Volume 6, Spring Issue, 1993

RULES OF THE ROAD FOR GLOBAL ELECTRONIC HIGHWAYS: MERGING THE TRADE AND TECHNICAL PARADIGMS

*Joel R. Reidenberg**

INTRODUCTION

This symposium on the legal problems and implications of new communications technologies comes at a particularly timely juncture. Instant access to data in remote locations has become a central factor in the growth of transnational business.[1] Telecommunications gateways allow the connection of information networks and information sources across both national and sectoral borders.[2]

Against the background of seamless global networks, North America is pushing toward a continent-wide zone for information exchange, the European Community is striving to manage cross-border information flows, and leaders in the United States are beginning to debate a high-speed, national data network.[3] Even Eastern European nations are

---

* Associate Professor, Fordham University School of Law. A.B., 1983, Dartmouth College; J.D., 1986, Columbia Law School; D.E.A. dr. int'l éco., 1987, Université de Paris I (Panthéon-Sorbonne). The author gratefully acknowledges research support provided under a grant from the Fordham University School of Law and thanks Professors Paul Schwartz and Spiros Simitis for their helpful comments on an earlier draft of this paper.

1. *See, e.g.*, KARL SAUVANT, INTERNATIONAL TRANSACTIONS IN SERVICES: THE POLITICS OF TRANSBORDER DATA FLOWS (1986); TRANSBORDER DATA FLOWS (Hans-Peter Gassmann ed., 1983) (proceedings of OECD conference held in December 1983); Joel R. Reidenberg, *The Privacy Obstacle Course: Hurdling Barriers to Transnational Financial Services*, 60 FORDHAM L. REVIEW S137 (1992); René Laperrière et al., *The Transborder Flow of Personal Data from Canada: International and Comparative Law Issues*, 32 JURIMETRICS J. 547 (1992).

2. *See, e.g.*, Patrick J. Leahy, *New Laws for New Technologies: Current Issues Facing the Subcommittee on Technology and the Law*, 5 HARV. J.L. & TECH., Spring 1992, at 1 (describing the Internet and its linkage of a multitude of local networks and information sources).

3. *See* John Markoff, *Building the Electronic Superhighway*, N.Y. TIMES, Jan. 24, 1993, §3, at 1 (describing the debate over the creation of a national fiber optic network); Preamble, Amended Proposal for a Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, COM(92)422 final—SYN 287 [hereinafter Amended Proposal] (noting the need for intra-European information flows); Proposed North American Free Trade Agreement § 1302(5) (1992) (exempting security and privacy laws from prohibitions on regulatory barriers to information flows within North America).

grappling with "informatization."[4] Already, global information networks have changed both the way business is done and have altered the nature of national markets.[5]

As we create new electronic "highway" systems, flows of information and access to global information networks depend increasingly on emerging fair information practice rules and, specifically, the treatment of personal information or information about individuals. Regulation of information practices will determine the availability of data and the possibilities for interconnection of networks. Standards of fair information practice around the world are as critical to electronic highways as traffic lights and speed limits are to asphalt roadways. They establish the new rules of the road for information systems.

International efforts to define fair information practices[6] for global networks derive from two distinct paradigms. Traditionally, regulatory standards have been cast in trade terms. The trade perspective seeks to promote free flows of information and define standards that balance free flows against human rights values. Fair information practices also draw on another rarely emphasized technical paradigm. This approach seeks to eliminate any technological obstacles to free flows of information by defining standards for system integrity and interoperability. Nevertheless, these technical standards are set in ways that also define fair information practices.

While each paradigm provides a basis to establish rules for global electronic highways, the two are surprisingly self-contained and tend not to fit within the broader trends in global information networks and practices. Instead of facilitating the definition of fair information practice standards, the distinct trade and technical perspectives obscure the tendency of global networks to shift norms for the regulation of private sector actors into a combined arena of both national and network jurisdiction. Global information networks challenge regulatory and

---

4. *See, e.g.*, *Data Protection Round-up*, PRIVACY L. & BUS., Oct. 1992, at 25-28 (Hungary, the former Czechoslovakia, and Poland have each become concerned with fair information practices); ABA CENTRAL AND EAST EUROPEAN LAW INITIATIVE, ANALYSIS OF BULGARIA'S DRAFT INFORMATION LAW (1992) (Bulgaria is contemplating legislation on information practices).

5. *See* PROJECT PROMETHEE, NETWORKS & MARKETS: MORE THAN A MARRIAGE OF CONVENIENCE (1992).

6. This Article focuses only on personal information and fair information practices in the context of the private sector.

political assumptions and defy simple regulation of fair information practice. These independent approaches to the establishment of fair information practice rules suggest that international data flows require complex standards, including overlapping regulation, rather than isolated one-dimensional rules.

