# Five Challenges for Regulating the Global Information Society

by
Pamela Samuelson*

## I. Introduction

Information technology (IT) is unquestionably having a profound effect on many aspects of the social, cultural, economic, and legal systems of planet Earth.[1] IT has enabled significant advances in global communications technologies, particularly the Internet, that make it more possible than ever before to contemplate the development of a global information society.[2] Such a society may offer many benefits to humankind, but constructing policies to enable and promote this information society presents significant challenges. Among the most difficult questions now confronting legal decisionmakers are these: Can existing laws successfully be applied to activities occurring via new communications media such as the Internet? Can existing law be adapted to regulate these activities? Are existing laws outmoded or inadequate? Are completely new laws needed to deal with Internet and other information technology developments?

Experience thus far addressing these questions in the European Union (EU) and United States (U.S.) suggests that existing law can sometimes be applied with relative ease to Internet activities and that existing law can sometimes be adapted to reach Internet activities.[3] However, in some instances, new laws seem to be needed. When old laws do not fit and cannot easily be adapted, it may be necessary to go back to first principles and consider how to accomplish societal objectives in the new context of the Internet. Decisions about the law of Internet, whether carried out by judges, legislatures, or regulators, will have an important impact on the kind of information economy that will emerge. The EU is to be commended for realizing that regulating the Internet is about more than information infrastructure and economics.[4] Deciding how to regulate the Internet is also about constructing an information society in which social and cultural values can be preserved. This article will offer some suggestions about how regulators might more wisely make policy choices to promote a global information society.

## II. Five Challenges for Policymakers

---

* Professor of Information Management and of Law, University of California at Berkeley. This paper is based on a presentation given at a conference on Communications Regulation in the Global Information Society held at the University of Warwick in June of 1999. Thanks to Chris Marsden for organizing such an excellent conference and thanks to Leah Theriault for excellent work in bringing this paper to fruition.

[1] See, e.g., MANUEL CASTELLS, THE RISE OF THE NETWORK SOCIETY (1996).

[2] See, e.g., EUROPE AND THE GLOBAL INFORMATION SOCIETY: RECOMMENDATIONS TO THE EUROPEAN COUNCIL, *available at* http://www2.echo.lu/eudocs/en/bangemann.html.

[3] See *infra* Section IIA.

[4] See, e.g., Commission of the European Communities, Green Paper on the Convergence of the Telecommunications, Media and Information Technology Sectors, and the Implications for Regulation Towards an Information Society Approach COM(97)623 (December 1997); Cf. INFORMATION INFRASTRUCTURE TASK FORCE, THE NATIONAL INFORMATION INFRASTRUCTURE: AN AGENDA FOR ACTION (Dec. 1993) (emphasizing infrastructure and economic issues).

For the first decade or so after the development of computer networks and related communications technologies, there was little need for policymakers to pay attention to activities taking place there. Back then, the user community was, for the most part, a relatively homogenous group of researchers at universities and commercial laboratories who tended to use the networks to communicate the results of their work or work-in-progress and not to cause trouble.[5] Once networking and other technologies evolved to the point that ordinary people could easily use the network, and once the National Science Foundation lifted the earlier ban on commercial activities on the networks, policymakers came to realize that they would have to decide how to regulate this new medium of communication.[6] They face at least five key policy challenges today:

1. whether they can apply or adapt existing laws and policies to the regulation of Internet activities, or whether new laws or policies are needed to regulate Internet conduct;
2. how to formulate a reasonable and proportional response when new regulation is needed;
3. how to craft laws that will be flexible enough to adapt to rapidly changing circumstances;
4. how to preserve fundamental human values in the face of economic or technological pressures tending to undermine them; and
5. how to coordinate with other nations in Internet law and policy making so that there is a consistent legal environment on a global basis.[7]

Examples of each challenge will be discussed below.

