive, tenets. It can only put in place the mechanisms by which individuals can assert their own privacy interests and claims, if they so wish.

Third, there is common consensus that the focus of protection should be the individual, or the "natural person," rather than organizations, corporations, or other "legal persons." Some societies (in Scandinavia, for example) have attempted to embrace the rights of natural and legal persons in their data protection legislation. Essentially, however, the common consensus is that the goal of information privacy policy – to give individuals greater control over information relating to them – necessitates making a distinction between the subject of the information (the data subject) and the controller of that information (the
data controller). This distinction is by no means unambiguous; there are plenty of instances where an individual might wear both hats at any one time. Nevertheless, information privacy policy did develop (domestically and internationally) on the assumption that the interests in the information about groups, corporations, and other organizations can, and should, be dealt with through other legal instruments.

This finally leads us to the issue with which I began, whether personal information can be regarded as property over which individuals can be given property rights. Classic economic theorizing would contend that an imperfect marketplace can be rectified in one of two ways. First, one can give a value to personal information so that the costs and benefits of transactions are allocated more appropriately. But it is very difficult to establish personal information as property in law and then to define rights of action over its illegitimate processing. Consumers may have some bargaining power with a direct marketing firm that wants to trade lists; citizens, however, have no bargaining power when faced with a warrant or any other potentially privacy-invasive technique backed up by the sanctions of the state. At the outset of the privacy debate, it was the power of government agencies that posed the most significant challenges.

It was therefore hard to resist the conclusion that only regulatory intervention might redress the imbalance. Consequently, information privacy was generally defined as a problem for public policy rather than an issue for private choice. More recently, as critiques of the dominant approach have surfaced, the personal data processing practices of the private sector have arisen as equally significant concerns. Moreover, as Internet communications and e-commerce have risen to prominence, a variety of market-based solutions have been proposed, all of which have been based on the premise that personal information can be given a property value to be traded and exchanged within the personal information market. These kinds of arguments had, however, very little influence on the experts and legislators who grappled with the information privacy problem in the 1970s.

These assumptions would not be accepted by every scholar and commentator. They were, and are, deeply contested. The basic point at this juncture in the analysis is that privacy protection policy was placed on a particular trajectory as a result of some common assumptions about the nature of the information privacy problem. The policy responses that developed (data protection or information privacy statutes) for the most part were driven by a shared understanding among elites about the nature of the problem they were facing. Those shared assumptions, based on fundamental liberal principles, have had some profound and

widespread policy implications in every advanced industrial state. Assuming, then, that we each have information privacy rights, claims or interests, how can one frame a public policy to protect those rights?

III. THE FAIR INFORMATION PRACTICES DOCTRINE

Once these and other assumptions are accepted about how one can and cannot develop public policy on privacy, a logic is set in motion that leads inevitably to a basic set of procedural rights. Hence, a set of "fair information principles" ("FIPs") evolved that logically had to converge around a set of key and basic principles. The historical origins of fair information practices can be briefly traced to policy analysis in Europe and the United States in the late 1960s and early 1970s. Those experts who were attempting to resolve this issue in national arenas shared a strong desire to draw lessons from their counterparts overseas. This intense process of lesson-drawing produced an international consensus on how best to resolve the privacy problem through public policy.

While the codification of the principles may vary, they essentially boil down to a number of basic tenets. For example, an organization (public or private):

- must be accountable for all the personal information in its possession;
- should identify the purposes for which the information is processed at or before the time of collection;
- should only collect personal information with the knowledge and consent of the individual (except under specified circumstances);
- should limit the collection of personal information to that which is necessary for pursuing the identified purposes;
- should not use or disclose personal information for purposes other than those identified, except with the consent of the individual (the finality principle);
- should retain information only as long as necessary;
- should ensure that personal information is kept accurate, complete, and up-to-date;
- should protect personal information with appropriate security safeguards;
- should be open about its policies and practices and maintain no secret information system; and
- should allow data subjects access to their personal information with an ability to amend it as inaccurate, incomplete, or obsolete.\footnote{See generally Colin J. Bennett, Regulating Privacy 95-115 (1992) (describing policy convergence in Europe and the United States in the area of fair information practices).}