I. THE TRADE PARADIGM: BALANCING FREE FLOWS OF INFORMATION AND HUMAN RIGHTS

The conventional view of fair information practice standards uses a trade paradigm. Rules for data processing must resolve an inherent tension between the desire for free flows of information and the concern over human rights. Under the trade theory, economic progress and trade competitiveness depend on free flows of information across borders.[7] However, Rolv Ryssdal, President of the European Court of Human Rights, recently noted that "activities in the field of data protection are firmly rooted in fundamental rights and freedoms."[8] The rights of privacy and "information self-determination"[9] conflict with the trade value of free flow. Information self-determination gives control over the flow of personal information to individuals and thereby limits free flows. Free flow gives control of information to private actors and thus limits an individual's power of decision. By viewing fair information practices in trade terms, regulatory efforts attempt to create a balance between the

---

7. *See* Organization for Economic Cooperation and Development, *Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, OECD Doc. C(80)58 final, *reprinted in* 20 I.L.M. 422 [hereinafter OECD Guidelines]; Council of Europe, Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, Europ. T.S. No. 108, *reprinted in* 20 I.L.M. 317 [hereinafter European Convention]; Amended Proposal, *supra* note 3, Preamble ¶¶ 1-6.

8. Rolv Ryssdal, Data Protection and the European Convention on Human Rights, XIII CONF. DATA PROTECTION COMM'RS 39 (1991) (transcript available from the Council of Europe) [hereinafter Proceedings].

9. The term "information self-determination" was coined by a German constitutional court in a suit challenging attempts by the state to gather personal information for the census. *See* Judgment of the First Senate (Karlsruhe, Dec. 15, 1983), *translated in* 5 HUM. RTS. L.J. 94 (1984). For a comparative analysis of this important decision, see Paul Schwartz, *The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination*, 37 AM. J. COMP. L. 675 (1989).

two competing sets of values. This perspective presents an inherently unstable balance. Global information networks and markets change the context of information practices on a continual basis. These dynamic circumstances for international data flows defy a satisfactory definition of fair information practices on a generic or momentary basis. Generic omnibus rights will be difficult to apply in specific circumstances and contextual applications will become anachronistic with technical advances.

A. Toward a Broad Balancing

During the 1970s, European countries began to enact broad data protection laws to formulate the balance for the early phase of computerization. These laws specified general principles of fair information practice and authorized national regulators to prohibit the export of personal information to countries that lacked sufficient privacy protection.[10]

Because fair information practice standards existed only through narrowly-targeted regulation in the United States,[11] the American business community warned that these European rules were protectionist and would threaten trade relations.[12] The complaints emphasized that any balance should be more tilted toward free flows of information. The specter of an electronic short-circuit began to loom for international data flows to the United States as well as other countries. In fact, during the late 1980s, some restrictions on international data transfers were imposed by European national authorities. France, for example, restricted data flows to Italy and Belgium, and the United Kingdom banned the transfer of direct marketing lists to the United States.[13] More recently, the

---

10. *See* Reidenberg, *supra* note 1, at S160-65.

11. *See* Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?*, 44 FED. COMM. L.J. 195 (1992).

12. *See* John M. Eger, *Emerging Restrictions on Transnational Data Flow: Privacy Protection or Non-Tariff Trade Barriers?*, 10 LAW & POL'Y INT'L BUS. 1055 (1978); Robert Bigelow, *Transborder Data Flow Barriers*, 20 JURIMETRICS J. 8 (1979); *International Data Flow: Hearings Before Subcomm. on Gov't Information of the House Comm. on Gov't Operations*, 96th Cong., 2d Sess. 1 (1980).

13. *See* Délibération No. 89-78 du 11 juillet 1989, *reprinted in* Commission nationale de l'informatique [C.N.I.L.], 10e Rapport, at 32-34 (1989) (restriction on electronic transmission of personnel records from France to Italy); Délibération No. 89-98 du 26 sept. 1989, *reprinted in* C.N.I.L., 10e Rapport d'activité, at 35-37 (1989) (restriction on the transfer of health records from France to Belgium); U.K. OFFICE OF THE DATA PROTEC-

European Community has shown interest in scrutinizing transborder data flows.[14]

Even within the European Community, there was growing concern about balancing values for cross-border data flows. Businessmen worried that differences in standards for fair information practice would be harmful to economic relations between the member states, and human rights activists were concerned that some countries lacked any standards. Countries with data protection legislation, such as France, were critical of potential "data havens" where privacy laws were seen as lax or non-existent.[15] By 1984, the United Kingdom feared that it would become isolated from its European information partners and adopted a data protection law despite years of seemingly endless discussion.[16] Even non-member countries such as Switzerland were motivated to enact data protection legislation.[17] By 1990, the concerns in the European Community over the trade distorting effects of divergent standards for fair information practices reached a critical stage. The Commission began the formal process of developing common rules.[18]

Also beginning in the 1970s, the predominant multilateral efforts to define fair information practices centered on the trade terms. The Organization for Economic Cooperation and Development ("OECD") and the Council of Europe each worked to establish a set of principles that balanced the two sets of interests: free flows of information and human rights.[19] With the enactment of various national laws in Europe, the American computer sector became alarmed at the prospect of government-imposed restrictions on the flow of data from Europe to the United

---

TION REGISTRAR, SEVENTH ANNUAL REPORT 33-34 (1990) (ban on the transfer of mailing lists from the United Kingdom to the United States).