A. Old Law or New Law?

Many examples illustrate the dilemma policymakers now face in considering whether they can apply existing laws or need to adopt new laws. In this age of

---

[5] See, e.g., Barry A. Leiner, et al., *A Brief History of the Internet*, (last modified Feb. 20, 1998) *available at* <http://www.isoc.org/internet/history/brief.html>; but see, KATIE HAFNER AND JOHN MARKOFF, CYBERPUNK: OUTLAWS AND HACKERS ON THE COMPUTER FRONTIER (1995) (well before the inception of the Internet, computer enthusiasts known as hackers engaged in disruptive and quasi-criminal behavior in networked environments).

[6] See, e.g., LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (2000).

[7] These five challenges were first discussed in Pamela Samuelson*, A New Kind of Privacy? Regulating Uses of Personal Data in the Global Information Economy*, 87 Calif. L. Rev. 751(1999) (reviewing PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW: A STUDY OF UNITED STATES DATA PROTECTION (1996) and PETER P. SWIRE AND ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE (1998)). They have also been elaborated upon in Pamela Samuelson, *Internet Law and Policy: A U.S. Perspective*, (forthcoming 2000), delivered at the Japanese-American Society for Legal Studies Symposium on Internet and Private Law held at Sendai, Japan, on September 26, 1999.

convergence of communications technologies,[8] in which the content being delivered (e.g., voice, video, text) is no longer confined to a particular delivery infrastructure (e.g., copper wires or fiber optic cable, co-axial cable, airwaves), policymakers must decide, first, whether to regulate at all, and second, what specific kind of regulation is appropriate. Convergence makes this second choice particularly problematic, as regulators are faced, not just with a choice between an old law and a new law, but with a choice between multiple existing regulatory forms.

Consider, for example, Internet "streaming" of video or audio signals.[9] When a content provider streams video and/or audio over the Internet, should it be treated like a television broadcaster, a radio broadcaster, or a passive content provider? Should the choice depend on whether this streaming service is offered over the existing telecommunications infrastructure, over cable lines, or via a new wireless technology? To date, the U.S. Federal Communications Commission (FCC) has responded to these challenges with a 'hands-off' approach, declining to graft the regulatory regimes of realspace onto their cyberspace analogs.[10] The FCC maintains that its refusal to force new Internet services into old communications regulation categories has fostered the development of new Internet business models, and has increased public participation in the Internet by lowering the cost of content and service delivery.[11]

Competition law (and its American counterpart, antitrust law) provides another example of the conflict between old ways of regulating and new ways of doing business. Microsoft founder Bill Gates, for example, believes that U.S. antitrust rules are outmoded in the digital age.[12] Such laws may, in his view, have been needed to regulate manufacturing industries because monopolists or cartels in those industries could restrict output, control prices, and exclude competitors.[13] But in the digital age, anyone can write an operating system program and sell it in competition with Microsoft, and may the best competitor win! The U.S. Justice Department and judge overseeing the lawsuit filed by Justice Department to challenge to Microsoft's business practices have a different opinion about the viability of competition law in the information age.[14] Judge Jackson

---

[8] See generally, COMPUTER SCIENCE AND TECHNOLOGY BOARD, NATIONAL RESEARCH COUNCIL, KEEPING THE U.S. COMPUTER AND COMMUNICATIONS INDUSTRY COMPETITIVE: CONVERGENCE OF COMPUTING, COMMUNICATIONS, AND ENTERTAINMENT (1995).

[9] See, e.g., Lisa Napoli, *Webcast Audiences Aren't Just Sitting There, Survey Finds,* N. Y. Times (June 29, 1999) <http://www.nytimes.com/library/tech/99/06/cyber/articles/29radio.html>; Lawrie Mifflin, *Watch the Tube or Watch the Computer?*, N. Y. Times (February 1, 1999) <http://www.nytimes.com/library/tech/99/02/biztech/articles/01tube.html>.