\footnote{Colin J. Bennett & Rebecca Grant, Introduction to Visions of Privacy: Policy Choices for the Digital Age, supra note 9, at 3, 6.}
These principles are, however, relative. However conceptualized, privacy is not an absolute right; it must be balanced against correlative rights and obligations to the community, although the concept of "balance" and the process of "balancing" are highly ambiguous.\(^\text{12}\)

The fair information principles appear either explicitly or implicitly within all national data protection laws, including those in the United States, Australia, New Zealand, and Canada that are called Privacy Acts. They appear in self-regulatory codes and standards, such as that published by the Canadian Standards Association which forms the basis of Canada's new private sector data protection law.\(^\text{13}\) Appendix One contains a comprehensive overview of the state of personal data protection legislation in 2001. It demonstrates how rapidly data protection law diffused around the advanced industrial world in the 1980s and 1990s, and how societies more commonly characterized as "developing" are now beginning to pass similar laws.

Despite this harmonization, there are, of course, continuing debates about how the FIPs doctrine should be translated into statutory language. For example, there are disputes about: (i) how to regulate the secondary uses of personal data — through a standard of relevance, or through specific provisions about legitimate custodians; (ii) the limitation on collection principle and to what extent the organization should be obliged to justify the relevance of the data for specific purposes; (iii) the circumstances under which "express" rather than "implied" consent should be required; and (iv) the distinctions between collection, use, and disclosure of information, and whether these distinctions indeed make sense and should not be subsumed under the overarching concept of "processing." How these and other statutory issues are dealt with will, of course, have profound implications for the implementation of privacy protection standards within any one jurisdiction.

The laws have also differed on the extent of organizational coverage — those in North America and Australia have historically mainly regulated public sector agencies, whereas those elsewhere (especially in Europe) encompass all organizations. This distinction is rapidly changing, however, as countries like Canada, Australia, and Japan have moved to regulate private sector practices. Laws have also differed on the extent to which they regulate non-computerized files (i.e., the manila folder in the filing cabinet). This distinction is also eroding.

\(^{12}\) Charles D. Raab, From Balancing to Steering: New Directions for Data Protection in VISIONS OF PRIVACY: POLICY CHOICES FOR THE DIGITAL AGE, supra note 9, at 68, 69-73.

Most notably, they have differed with regard to the policy instruments established for oversight and regulation. Most countries, with the notable exception of the United States, have set up small privacy or data protection agencies with varying oversight, advisory, or regulatory powers. Some of these agencies have strong enforcement and regulatory powers; others act as more advisory "ombudsman-like" bodies. Some are headed by a collective commission (such as in France), others by a single "Privacy Commissioner" or "Data Protection Commissioner." In some regulatory regimes, instruments of "self-regulation" (such as company codes of practice) play a more important role than in others.

Finally, it can be noted that this deep and extending consensus surrounding the FIPs doctrine has occurred against a backdrop of profound skepticism as to whether it can actually protect personal privacy and stem the inexorable tide of surveillance. Authors who have examined the issue from a broader sociological perspective have continuously raised the concern that contemporary information privacy legislation is designed to manage rather than limit the processing of personal data. David Lyon has contended that "[t]he concept of privacy is inadequate to cover what is at stake in the debate over contemporary surveillance." From the perspective of those interested in understanding and curtailing excessive surveillance, the formulation of the privacy problem in terms of trying to strike the right "balance" between privacy and organizational demands for personal information hardly addresses the deeper issue. Information privacy policies may produce a fairer and more efficient use and management of personal data, but they cannot control the voracious and inherent appetite of modern organizations for more and more increasingly refined personal information. And this information is increasingly extracted through intrusive biometric technologies that are altering the very boundaries between the self and the outside world.

Despite these differences, quite early in the debates it was recognized that information privacy could not simply be regarded as a domestic policy problem. The increasing ease with which personal data might be transmitted outside the borders of the country of origin has produced an interesting history of international harmonization efforts and a concomitant effort to regulate transborder data flows. In the 1980s, these harmonization efforts were reflected in two international agreements, the 1981 Guidelines from the Organization for Economic Cooperation and Development and the 1981 Convention from the Council of Europe. In the 1990s, these efforts were extended through the 1995 Directive on Data Protection from the European Union, which tries to

---

harmonize European data protection law according to a higher standard of protection and to impose that standard on any country within which personal data on European citizens might be processed. These provisions, above all, have dictated the content of the world’s data protection law.  