14. In 1990, the Commission proposed a directive for fair information practice standards that contained a restrictive provision on international data flows outside the European Community. *See* Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data, COM(90)314 final—SYN 287 [hereinafter Proposed Directive]. The revised draft continues the scrutiny of international data flows. *See* Amended Proposal, *supra* note 3, art. 26; *see also infra* notes 23-28 and accompanying text.

15. *See* ANDRÉ LUCAS, LE DROIT DE L'INFORMATIQUE 66-67 (1987).

16. *See* COLIN J. BENNETT, REGULATING PRIVACY 91-93 (1992).

17. *See* Loi fédérale sur la protection des données du 19 juin 1992 [Federal Law on the Protection of Data, June 19, 1992] (Switz.).

18. *See infra* notes 23-28 and accompanying text.

19. For an excellent concise history of these efforts, see BENNETT, *supra* note 16, at 130-39.

States. At the same time, Europeans argued for increased attention to privacy concerns. While the principles adopted by the OECD and the Council of Europe are quite similar, the OECD emphasized the free flow of information in contrast to the Council of Europe, which stressed the human rights concerns. The OECD recommended a voluntary set of guidelines rather than a binding set of rules like those in the international treaty proposed by the Council of Europe. Other international organizations such as the International Bureau of Informatics, the U.N. Center on Transnational Corporations, and the International Telecommunications Union have also addressed fair information practices, but with considerably less recognition of their work in the international community.[20]

B. Toward Narrower Balancing

The dynamic environment for global information networks makes the broad balance sought in the trade dimension an ever-elusive goal. The increased computing power of sophisticated communications networks in the 1980s created specialized networks and customized information use. Inevitably, these technological and market developments moved the search for fair information practice standards from general principles to particularized contextual definitions. The Council of Europe, for example, recognized the need to define fair information practices under specific circumstances and issued recommendations for areas such as direct marketing, employment records, and means of payment.[21] National laws also moved in the direction of context-specific rules.[22]

The European Community's harmonization efforts demonstrate the same elusive quality in its search for the trade-dimension balance between free flow and human rights. In 1990, when the Commission of the European Community proposed a directive to harmonize the legal

---

20. *Id.* at 132-33.

21. *See* COUNCIL OF EUROPE COMMITTEE OF MINISTERS, RECOMMENDATION R(85)(20) ON THE PROTECTION OF PERSONAL DATA FOR PURPOSES OF DIRECT MARKETING (1985); COUNCIL OF EUROPE COMMITTEE OF MINISTERS, RECOMMENDATION R(89)(2) ON THE PROTECTION OF PERSONAL DATA USED FOR EMPLOYMENT PURPOSES (1989); COUNCIL OF EUROPE COMMITTEE OF MINISTERS, RECOMMENDATION R(90)(19) ON THE PROTECTION OF PERSONAL DATA USED FOR PAYMENT AND OTHER RELATED OPERATIONS (1990).

22. *See, e.g.*, Data Protection Act §§ 15-16 (1988) (Neth.) (providing rules for the protection of privacy in connection with personal data files), *translated in* Council of Europe Doc. CJ-PD (89) 4 (Jan. 27, 1989).

standards of fair information practice in each of the member states, the proposal was a classic example of the trade debate.[23] The spirit of the 1992 program logically extended concepts of free movement from goods and services to personal information. Consequently, the draft linked information flows to the development of the internal European Community market and sought to protect individual rights against data processing through a set of regulatory principles. Again, U.S. industries and their European trading partners urged the Commission to include a commitment to the principle of free exchange of data. In fact, the revised draft specifically sought this clarification in a title change.[24] This trade approach has fueled persistent debate over the effect of the directive. If the directive sets minimum standards for fair information practices, then further distortions on the free flow of information may still be encouraged by divergent actual levels of protection. However, if the directive sets mandatory standards, then additional limitations on free flows may be avoided. In its efforts, the Commission has had some difficulty establishing general regulations. The draft directive contained a provision for business groups to develop codes of conduct, and the Commission offered simultaneously a companion proposal explicitly directed to fair information practices in the telecommunications sector.[25] This approach flows from experiences in the member states, such as Germany and France, where sectorial implementation was critical.