[10] See Jason Oxman, Counsel for Advanced Communications, *The FCC and the Unregulation of the Internet*, (working paper July 1999) available at <http://www.fcc.gov/opp/workingp.html>.

[11] *Id.*

[12] Bill Gates, *U.S. v. Microsoft: We're Defending Our Right to Innovate*, The Wall Street Journal, (May 20, 1998) <http://www.microsoft.com/presspass/doj/5-20wsjoped.htm>.

[13] See, e.g., STANLEY J. LIEBOWITZ and STEPHEN E. MARGOLIS, WINNERS, LOSERS & MICROSOFT: COMPETITION AND ANTITRUST IN HIGH TECHNOLOGY (1999) (traditional antitrust concepts do not map well to the software market – despite having overwhelming market share, Microsoft was actually the driving force behind *decreasing* software prices)

[14] See Plaintiff's Complaint at 49, U.S. v. Microsoft, 65 F.Supp.2d 1 (D.D.C. 1999) (No. Civ. 98-1232 (TPJ), Civ. 98-1233 (TPJ)) *available at* <http://www.usdoj.gov/atr/cases/f1700/1763.htm>. For more

has found that Microsoft possessed monopoly power in the market for Intel-compatible PC operating systems, power which it used to maintain barriers to entry to new competitors.[15] Antitrust law will no doubt need to adapt to some degree to take into account considerations such as those that arise when a firm technologically ties its products so as to disadvantage a competitor,[16] or to respond to the presence of strong network effects, which are common in digital networked environments and may create intractable barriers to entry to the online marketplace.[17] But the general view in the U.S. is that antitrust and competition law continues to be viable in the digital age, and can successfully be adapted to deal with software and Internet companies.

Copyright law also poses challenges to the regulation of digital content and networked environments.[18] Although some commentators have suggested that copyright law is outmoded in the Internet environment,[19] the general view in the U.S. and the EU is that copyright law can be applied and adapted to protect expressive works in digital form.[20] Both the E.U. and the U.S. are adopting or have adopted legislation in an effort to ensure that copyright law keeps pace with technological change.[21]

---

comprehensive coverage of the Department of Justice's case, see generally, <http://www.usdoj.gov/atr/cases/ms_index.htm>.

[15] For Judge Jackson's findings of fact, see Court's Findings of Fact, U.S. v. Microsoft, 65 F.Supp.2d 1 (D.D.C. 1999) (No. Civ. 98-1232 (TPJ), Civ. 98-1233 (TPJ)) *available at* <http://www.microsoft.com/presspass/trial/c-fof/>.

[16] See, e.g., Brief of Professor Lawrence Lessig as *Amicus Curiae* at 6-8, U.S. v. Microsoft, 65 F.Supp.2d 1 (D.D.C. 1999) (No. Civ. 98-1232 (TPJ), Civ. 98-1233 (TPJ)) *available at* <http://cyber.law.harvard.edu/works/lessig/AB/abd9.doc.html>.

[17] Network externalities occur when the value of choosing a specific product increases as the number of consumers already using that product increases. Network externalities are particularly common in the digitized environment because of the importance of interoperable systems. For an explanation of network externalities see, Mark Lemley and David McGowan, *Legal Implications of Network Economic Effects*, 86 CALIF. L. REV. 479 (1998).

[18] For a comprehensive overview of these challenges, see e.g., COMMITTEE ON INTELLECTUAL PROPERTY RIGHTS IN THE EMERGING INFORMATION INFRASTRUCTURE, NATIONAL RESEARCH COUNCIL, THE DIGITAL DILEMMA: INTELLECTUAL PROPERTY IN THE INFORMATION AGE (1999) [hereinafter Digital Dilemma].

[19] John Perry Barlow, *The New Economy of Ideas*, WIRED 2.03 (1994), *available at* <http://metalab.unc.edu/wxyc/legal/economy.ideas.html>.