IV. THE INTERNATIONAL REGIMES FOR PRIVACY PROTECTION POLICY

A. The Council of Europe

The institutions of the Council of Europe first became interested in privacy and data protection in the late 1960s, when a Committee of Experts was established to advise on how best to protect privacy in the face of modern computing advances. Two resolutions in the 1970s led to the preparation of the Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data (Treaty 108), which was duly adopted in 1980 and opened for ratification in January 1981. European Conventions and Agreements are not statutory acts of the organization; they owe their legal existence simply to the will of those states that may become parties thereto, through their signature and ratification of the treaty. Ratification signifies that the principles of the Convention have been incorporated into domestic law and that, theoretically at any rate, the citizen of one ratifying country can seek redress in another for the mistreatment of his or her personal information. As of December 2001, thirty-three of the Council’s forty-one members had signed the Convention, and twenty-five had ratified it.

The Convention set out for the first time in an international legal text the basic information privacy principles outlined above. In this respect, the Convention has acted as a template for those countries without data protection legislation. However, the Council of Europe possesses no supranational legal structure to ensure that the principles are enforced in practice. It cannot, therefore, be assumed that ratification of the Convention signifies the actual implementation of a common minimum standard of data protection. Moreover, although the Convention seeks to establish an equivalent level of protection among contracting parties and, therefore, to assure the free movement of such data among those parties, the question of data transfers to non-contracting states is left up to national law. This means that the ratifiers’ mutual confidence in one another as safe destinations for personal data is undermined.

As an instrument to regulate the international flow of personal data, therefore, the Convention has been limited and has since been

16. BENNET & RAAB, supra note 1.
17. FRITS W. HONDIOUS, EMERGING DATA PROTECTION IN EUROPE 65 (1975).
superseded by the 1995 European Data Protection Directive, discussed below. This does not mean that the Convention has become redundant; it still serves as a model for newly democratizing states, and it was invoked as an underpinning document for protecting personal data within European inter-state arrangements such as Europol. Also pursuant to the Convention, the Council has adopted a number of influential recommendations, as a wide range of governmental, social and economic practices and technologies, including the Internet, have been developed and applied. The Council has also developed a Model Contract, outlining the obligations of both licensor and licensee, to ensure equivalent data protection in the context of international data flows.

B. The Organisation for Economic Co-operation and Development

It was within the Organisation for Economic Co-operation and Development ("OECD") arena in the late 1970s that the world witnessed the first transatlantic conflicts over privacy protection policy. To many Europeans, the American espousal of the principle that information flows should rarely be impeded was a veiled attempt to protect U.S. hegemony in the global marketplace. Some Americans, on the other hand, saw ulterior trade-protectionist motivations behind the data protection label. The negotiation of the Guidelines on the Protection of Personal Privacy and Transborder Flows of Personal Data was, therefore, difficult and contentious.

The Guidelines were based on a number of assumptions, stated in the Preface:

that, although national laws and policies may differ, Member countries have a common interest in protecting privacy and individual liberties, and in reconciling fundamental but competing values such as privacy and the free flow of information;
that automatic processing and transborder flows of personal data create new forms of relationships among countries and require the development of compatible rules and practices;
that transborder flows of personal data contribute to economic and social development;
that domestic legislation concerning privacy protection and transborder flows of personal data may hinder such transborder flows.

20. BENNETT, supra note 10, at 137.
Covering personal data in the public and private sectors, these Guidelines were thus intended to help harmonize national privacy legislation and provide a framework for facilitating international flows of data. They represented an important consensus on eight basic principles: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability.

On the issue of transborder data flows, Section 17 states that:
A Member country should refrain from restricting transborder flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A Member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other Member country provides no equivalent protection. 22

However,
Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection. 23

Efforts were also made to avoid unnecessary divergences between the OECD and Council of Europe agreements. However, there are some important differences that are worth noting. First, the Guidelines are explicitly voluntary: there is no penalty imposed for non-adoption, either by a country or an organization, and no penalty for non-compliance once adopted. In contrast, the Convention is legally binding, at least for those countries that have ratified it, although countries can meet the general requirements by adopting enforcement and oversight methods appropriate to their political, administrative, and legal systems. Second, the Convention applies solely to automated data processing, whereas the Guidelines apply to personal data regardless of the processing medium.