The treatment of data flows to destinations outside the European Community posed a similar dilemma for the trade perspective. Taking data privacy seriously would have a limiting effect on the free exchange of information with nations outside the Community. Under the initial draft, the export of personal information to non-European Community member countries was to be prohibited unless the destination assured a sufficient degree of protection.[26] "Data havens" would be blacklisted, and countries such as the United States were assumed to be targets for a blanket export prohibition, though individual exemptions might have been possible.[27] Because few non-European countries approach fair informa-

---

23. *See* Proposed Directive, *supra* note 14.

24. *See* Amended Proposal, *supra* note 3, Explanatory Memorandum, at 8.

25. *See* Proposed Directive, *supra* note 14, § 20 (provision relating to sectoral codes of conduct).

26. *See id.*, art. 24.

27. *See id.*, art. 25.

tion practice standards with the same rigor, the proposed directive risked isolating Europe from global information networks.

The revised version of the directive created a more nuanced balance between free flows of information and human rights.[28] Data exports are still subject to restriction if the foreign destination lacks adequate protection for individuals. The generic approach was tailored to a more narrow balancing of the free flow and human rights interests. Under the revised draft, national authorities may consider the specific circumstances of each data transfer on a case-by-case basis, rather than an overall country assessment, to determine the sufficiency of the destination's fair information practice standards.

Although the revised version appears more flexible, it causes greater complexity in the regulation of data flows. The second draft no longer gives foreign companies the same ability to lobby as a group with European partners against a blanket restriction on data flows. Moreover, companies will now have to argue separately before each of the twelve future national authorities. With or without the revised directive, national authorities under existing European laws are likely to scrutinize data exports to the United States more thoroughly because some American industries, such as direct marketing, have achieved notoriety for their limited standards of fair information practice. In short, the rules of the road for global "electronic highways" are becoming a higher priority issue for governments and transnational businesses.

C. Toward Customized Balancing

Traditional multilateral trade negotiations have not ignored the significance of fair information practices for the emerging electronic highway system. The endless search to define fair information practice standards for international data exchange in itself poses barriers to global information networking. When services appeared on the agenda for the Uruguay Round of GATT negotiations, negotiators became concerned that standards for transborder data flows might be used as protectionist trade impediments. Following the trend away from general principles, the services sector negotiating group reviewed proposals for the circumstanc-

28. *See* Amended Proposal, *supra* note 3, art. 26.

es permitting restrictions on transborder data flows.[29] Similarly, the negotiators for the proposed North American Free Trade Agreement contemplated fair information practices. The American delegation sought to ensure "fair access to and use of public networks"[30] for information services, and the proposed text defines conditions for privacy, security, and confidentiality legislation.[31]

Both sets of trade negotiations strongly tilt the balance toward free flows of information. The proposed trade treaties establish the standard that restrictions on information flows may not be discriminatory and most favored nation treatment would apply.[32] Signatory countries, for example, could not generically restrict data flows to the United States without also scrutinizing other countries and blacklisting those similar to the United States. In an age of global networks, non-discrimination forces rules of fair information practice to be narrowly defined for specific types of data flows and uses.

For international information exchanges, the trade paradigm moves toward definitions increasingly customized to specific circumstances. The French, for example, have used a contractual approach for data protection. When the destination of an information export does not have any omnibus law, the French government authority has required execution of a contract between the French data exporter and foreign importer to assure that the protections for individuals apply to the foreign data processing.[33] The International Chamber of Commerce in conjunction with the Council of Europe and the European Commission have prepared a model contract for international data transfers to promote this type of regulatory customization.[34] Despite the attempt to customize standards,

---

29. GATT Doc. MTN.TNS/W/FA, at 18 (1990) (measures necessary to secure compliance with laws or regulations for the protection of privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality are permissible provided they are not applied in a discriminatory manner or as a disguised restriction on international trade in services).

30. *See* SERVICES POLICY ADVISORY COMMITTEE, REPORT ON THE NORTH AMERICAN FREE TRADE AGREEMENT 12-13 (1992) (prepared in compliance with the Omnibus Trade and Competitiveness Act of 1988).

31. *See* Proposed North American Free Trade Agreement, art. 1302(5) (1992).

32. "Most favored nation treatment" means that a signatory to a treaty must grant another signatory the same treatment as the most favorable treatment accorded to any other nation.

33. *See* Déliberation No. 89-78 du juillet 1989, *reprinted in* C.N.I.L., 10e Rapport (1989).

34. *See Model Clauses for Inclusion in a Model TBDF Contract*, PRIVACY L. & BUS., Dec. 1992, at 17-18; MODEL CONTRACT TO ENSURE EQUIVALENT DATA PROTECTION IN

this contractual approach may not satisfy the proper balancing. Problems of scope and enforcement may remain.[35]

The trend in the trade dimension toward micro-level balancing suggests that fair information practice standards may become part of the technological architecture of global networks.[36] Network configuration and the choice of technologies may be used to assure fair information practices for specific international circumstances. This evolution leads to narrowly drawn standards for international data flows and a growing importance for the technical dimension. Technical choices become critical to implement standards in particular circumstances, and the technical decisions themselves may determine standards.