[20] See e.g., INFORMATION INFRASTRUCTURE TASK FORCE WORKING GROUP ON INTELLECTUAL PROPERTY RIGHTS, INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE: THE REPORT OF THE WORKING GROUP ON INTELLECTUAL PROPERTY RIGHTS *available at* <http://www.uspto.gov/web/offices/com/doc/ipnii/>; Digital Dilemma, *supra* note 18 at 239 ("Intellectual property will surely survive the digital age. It is clear, however, that major adaptations will have to take place to ensure sufficient protection for content creators and rights holders, thereby helping to ensure that an extensive and diverse supply of IP is available to the public."); Commission of the European Communities, Green Paper on Copyright and Related Rights in the Information Society COM(95)382 (July 1995).

[21] The U.S. Congress has enacted legislation to implement the provisions of the WIPO Copyright Treaty, adopted by the Diplomatic Conference on Dec. 20, 1996, WIPO Doc. CRNR/DC/94 (Dec. 23, 1996) [hereinafter WIPO Copyright Treaty]. See Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998). The E.U. response to the WIPO Copyright Treaty can be found in its draft copyright directive: Amended proposal for a European Parliament and Council Directive on the harmonization of certain aspects of copyright and related rights in the Information Society, COM(1999)250 (May 1999).

The EU has decided that at least one new intellectual property law is needed to respond to challenges of the information age. It has directed member states of the EU to enact "sui generis" (of its own kind) legislation to provide intellectual property protection for the contents of databases.[22] The sui generis right gives those who have made substantial investment in collecting or maintaining a database an exclusive right to control unauthorized extractions and uses of 'more than an insubstantial part' of the database.[23] The EU has sought to persuade other nations to enact similar legislation.[24] Some have objected to an EU-style sui generis legal regime for databases because it would seem to grant exclusive rights in the data in databases and unduly impede the free flow of information and innovation.[25] The U.S. and Japan are among the countries now exploring an alternative approach to database protection that might adapt unfair competition principles to protect databases against market-destructive appropriations.[26] To appropriately tailor unfair competition principles to the needs of the database industry may also require new legislation.

Like database protection, the issue of safeguarding the privacy of personal information has generated varied responses from nations around the globe. The EU has been at the forefront of the legislative response to this issue: its Personal Data Directive implements a comprehensive regime which mandates that individuals be protected against unauthorized gathering and processing of personal information.[27] Other countries, including Canada, seem to agree that greater legal protection of personal data is necessary.[28] However, the U.S. has been resisting this policy initiative and urging self-regulation by industry as a better alternative.[29]

B. Proportionality

---

[22] European Parliament and Council Directive 96/9/EC of 11 March 1996 on the Legal Protection of Databases, 1996 O.J. (L 77) 20 [hereinafter "Database Directive"].

[23] Database Directive, *supra* note 22, Art. 7.

[24] Database Directive, *supra* note 22. The EU has been trying to persuade the international community to adopt its database regime ever since the WIPO diplomatic conference in Geneva, in December of 1996: Proposal Submitted by the European Community and Its Member States for the Sixth Session of the Committee of Experts on a Possible Protocol to the Berne Convention, WIPO Doc. BCP/CE/VI/13 (Feb. 1, 1996). See Pamela Samuelson, *The U.S. Digital Agenda at WIPO*, 37 VA. J. INT'L. L. 369 (1997) (for an account of this effort) [hereinafter Digital Agenda].

[25] J.H. Reichman & Pamela Samuelson, *Intellectual Property Rights in Data?*, 50 VAND. L. REV. 51, 84-95 (1997).

[26] There are currently two database protection measures before the U.S. Congress: the Collections of Information Antipiracy Act, H.R. 354, 106th Cong. (1999); and the Consumer and Investor Access to Information Act of 1999, H.R. 1858, 106th Cong. (1999).

[27] European Parliament and Council Directive 95/46/EC of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O. J. (L 281) 31 [hereinafter "Personal Data Directive"].