By the beginning of the 1980s, these two international instruments were used as models for national legislation in Europe and for voluntary codes of practice outside. The American and Canadian governments both tried to monitor the extent to which the OECD Guidelines were adopted within their respective societies, without any clear indication of what “adoption” entailed, nor any serious commitment. 24 By the 1990s, however, attention shifted to the question of computer security and the

22. Id. at pt. 3, § 17.
23. Id. at pt. 3, § 18.
negotiation of a set of guidelines on the Security of Information Systems. These guidelines were intended to provide the required framework for the protection of the availability, integrity, and confidentiality of information systems and were updated in 2001. The third element in the OECD's package is the Guidelines for Cryptography Policy published on 27 March 1997, following several years of heated international controversy concerning the export of cryptographic products for civilian use. This non-binding agreement identifies the basic issues countries should consider in drawing up cryptography policies at the national and international level.

Each of these elements (privacy, security, cryptography) converged in the mid-1990s when the subject of electronic commerce surfaced as an OECD priority, causing shifts in OECD rhetoric and policy. First, the discourse tends to reflect the more interactive, dynamic, and networked nature of contemporary data transmissions. Second, in keeping with what has become a widespread consensus, the concentration on legislation in the 1970s and 1980s has now given way to recognition of a multiplicity of solutions needed in addition to law, including self-regulation, privacy-enhancing technologies, contractual approaches, and consumer education. Finally, privacy protection is advanced not as a barrier to international communications and trade, but as a necessary condition without which individuals will avoid the use of public networks for commercial transactions.

C. The European Union Arena

By the late 1980s, it became readily apparent that there was no rush to ratify Treaty 108, and there remained significant legal differences among the legislation of those that had ratified. The OECD Guidelines served more as a means to justify self-regulatory approaches than as a guide to promote sound data protection practices throughout the advanced industrial world. At the same time, it was becoming increasingly clear that discrepancies in data protection could impede the free flow of personal information throughout the EU and obstruct the creation of the Internal Market scheduled for completion by 1992. Data protection had ceased to be merely a human rights issue; now it was also intrinsically linked to the operation of international trade.

---

25. Guidelines, supra note 19.
The EU response to the emerging issues was by far the most influential international policy instrument to date: the Directive on the Protection of Personal Data with Regard to the Processing of Personal Data and on the Free Movement of Such Data (EU, 1995). This Directive emerged after five years of drafting and redrafting as the document passed through the complicated and lengthy EU decision-making process. The substance of the Directive can be understood as the reflection of negotiated bargains among a range of public and private sector stakeholders.

The Directive aims to ensure a high level of protection for the privacy of individuals in all Member States and also to ensure the free flow of information throughout the Single Market by fostering consumer confidence and minimizing differences between the Member States' rules. The reader is initially confronted with a series of recitals in the form of seventy-one "whereas" statements that state intentions that place this Directive in the context of other values and policies that help with interpretation and reflect the variety of interests that shape its content. The familiar set of fair information principles, around which previous national laws and international agreements have converged, do not appear in one easily accessible place. The principles of consent, access, notification, security, etc. are reflected in particular Articles, but the document is very much a legal text whose main purpose is to give guidance to drafters of national data protection legislation.

Despite the complexity, the Directive has jettisoned certain artificial and outdated concepts. For instance, there is now little distinction between public and private sector data processing; earlier drafts differentiated between the sectors in regard to the fair obtaining and legitimacy of processing of personal data. Some antecedent laws only cover "automated" data processing, whereas the Directive applies to "any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis." The Directive also attempts to avoid artificial distinctions between information collection, use, and disclosure, preferring to define "processing" as embracing all these phases as well as other operations. Like Treaty 108, however, the Directive does include specific provisions for "sensitive" forms of data.

---


29. Very briefly, the process consisted of: (1) the initiation of a draft proposal by the Commission of the European Communities (17 members appointed by the governments of the member states); (2) commentary on the draft by the European Parliament (518 members elected from member states) and by parliamentary committees; (3) revision by the Commission in the light of comments; (4) negotiation of a "common position" within the Council of Ministers (the executive body consisting of one member from each of the 12 member states with weighted votes); (5) final approval by the EU Parliament; and (6) publication.