II. THE TECHNICAL PARADIGM: STANDARDIZATION OF SYSTEM ARCHITECTURE

While the trade dimension receives most of the international attention, fair information practice standards have also emerged using a distinctly technical paradigm. Integrity and interoperability of information networks are usually defined in terms of technical criteria.[37] Unlike the trade dimension trend toward context-specific definitions of fair information practice, the technical perspective is moving toward defining broader, normative standards within the architecture of global networks. The paramount value is the elimination of technological obstacles to system interconnection.

A. Integrity

The integrity of information flows depends on system reliability and confidentiality. Fair information practice rules typically mandate

---

THE CONTEXT OF TRANSBORDER DATA FLOWS WITH EXPLANATORY MEMORANDUM (Nov. 2, 1992) (available from Council of Europe T-PD 7 revised).

35. *See* Ulrich Lepper, *Experience with Contracts on Transborder Data Flows in the Credit Sector*, *in* Proceedings, *supra* note 8, at 50-51.

36. *See* Reidenberg, *supra* note 1, at S175-76.

37. For an excellent overview of the standards process in the European Community and the United States, see STEPHEN WOOLCOCK, MARKET ACCESS ISSUES IN EC-US RELATIONS: TRADING PARTNERS OR TRADING BLOWS? 92-110 (1991).

adequate security to preserve integrity.[38] Provisions in the multilateral instruments on transborder data flow stipulate a requirement of security.[39] Omnibus data protection laws require data processors to take measures to assure the integrity of personal information.[40] Industry-specific or sectoral laws similarly require security measures.[41] In addition, private contracts will also customarily obligate system operators to assure security.[42]

Security measures are usually part of the infrastructure of global information networks. Technological safeguards protect against unauthorized manipulation of computer systems and are an integral part of fair information practice standards. "Soft" policy solutions such as password access or restricted sites may limit unauthorized manipulation. "Hard" physical solutions such as semi-conductor chips on credit cards may also be used to assure security by imposing barriers to the access and manipulation of data.[43] These two technical methods may be combined when particular circumstances or types of information flows require higher level security. For example, in Sweden, subscribers to the Swedish TeleGuide electronic shopping network receive a magnetic card containing name, address, and bank account data.[44] With a PIN, the subscriber may access the network from any TeleGuide terminal. Other payment networks in Europe are increasingly using more sophisticated chip card technology to offer transaction authorization at the local level (i.e., purchase site) as well as at the system level (i.e., centralized

---

38. *See, e.g.*, Proposed Directive, *supra* note 14, Preamble ¶ 21.

39. *See* European Convention, *supra* note 7, art. 7; OECD Guidelines, *supra* note 7, art. 11.

40. *See, e.g.*, Loi No. 78-17 du 6 janvier relative à l'informatique, aux fichiers et aux libertés, art. 29, 1978 J.O. 227, 229 [Law No. 78-17 of Jan. 6 relating to data processing, files, and freedoms] (Fr.); Data Protection Act § 8 (1988) (Neth.) (providing rules for the protection of privacy in connection with personal data files), *translated in* Council of Europe Doc. CJ-PD (89) 4 (Jan. 27, 1989); Amended Proposal, *supra* note 3, art. 17.

41. Banking rules, for example, typically require a high degree of security. *See, e.g.*, U.S. GENERAL ACCOUNTING OFFICE, ELECTRONIC FUNDS TRANSFER OVERSIGHT OF CRITICAL BANKING SYSTEMS SHOULD BE STRENGTHENED, GAO Doc. IMTEC-90-14 (1990).

42. *See* GEORGE BRANDON & JOHN K. HALVEY, DATA PROCESSING CONTRACTS 165-67, 357 (3d ed. 1990).

43. Chip cards may be used only with a machine programmed to read the code on the chip.

44. *See* Matthew Rose, *French Minitel Idea Slumps in Sweden*, DM NEWS, Feb. 1, 1993, at 1.

authorization centers).[45] Various network transactions may demand higher security than others. For example, the computerization of health records for remote access might require greater confidentiality measures than home shopping networks.

Because technical security safeguards are implemented through network architecture, national and international standards organizations are struggling to develop policies and measures for different levels of security. The European Committee for Standardization/European Committee for Electrotechnical Standardization ("CEN/CENELEC") and its national members, for example, have considered security needs for European payment systems. The Consultative Committee for International Telegraph and Telephony ("CCITT") has addressed security issues for global telecommunications, and the United Nations effort to develop an electronic data interchange standard, EDIFACT, has also worked on security for electronic-based transactions. Coordinated efforts are essential to avoid incompatible security standards that would establish technological barriers to global network interconnection. Standards also offer a variety of choices for the level of security measures. For example, standard encryption techniques are available to secure confidentiality, while standard techniques to build system "firewalls" can be used to protect against intrusions. Meanwhile, standards for authorization protocols can be found to verify legitimate users, and standards to segment chip memory can offer multi-user validation and access limitations. These standardizations all facilitate the connection of global information networks.