[28] The Canadian privacy legislation has not yet passed, but was amended by the House of Commons on February 7, 2000 after Third Reading in the Senate. See, The Personal Information Protection and Electronic Documents Act, Bill C-6, 2nd session 36th parl. (1999). Information on this legislation is available at <http://e-com.ic.gc.ca/english/privacy/632d1.html#privup>. The legislation is designed to promote ecommerce by protecting online privacy.

[29] See, e.g., Joel R. Reidenberg, *Restoring Americans' Privacy in Electronic Commerce*, 14 BERKELEY TECH. L. J. 771 (1999); PETER P. SWIRE AND ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE (1998).

Once it is clear that new legislation is needed, a second challenge for policymakers is to adopt a reasonably proportionate response to resolve the problems. Even when correct in concluding that some new legal protection may be desirable, legal decisionmakers are not always as careful as they should be about adopting a legislative "cure" that fits the dysfunction it aims to fix. Sometimes overreaction is due to legal decisionmakers having oversimplified the nature of the problem, singling out a single cause, for example, when the problem may have multiple causes. Sometimes overreaction may arise when legal decisionmakers are unclear about what an effective approach would be.

Consider, for example, the problem of indecent speech on the Internet. To protect children against harmful exposures to indecent material on the Internet, the U.S. Congress enacted the Communications Decency Act[30] which the U.S. Supreme Court eventually ruled was unconstitutional in *Reno v. ACLU*.[31] The Supreme Court had no quarrel with the idea that protecting children against obscene and indecent speech was an important governmental interest. However, it decided that the CDA provisions at issue in that case were not narrowly tailored to achieve that legitimate interest.[32] The provisions were so broad that they interfered with the free speech rights of adults to engage in frank discussions on the Internet that might include some statements that would be indecent as to children. The Supreme Court said that Congress couldn't constitutionally reduce the level of discourse on the Internet to that suitable for small children.[33] In the aftermath of this decision, the U.S. Congress passed the Child Online Protection Act (COPA) to regulate the distribution of material "harmful to children" on commercial websites.[34] This too has been challenged as unconstitutionally overbroad.[35]

The predominant view in the U.S. is that both the European database directive and the personal data protection directive are examples of disproportionately overprotective legislation that would better be handled with more limited measures.[36] Giving database makers exclusive rights to control extractions of data may, for example, unduly impede legitimate businesses that make use of data generated by another firm. Internet search engines, for example, rely on indexes created by analyzing the contents of websites, which inevitably involves the extraction of data from websites and the reuse of these data in constructing the indexes. American commentators tend to criticize the European directive on personal data protection as overbroad, unnecessary in many instances in which firms have incentives to protect personal data, and unsuitable to the emerging technological environment in which data and data processors are widely distributed rather

---

[30] Communications Decency Act of 1996, 47 U.S.C.A. §223 (Supp. 1997).
[31] 117 S.Ct. 2329 (1997).
[32] *Id.* at 2348.
[33] *Id.* at 2346.
[34] Child Online Protection Act, Pub. L. No. 105-277, 112 Stat. 2681-736 (1998).
[35] American Civil Liberties Union v. Reno, 31 F.Supp.2d 473 (E.D.Pa. 1999) (granting preliminary injunction blocking enforcement of the law).
[36] Database Directive, *supra* note 22; Personal Data Directive, *supra* note 27.

than being situated in one place as was true in the mainframe computer era on which the data protection regulations seem to be based.[37]

One reason that the Clinton administration's policy document, *A Framework for Global Electronic Commerce,* proposed that regulation should be "predictable, minimalist, consistent, and simple" was to avoid disproportionate legislative actions likely to create more problems than they can solve.[38] The wise approach may be to adopt a minimalist approach first, and only if experience proves that more regulation is needed should one amend the law to deal with the residual abuses.