30. EU Data Protection Directive, supra note 28, at art. 2(c).
Unlike the Convention, the Directive specifies the nature and function of a Member State's "supervisory authority." Each country must provide one or more public authorities responsible for monitoring the application, within its territory, of the national provisions adopted pursuant to the Directive. These authorities must act with complete independence and must be endowed with enumerated powers: effective powers of intervention (especially *before* processing operations begin); powers to engage in legal proceedings; and powers to hear claims concerning the protection of rights, freedoms, and the lawfulness of data processing under the Directive. In addition, Member States should provide that supervisory authorities are consulted when administrative measures with privacy implications are being developed. In total, these provisions endow a greater range of power and responsibility than many prior European data protection regimes.

Articles 29 and 30 of the Directive establish an advisory Working Party composed of representatives from the supervisory authorities in each Member State, joined by representatives of the European Commission and of other Community institutions. The Working Party is expected to give the Commission advice on: (i) divergent national laws; (ii) the level of protection in third countries; (iii) codes of conduct; and (iv) proposed amendments to the Directive. Executive decision-making power over the Directive is granted to a body simply called "The Committee," comprised of representatives from the Member States and chaired by someone from the Commission. This is a mechanism by which the Commission can adopt decisions and regulations pursuant to the Directive, in particular the determination of the adequacy of protection within non-EU third countries.

For some countries outside the EU, the extra-territorial implications of the Directive have caused considerable anxiety. Article 25 stipulates "Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if ... the third country in question ensures an adequate level of protection." The adequacy of protection shall be assessed "in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations." Particular consideration is to be given to the nature and purpose of the data and the "rules of law, both general and sectoral" and the "professional rules and security measures which are complied with." Article 26 lists a number of derogations from this provision.

31. *Id.* at art. 28(1).
32. *Id.* at art. 31.
33. *Id.* at art. 25(1).
34. *Id.* at art. 25(2).
35. *Id.*
Where the Commission decides that a third country does not ensure adequate protection, Member States should “take the measures necessary to prevent any transfer of data of the same type to the third country in question.”36 Then the Commission “shall enter into negotiations with a view to remedying the situation.”37 Thus, if the Commission finds an inadequate level of protection, Member States are mandated, rather than simply permitted, to prohibit the transfer. This represents a stronger approach than embodied within either the OECD Guidelines or the Council of Europe Convention. Even though both these instruments contain a principle of equivalence (arguably stronger than adequate), neither of these instruments require signatories to block the transfer of data to countries that cannot ensure an equivalent level of protection.

Subsequent to the passage of the Directive, the Article 29 Working Party issued a series of policy statements designed to clarify how Articles 25 and 26 of the Directive would be interpreted. “Adequate protection” requires both content and enforcement. The content principles should include: purpose limitation, data quality and proportionality, transparency, security, rights of access, rectification and opposition, and restrictions on onward transfers to further third countries. Rather than specifying certain structural requirements, however, the Working Group detailed the essential functions that a data protection system should perform:

(1) to deliver a good level of compliance with the rules. (No system can guarantee 100% compliance, but some are better than others). A good system is generally characterised by a high degree of awareness among data controllers of their obligations, and among data subjects of their rights and the means of exercising them. The existence of effective and dissuasive sanctions is important in ensuring respect for rules, as of course are systems of direct verification by authorities, auditors, or independent data protection officials.

(2) to provide support and help to individual data subjects in the exercise of their rights. The individual must be able to enforce his/her rights rapidly and effectively, and without prohibitive cost. To do so there must be some sort of institutional mechanism allowing independent investigation of complaints.

(3) to provide appropriate redress to the injured party where rules are not complied with. This is a key element which must involve a system of independent arbitration which allows compensation to be paid and sanctions imposed where appropriate.38