The choices for technical standards also define fair information practice. For example, the widely used encryption standard DES is not the most secure encryption standard available.[46] To define and adopt DES for a network rather than the more secure RSA encryption standard

---

45. Visa, for example, now embeds microprocessors on cards issued in France. *See* Penny Pagano, *Consumers Can Charge Everything*, L.A. TIMES, Sept. 27, 1985, §6, at 4; David Olmos, *Deal with AT&T; High-Security Card Planned by Codercard*, L.A. TIMES, July 13, 1988, §6, at 6; William Gruber, *Automated Tellers to Meet Bank Card*, CHI. TRIB., Aug. 10, 1987, at C5.

46. DES is a widely used U.S. federal government standard that must be incorporated in hardware used for government contracts that require encryption security. DES is subject to stringent U.S. export controls. RSA is a proprietary standard that is a more sophisticated, more secure encryption algorithm. Companies seeking higher levels of security prefer to use RSA.

sets the satisfactory level of security at a lower point. In addition, the technical decisions that locate safeguards at particular places in global information networks also define responsibility for fair information practices.[47] The choice of authorizing access by a network central processor rather than a chip card processor assigns responsibility in different ways. These technical standardization efforts, thus, have a broader significance for fair information practices.

While the technical perspective emphasizes technological solutions to maintain the integrity of global networks, "hard" and "soft" solutions do not settle security issues. Computer crime statutes around the world seek also to protect integrity through prohibitions on computer tampering and unauthorized use.[48] The criminalization of these security breaches suggests that the purely technical answers to system integrity do not set a complete standard of fair information practice. Paradoxically, computer crime laws are not always an effective instrument to establish a higher standard. Victims frequently have an incentive not to acknowledge unauthorized access or use. By publicly recognizing illegal access or use, the victim announces that its information system may not be adequately secure, and that the integrity of the system is not assured.

B. Interoperability

Beyond the integrity of global information networks, the technical dimension seeks interoperability of communications systems. Interoperability requires that communications protocols be technically compatible for diverse technologies to interconnect. Common standards, such as the ISDN protocols, are necessary to achieve interoperability.[49] International technical organizations seek to define these standards.[50] The results have

---

47. DES, for example, is usually implemented at the hardware level, while other encryption techniques are implemented at any level, hardware or software.

48. *See, e.g.*, N.Y. PENAL LAW § 156 (McKinney 1991); COUNCIL OF EUROPE RECOMMENDATION R(89)(9) ON COMPUTER-RELATED CRIME (1989); JÉRÔME HUET & HERBERT MAISL, DROIT DE L'INFORMATIQUE ET DES TÉLÉCOMMUNICATIONS 833-57 (1989).

49. *See* Joachim Scherer, *European Telecommunications Law: The Framework of the Treaty*, 12 EUR. L. REV. 354, 355 (1987).

50. Standards are defined, for example, by the International Standards Organization ("ISO"), CEN/CENELEC, and national or regional groups such as the European Telecommunications Standards Institute ("ETSI"). The standardization process can be controversial. *See* Roger Tuckett, *Access to Public Standards: Interoperability Revisited*, 14 EUR. INTELL. PROP. REV. 423 (1992); Diana Good, *How Far Should IP Rights Have To*

significant implications for information use. For example, the X.400 and X.500 e-mail transmission standards defined by CCITT allow "functionality and communications" within network architecture.[51] This means that the network can do much more than merely transmit messages from point to point. The network can translate different transmission protocols to connect previously incompatible information technologies. It can provide network-based directory assistance, and it can package a wealth of transaction data with messages.

The technical choices made for interoperability set the parameters directly in global network architecture. The interoperability standards cannot be isolated from broader definitions of fair information practice. Caller identification and call blocking show the illusion of such a separation.[52] The service raises important questions of fair practice. "Caller identification" displays the telephone number of the calling party to the recipient. "Call blocking" enables the calling party to block his identification to the recipient on either a per line or per call basis. Yet, communications protocols define if and how the services can be offered between regional or national networks. For example, if a common protocol enables caller identification, but not call blocking, the technical choice defines an important fair information practice standard. Even the choice of the technology sets fair information practice standards. Only one of the two presently available technologies can accommodate "call blocking."[53] Similarly, if a common protocol cannot support particular security technology, then the level of security may be limited by the interoperability standard.

The technical dimension is increasingly linked to more expansive definitions of fair information practice standards. Varying rules of conduct for information systems can hinder the interoperability of global

---

Give Way to Standardization: The Policy Positions of ETSI and the EC, 14 EUR. INTELL. PROP. REV. 295 (1992).

51. *See* Mitzi Waltz, *Opening the Gateways for Cross-Platform E-mail*, MACWEEK, Dec. 14, 1992, at 107.