C. Flexibility

More difficult to achieve than proportionality is the challenge of developing legal norms capable of adaptation to a rapidly changing technological and business environment. Yet another reason to enact laws that are "predictable, minimalist, consistent and simple" is that such laws may be more flexible and adaptable than those that are more complex and ambitious. Not even the most visionary of computer scientists can predict how technology will evolve, how this evolution will affect business organizations, and how innovative entrepreneurs will use information technology to transform their businesses and invent new business models. How, then, can legal decisionmakers expect to devise laws that will promote the new economy?

One strategy for building adaptability into law is to devise laws that are as "technology-neutral" as possible. For a legislature to adopt, for example, a digital signature law that endorses a particular technology may be a mistake for at least two reasons: first, because such a law is likely to become outmoded as technology evolves; and second, because such a law may unwittingly tilt the market so as to benefit certain developers to the detriment of competitors who offer a different solution, as well as the public who might have preferred that other technology if given a chance.[39]

Another strategy may be to construct laws that are simple and minimalist in character. Compare, for example, the Uniform Electronic Transactions Act (UETA) and the Uniform Computer Information Transactions Act (UCITA), two proactive state legislative initiatives aimed at regulating electronic commerce.[40] UETA validates contracts entered into electronically, and validates electronic signatures.[41] That is, if a state's laws require a "signature" for contracts to be valid, UETA says that an electronic

---

[37] See, e.g., SWIRE & LITAN, *supra* note 29, at 50.
[38] See WILLIAM J. CLINTON & ALBERT GORE, JR., A FRAMEWORK FOR GLOBAL ELECTRONIC COMMERCE 3 (1997), *available at* <http://www.iitf.nist.gov/eleccomm/ecomm.htm>, [hereinafter FRAMEWORK].
[39] See, e.g., Jane K. Winn, *Open Systems, Free Markets, and Regulation of Internet Commerce*, 72 TULANE L. REV. 1177 (1998).
[40] UNIFORM COMPUTER INFORMATION TRANSACTIONS ACT (final draft as of November 1, 1999) *available at* <http://www.law.upenn.edu/bll/ulc/ucita/ucitanc.htm> [hereinafter UCITA]; UNIFORM ELECTRONIC TRANSACTIONS ACT (1999) *available at* < http://www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm > [hereinafter UETA].
[41] UETA, *supra* note 40, § 7.

signature will suffice.[42] UCITA establishes rules for commercial transactions in computer-readable information. It too validates electronic contracts, but contains some differing and more complicated standards for formation of electronic information contracts (in contrast to transactions involving other subject matter).[43]

Of the two laws, I predict UETA will be more successful over time. This is in part because it is predictable, minimalist, consistent, and simple, and in part because it doesn't endorse any particular technological approach. UCITA is very complex, difficult to predict in important ways, and very ambitious in the wide range of activities and subject matter it aims to regulate. In addition, it gives special advantages to those who choose certain technological approaches over others.[44] Its electronic contracting rules are, moreover, inconsistent with those of UETA. This will almost certainly create confusion, particularly when a transaction involves both computer information covered by UCITA (e.g., software) and goods covered by UETA (e.g., a computer).

A third thing to watch for is making legislation in advance of technological developments. UCITA, for example, contains rules about contracts made by "electronic agents" (i.e., computer programs that a person can program to seek out information or resources of a particular kind and negotiate contracts with other electronic agents through the exchange of electronic messages).[45] Many companies are working on developing electronic agents; however, this technology is still very immature and it is not yet clear that electronic agents will be a significant force in electronic commerce. One might argue that UCITA does a service by adopting rules that will validate electronic agent contracting, or one might argue that the law should wait until commercial practice with use of electronic agents provides a firmer basis on which to make judgments about how the law should be configured to deal with this new phenomenon.