---

36. Id. at art. 25(4).
37. Id. at art. 25(5).
38. Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, First Orientations on Transfers of Personal Data to Third Countries – Possible Ways Forward in
Throughout this process, the standard of data protection within the United States posed the most difficult dilemmas. If the United States were found to meet the “adequacy” test under the Directive, despite the fact that many areas of the American economy are not obliged to maintain data protection standards, then the credibility of the EU Directive would be undermined. If, on the other hand, the Directive were enforced to the letter, then the broad bans on data flow would seriously disrupt international trade and travel and would almost certainly lead to a transatlantic trade dispute. In recognition of this dilemma, a high-level dialogue between John Mogg, then Director-General of DG XV, and U.S. Under-Secretary for Commerce, David Aaron, resulted in the Safe Harbor Agreement. The intent of this Agreement is to bind those companies that subscribe to Safe Harbor to a set of privacy principles overseen and enforced by the Federal Trade Commission. As of December 2001, some 148 U.S. companies had committed themselves to the privacy principles of the Safe Harbor Agreement, breach of which would open these companies to challenge under the Federal Trade Commission’s power to regulate “unfair and deceptive” trade practices.\footnote{Assessing Adequacy 7 (June 1997), at http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp4en.pdf.}

Apart from the Safe Harbor proposal, a number of concerns remain about the implementation of Articles 25 and 26, and indeed about the Directive as a whole.\footnote{International Trade Administration Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45666-01 (Jul. 24, 2000). See also 65 Fed. Reg. 56534-01 (Sept. 19, 2000) (correcting final documents published on July 24, 2000).} The Directive provides for the Commission (with the Article 31 Committee’s approval) to set an EU-wide standard for acceptance of transfers to specific third countries. But there is at least the danger that judgments about adequacy will be susceptible to the vagaries of the European policy process and are likely to be enmeshed with the resolution of issues unrelated to information privacy. Log-rolling, therefore, may override the more predictable and rational pursuit of a data protection standard. Another lingering concern is that neither the supervisory authority nor the data controller has the capacity to scrutinize the processing of personal data in another jurisdiction, nor can they be fully satisfied that data subjects can exercise their privacy rights. The Directive does not avoid the central dilemma inherent in former attempts to regulate international data transmissions by the Convention or through model contracts. In the absence of an audit mechanism that ensures that personal data are \emph{actually} processed fairly and legally in a third country, judgments about adequacy will probably continue to be

\footnote{Opinions about the current operation of the Directive were aired at a large conference in Brussels in October 2002. See Brussels Conference Debates Changes to EU Data Protection Laws, Privacy Laws and Business, Nov. 2002.}
made in a non-empirical way, according to the analysis of the "black letter of the law" or other formal indicators.\textsuperscript{41}

These same concerns about the extra-territorial compliance with European law are surfacing with respect to a new Directive passed in July 2002 on "privacy and electronic communications."\textsuperscript{42} This replaces an early telecommunications privacy directive and establishes a range of new rules concerning the privacy of communications on the Internet. Particularly controversial are those provisions concerning the retention of "traffic data," the processing of "location data," and the control of unsolicited communications, especially "spam" e-mail. This Directive should be transposed into the national laws of the Member States by October 2003.

\textbf{D. The International Standards Arena}

The perceived gap in the enforcement process for data protection has led some to contend that the data protection question should be taken up by the world's standards-setting and certification bodies, institutions with many years of experience of observing and measuring levels of compliance with various international norms. Information security standards have played a peripheral but important role in privacy protection for some years. In the 1990s, however, the idea of a more general management standard for the complete set of privacy principles emerged onto the international agenda. In large measure, the idea has stemmed from the negotiation in Canada of the Model Code for the Protection of Personal Information under the auspices of the Canadian Standards Association.\textsuperscript{43} The publication of this standard prompted a series of attempts to produce a similar instrument at the international level, with the idea that privacy protection could be regarded as an element of quality management, similar to that of the ISO 9000 series of quality management standards.

The process first began within the institutions of the International Organization for Standardization (ISO). The expected resolution, however, did not materialize, mainly as a result of some very intensive lobbying by certain U.S. multinational business interests. From there, the idea migrated to European standards bodies. The Comité Européen de Normalisation ("CEN"), responsible for the negotiation of standards within Europe, began to study the feasibility of an international privacy

\textsuperscript{41} Charles D. Raab, et al., Application of a Methodology Designed to Assess the Adequacy of the Level of Protection of Individuals with Regard to Processing Personal Data: Test of the Method on Several Categories of Transfer, European Commission Tender No. XV/97/18/D at 127-99 (Sept. 1998), available at http://europa.eu.int/com/internal_market/privacy/docs/studies/adequat_en.pdf.