52. *See* Glenn C. Smith, *We've Got Your Number! (Is it Constitutional to Give It Out?): Caller Identification Technology and the Right to Informational Privacy*, 37 UCLA L. REV. 145 (1989).

53. *See* FINAL REPORT OF THE PRIVACY AND TECHNOLOGY TASK FORCE 10 (1991) (submitted to Senator Patrick J. Leahy). The Automatic Number Information ("ANI") technology cannot accommodate call blocking, unlike the other caller identification choices using Common Channel System Signaling 7 technology.

networks. The Canadian Standards Association ("CSA"), for example, feared that the proposed European directive on data protection would limit the connections between Canadian information networks and European information sources.[54] As a result, CSA began work on a privacy code.[55] Yet, in keeping with the technical perspective, CSA contemplates the eventual implementation of the privacy code by its members and others through technical solutions.[56] There is also speculation that the International Standards Organization ("ISO") might similarly address broader fair information practice issues.[57]

In contrast to the trend in the trade dimension, these technically defined standards are moving toward an expansive vision of fair information practice. Technical choices lead to normative decisions about fair information practice standards. Yet, the technical dimension subtly introduces these standards through the network architecture itself, rather than through a broader debate on the norms.

III. THE GOVERNANCE OF GLOBAL INFORMATION NETWORKS

The trade and technical paradigms each obscure the link between fair information practice standards and governance. Choices under each perspective are essentially governance decisions. They determine who sets rules of the road for global networking and how standards are defined. This establishment of rules of conduct, whether through trade balancing or technical standardization, is based on particular visions of social relations, the role of the state, and the relationship between nations. Each perspective raises different sets of values and assumptions. Global information networks juxtapose these different visions.

In searching for a balance between free flows of information and human rights, the trade perspective sets norms for relationships among

---

54. CANADIAN STANDARDS ASSOCIATION, PROPOSAL FOR A MODEL PRIVACY CODE (1992), *reprinted in* 1992/2 REVUE DE DROIT DE L'INFORMATIQUE ET DES TÉLÉCOMS 88. Work on the code has not yet been completed.

55. *Id.*

56. *Id.* at 90.

57. *See* Charlotte-Marie Pitrat, *Protection de la vie privée dans le secteur privé: le Canada et le Québec bougent*, 1992/2 REVUE DE DROIT DE L'INFORMATIQUE ET DES TÉLÉCOMS 86, 87.

citizens. European democracies tend to assume that the state is needed to develop the social community within which individuals develop.[58] As a result, European countries view data protection regulation as the realm of "public law"[59] and define substantive rights and obligations in a way that reflects a statist vision of governance. For example, computer databases must often be registered with the government.[60] Registration frequently involves the disclosure to the data protection authority of detailed information concerning the registrant's data base and computer operations.[61] Europeans also tend to give more weight to human rights concerns. This higher value may be seen in the special provisions for "sensitive" data such as information pertaining to race, health, sexual preferences, and political opinions as well as with the careful administration and judicial evaluation of context to determine if other data may be sensitive.[62] The American approach, in contrast, is founded on principles of private rights and libertarian governance.[63] Americans are more suspicious of the state,[64] and, consequently, fair information practice standards usually weigh free flows of information more heavily.

With the dramatic political changes in Eastern Europe and the fall of the Berlin Wall, many formerly communist countries are also trying to develop concepts of fair information practice to match their emerging democracies. Hungary's constitutional court declared the existence of fair

---

58. *See* Yves Poullet, *Data Protection Between Property and Liberties: A Civil Law Approach*, *in* AMONGST FRIENDS IN COMPUTERS AND LAW 161, 175 (H.W.K. Kasperson & A. Oskamp eds., 1991).

59. *See* Peter Blume, Remarks at Privacy Laws & Business Conference on New European Community Data Protection Law, St. John's College, Cambridge (July 1992), *in* Peter Blume, *Legal Culture and the Possibilities of Control*, 3 LECTURES ON DATA PROTECTION (1992).

60. *See, e.g.*, 1984 Data Protection Act, ch. 35 (U.K.); Loi No. 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, art. 16, 1978 J.O. 227, 228 [Law No. 78-17 of Jan. 6 relating to data processing, files, and freedoms] (Fr.).

61. *See, e.g.*, U.K. Data Protection Registrar, Form DPR1 Application for Registration, Part B (1984) (U.K.); Délibération No. 79-03 du 23 octobre 1979 portant adoption d'un calendrier d'appel et d'un modèle de déclaration et de demande d'avis nécessaires à la mise en oeuvre des traitements automatisés d'informations nominatives, *reprinted in* C.N.I.L., J.O. Informatiques et libertés No. 1473, at 113, 119 (1991).

62. *See, e.g.*, European Convention, *supra* note 7, § 6; Schwartz, *supra* note 9.