\textsuperscript{43} CSA 1996, supra note 13.
standard, supported by the Article 29 Working Party.\textsuperscript{44} At an open seminar in Brussels in March 2000, it was proposed to begin standardization activities along three paths: a general data protection standard which would set out practical operational steps to be taken by an organization in order to comply with relevant data protection legislation, principally the EU Directive; a series of sector-specific initiatives in key areas such as health information and human resources management; and task-specific initiatives mainly related to the online environment. A formal resolution gave three standards bodies (CEN, CENELEC, and ETSI) a mandate to study the potential for further standardization work in support of the European Directive. From there, the reins were taken up under the auspices of the Initiative on Privacy Standardization in Europe ("IPSE").\textsuperscript{45}

Proponents contend that an international standard would attract attention and international certification efforts from different national standards bodies. It would give businesses outside Europe a more reliable and consistent method by which to demonstrate their conformity to international data protection standards. It would also provide a more reliable mechanism for the implementation of Article 25 of the Directive. As mentioned earlier, the scrutiny of laws and contracts provides no assurances to European data protection agencies that data protection rules are complied with in the receiving jurisdiction. Required registration to a standard, which would obliged independent and regular auditing, would provide a greater certainty that adequate data protection is being practiced by the receiving organization, wherever it is located. This requires, of course, require concomitant efforts to harmonize systems of conformity assessment and auditor certification. At the end of the day, bilateral and multilateral mutual recognition agreements would also have to be negotiated to ensure that domestic conformity assessment programs are commonly respected. These initiatives have, however, been met with very high levels of resistance from businesses in information-intensive sectors.\textsuperscript{46} At the time of writing, it is by no means clear that personal data protection will have a permanent place within standards-setting and certification bodies.


V. CONCLUSION: PRIVACY PROTECTION AND WORLD TRADE

I began this essay with an anecdote designed to point out the differences between privacy and intellectual property. I have argued that privacy protection is now a distinct policy sector characterized by an increasing number of statutory laws and overseen by an increasingly institutionalized network of privacy and data protection authorities. In addition, there are international networks of corporate privacy officers and privacy advocates. And a variety of small businesses offer privacy-enhancing technologies for the concerned consumer. A lot of people, in many countries, have a stake in the continued presence of privacy protection on national and international agendas. In one respect, however, the issues of privacy protection and intellectual property are converging. Privacy protection, like intellectual property protection, has became a trade-related question. Sooner or later, therefore, it is likely that it will be injected into the wider panoply of issues negotiated and arbitrated within the World Trade Organization ("WTO"). It is fitting, therefore, to conclude this article with some speculation about how data protection might relate to the wider politics of international trade.

From the outset of the European data protection movement in the 1970s, American commentators have been concerned that the extraterritorial provisions within these laws could be used as a non-tariff trade barrier to protect what was considered the less-developed and less-innovative information technology industries within Europe. As the harmonization efforts of the Council of Europe, the OECD, and the European Union have progressed, and as data protection has become of central importance to international electronic commerce, so rhetoric about European motives has been ratcheted up. Regardless of European motives, which are obviously diverse and complex, the very prospect that the EU Directive might have the effect of protecting European business interests against American competition raises a series of fascinating questions about whether or not these European regulations violate the existing rules of the world trading system. Swine and Litan\(^\text{47}\) argue that, at the very least, European data protection law will force U.S. businesses that wish to operate within Europe to comply with those rules and to be constrained in the ways in which they use personal information. They also maintain that European firms would be more inclined to contract with domestic information processing companies with whom they can freely exchange personal data under the umbrella protection of the Directive.

Any action by the United States, or any other non-European state against the trade-protectionist effects of data protection law would most likely be covered by the General Agreement on Trade in Services

under which states make market access commitments for various sectors and activities. If a personal data transfer is covered under one of these commitments, then the European Union is obliged to treat U.S. companies no less favorably than European ones. According to Article VI of GATS: "In sectors where specific commitments are undertaken, each Member shall ensure that all measures of general application affecting trade in services are administered in a reasonable, objective and impartial manner." Any challenge to the operation of the Directive would then hinge on the meaning of the word "reasonable." In addition, and perhaps more importantly, any ban on data transfers under the provisions in Articles 25 and 26 of the Directive must be applied in an even-handed manner. Thus, if the European Union were to ban data exports to one country, but not to another with equally inadequate data protection, then it could fall foul of the "most favored nations" clause of the GATS, Article II of which states: "[w]ith respect to any measure covered by this Agreement, each Member shall accord immediately and unconditionally to services and service suppliers of any other Member treatment no less favorable than that it accords to like services and service suppliers of any other country."