63. *See* Reidenberg, *supra* note 11, at 208-09; David W. Leebron, *The Right to Privacy's Place in the Intellectual History of Tort Law*, 41 CASE W. RES. L. REV. 769, 785-88 (1991); Paul Schwartz, *Data Processing and Government Administration: The Failure of the American Legal Response to the Computer*, 43 HASTINGS L.J. 1321, 1350-51 (1992).

64. *See* Herbert J. Spiro, *Privacy in Comparative Perspective*, *in* XIII NOMOS 121, 122 (J. Roland Pennock & John W. Chapman eds., 1971).

information practice rights just as the nation sought to distance itself from the Soviet political system.[65] Czechoslovakia, between its freedom and demise, enacted a fair information practices law.[66] Meanwhile, Poland also saw the need for fair information practice standards,[67] and Bulgaria began to consider statutory rights and obligations.[68]

As global information networks took shape, the trade perspective adopted narrower evaluations of fair information practice to accommodate the complexity of information-sharing arrangements. These narrower evaluations set norms in favor of free flows of information. Global information networks enable information to be available instantaneously in virtually any part of the world. This availability and control of information affects an individual's ability to participate in society.[69] Yet, the narrow examination of particular international data flow circumstances will not address the overall concentration of control over a tremendous amount of personal information in the private sector. While the effect of this concentration can be either positive or negative,[70] the overall shift challenges traditional norms of relations between individuals and industry as well as the role of the state as an arbiter of fair information practices.

The choice between the trade and technical perspectives also involves norms of governance. The technical paradigm locates control of information practices in the network infrastructure. Technical organizations rather than governments define the norms for integrity and interoperability. As the trend in standards organizations demonstrates, these standards of fair information practice are expanding to cover all aspects of network use.[71] National boundaries become secondary to network borders. In contrast, the trade paradigm obligates national

---

65. *See* László Majtenyi, *Central and East European Countries: Progress Towards the Elaboration of Data Protection Laws—Hungary*, *in* Proceedings, *supra* note 8, at 80.

66. *See Czechoslovakia Enacts Data Protection Law*, PRIVACY L. & BUS., Oct. 1992, at 8; Jirí Fronek, *Central and East European Countries: Progress Towards the Elaboration of Data Protection Laws—Czechoslovakia*, *in* Proceedings, *supra* note 8, at 77.

67. *See* Ewa Letowska, *Central and East Europe Countries: Progress Towards the Elaboration of Data Protection Laws—Poland*, *in* Proceedings, *supra* note 8, at 83.

68. *See* ABA CENTRAL AND EAST EUROPEAN LAW INITIATIVE, ANALYSIS OF BULGARIA'S DRAFT INFORMATION LAW (1992).

69. *See* Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. PA. L. REV. 707, 732-34 (1987).

70. Some of the positive aspects of widely available personal information are customization of consumer products and better targeting of consumers. Some of the negative aspects are loss of privacy and isolation for those outside "information profiles."

71. *See supra* notes 54-57 and accompanying text.

authorities and multilateral instruments to define standards of fair information practice and assumes that regulatory jurisdiction will be based on national borders.

CONCLUSION

Global information networks do not conform neatly to any clear choice between technical and trade norms of governance. Networks operate within and across national borders and link separately controlled information systems. For example, a simple transaction-processing network may involve data capture in one country, a transaction authorization system at a remote computer site located in a second country, and settlement processing in a third country on another computer system. Thus, setting standards for fair information practices will depend on both the trade and technical sides. National governance principles will guide trade-based standards, and network governance principles will inform technical standards.

If global information networks are to be free of unnecessary roadblocks, policymakers must develop complex interactions to accommodate the variety of normative choices and standards that confront each other on the networks. Standards of fair information practices will not come from a single source or a single view.[72] The inextricable link between standards of fair information practice and governance suggests that a complex system of overlapping regulation or co-regulation will be needed to set the terms for information flows on global networks. Co-regulation permits national and network definitions of fair information practice to mesh. Global networks must be able to accommodate different norms of governance. Trade-based standards in one part of a global network may overlap with technical standards in other parts of the global network. Without co-regulation, transborder data flow prohibitions would seek to export normative values rather than to restrict the transmission of personal information.

To prevent global electronic gridlock, we must understand and appreciate more thoroughly the evolving governance norms for global

---

72. *See* Spiros Simitis, *New Trends in National and International Data Protection*, *in* RECENT DEVELOPMENTS IN DATA PRIVACY LAWS: BELGIUM'S DATA PROTECTION BILL AND THE EUROPEAN DRAFT DIRECTIVE 22-23 (J. Dumothier ed., 1992).

information networks. The movement toward contextual evaluations[73] marks the beginning of more sophisticated and appropriate global network regulation.

73. *See, e.g.*, Reidenberg, *supra* note 1, at S171-76. *Compare* Proposed Directive, *supra* note 14, art. 24 *with* Amended Proposal, *supra* note 3, art. 26.