The requirement for impartiality explains the careful attempts by the Directive's Article 29 and 31 Committees to develop a clear methodology for the assessment of adequacy, as well as their attempts to gain a more comprehensive and empirical understanding of aspects of data protection in third-world countries. Moreover, both committees adopted formal commitments to non-discrimination in 2000. Citing provisions from the European Convention on Human Rights, the Article 31 Committee affirmed its commitment to the principle of non-discrimination and to the "general principle of equality, of which the prohibition of discrimination on grounds of nationality is a specific enunciation, is one of the fundamental principles of Community law." It also went on to explain that it is "important to be able to judge different situations on their merits and not to regard the equal treatment principle as imposing a single model on third-world countries."

49. Id. at 289.
51. GATS, supra note 48, at 286. 
54. Id.
and flexible methods for assessing adequacy can be applied in an even-handed manner.

Notwithstanding these difficulties, Shaffer has concluded that any third-world country attempt to challenge EU data protection rules before the WTO would probably not succeed for three reasons. First, it can be argued that any ban on data transfers would harm EU-owned and registered companies as much as it would those companies outside the European Union.\textsuperscript{55} Second, the European Union's action is directed toward a legitimate public policy objective that is explicitly mentioned in the GATS as a general exception:

Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services, nothing in this Agreement shall be construed to prevent the adoption or enforcement by any Member of measures ... necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to ... the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts.\textsuperscript{56}

Third, he contends that any WTO dispute settlement panel would be reluctant to rule on the substantive policy interests, but would prefer to focus instead on procedural questions. This deference is, Shaffer argues, supported by recent WTO jurisprudence.\textsuperscript{57}

We have no way of judging whether these predictions are correct. It is probable, however, that at some point, and in some context, international data protection rules will be tested within the WTO. Much prior analysis has understandably considered these scenarios in the context of an American challenge to European rules. But we should bear in mind that transborder data flow provisions appear in most national laws. Potential disputes could arise between any number of trading partners in almost any area of the world.\textsuperscript{58} For this reason, the complicated and, for data protection experts, somewhat unfamiliar world of international trade policy will probably arise as a significant arena in which data protection rules are negotiated in the future.

\textsuperscript{55} Shaffer, \textit{supra} note 50, at 17.
\textsuperscript{56} GATS, \textit{supra} note 48, at 294-95.
\textsuperscript{57} Specifically, the "Shrimp-Turtle Case," which involved a U.S. ban on foreign shrimp imports due to a U.S. finding of inadequate sea turtle conservation policies in South East Asia.
\textsuperscript{58} It is worth noting that, even before the Directive came into force, the Spanish authorities in 1999 fined Microsoft almost $60,000 for breaching Spanish data protection controls by improperly collecting data from its European employees on a U.S. Web site.
THE DIFFUSION OF INFORMATION PRIVACY LEGISLATION
BY REGION

<table>
<thead>
<tr>
<th>Region</th>
<th>1970s</th>
<th>1980s</th>
<th>1990s</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Luxembourg (1978)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>E. Europe</strong></td>
<td></td>
<td></td>
<td>Slovenia (1990)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Hungary (1992)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Czech. (1992)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Estonia (1996)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Lithuania (1996)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Poland (1997)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Slovakia (1998)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Latvia (2000)</td>
</tr>
<tr>
<td><strong>S. America</strong></td>
<td></td>
<td></td>
<td>Chile (1999)</td>
</tr>
<tr>
<td><strong>Australasia</strong></td>
<td>New Zealand (1982)</td>
<td></td>
<td>South Korea (1994)</td>
</tr>
<tr>
<td><strong>East Asia</strong></td>
<td></td>
<td>Japan (1988)</td>
<td>Taiwan (1995)</td>
</tr>
</tbody>
</table>

59. This table establishes the first date that information privacy legislation was enacted in each country either for the public sector, or for both private and public sectors. It does not incorporate legislative actions at the sub-national levels. It does not include FOI (access to information) laws. It does not include legislation that only regulates private sector enterprises. It does not include subsequent amendments.