One of the foremost scholars of commercial law has observed that commercial law rules should be "accurate" (i.e., reflective of the way commercial transactions are actually conducted), not "original" (i.e., invented by a smart law professor perhaps out of his imagination).[46] As laudable as it may be to aspire to make commercial law rules accurate (as well as making them simple and technology neutral), the reality today is that rapid change may require evolving rules to deal with an evolving business market place. Simpler rules are more likely than complex rules to be adaptable to changing circumstances. Both UETA and UCITA should be studied carefully by policymakers

---

[42] *Id*., § 7(d)

[43] UCITA, *supra* note 40, § 103(b) (explaining the applicability of the Act to 'computer information transactions' when those transactions also involve other subject matter). See also § 103(d) (listing specific transactions and subject matter that are excluded from the Act).

[44] See, e.g., Amelia H. Boss, *Searching for Security in the Law of Electronic Commerce*, 23 NOVA L. REV. 585 (1999).

[45] See Michael Froomkin, *Article 2B as Legal Software for Electronic Contracting – Operating System or Trojan Horse?,* 13 BERKELEY TECH. L.J. 1023 (1998).

[46] Grant Gilmore, *On the Difficulties of Codifying Commercial Law*, 57 Yale L.J. 1341 (1951). For a comprehensive overview of the many problems with UCITA, see generally: Symposium, *Intellectual Property and Contract Law in the Information Age: The Impact of Article 2B of the Uniform Commercial Code on the Future of Transactions in Information and Electronic Commerce*, 13 BERKELEY TECH. L. J. 809 (1998) and 87 CAL. L. REV. 1 (1999).

outside of the U.S. because it is quite likely that U.S. companies and officials will eventually try to persuade other countries to adopt similar laws to promote electronic commerce.[47]

### D. Preserving Values

Technological and economic developments have made it more difficult to ensure that certain societal values, such as those favoring privacy, innovation, and freedom of expression, will continue to be preserved. Computer- and Internet-based technologies, for example, threaten privacy because they make it very inexpensive and easy to collect and process information about individuals.[48] These technologies allow the gathering of data in a manner that is often invisible to the individual concerned. These data can then be automatically compiled and cross-correlated with data on the individuals derived from different sources (a practice known as "data mining") to amass virtual libraries of personal data. When an Internet user visits a commercial website, for example, the host of that website can use technology to glean information about the individual based on what the individual does at the site and how his browser is set. It can also plant "cookies" (identifying digital information) on the user's computer so that the host site can more easily keep track of who is (re)visiting its site.[49] Upon a second visit, the host system will check the user's cookies file to determine if the user has been there before and may add new cookies to the file. With usage-, browser-, and cookie-based information, sites can compile profiles of users.[50] The economic pressure on data privacy arises from the fact that compilations of personal data can be very valuable. Many firms exploit user data not only by using it to market new products to the users, but they may also sell user data to other firms seeking to sell their products or services to people with certain characteristics.[51]

In a valiant effort to counteract technological and economic pressures on individual privacy, the E.U. has developed a comprehensive set of rules to protect personal data against unauthorized reuses or processing by private sector entities.[52] These rules derive in part from previously issued guidelines such as those published by the Organization for Economic Cooperation and Development (OECD).[53] Although the

---

[47] See e.g., Pamela Samuelson and Kurt Opsahl, *Licensing Information in the Global Information Market: Freedom of Contract Meets Public Policy*, 21 E.I.P.R. 386 (1999).

[48] See, e.g., Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 Stan. L. Rev. 1193, 1198-99 (1998).

[49] *Id*. at 1227-8.

[50] See e.g., Opening Remarks of FTC Chairman Robert Pitofsky, Public Workshop on Online Profiling, November 8, 1999, available at http://www.ftc.gov/opa/1999/9911/onlinepitofsky.htm.

[51] *Id*. See also, NATIONAL TELECOM. & INFO. ADMIN., U.S. DEPT OF COMMERCE, PRIVACY AND THE NII: SAFEGUARDING TELECOMMUNICATIONS-RELATED INFORMATION 15-16 (1995) (Appendix A on business of marketing profiles).

[52] Personal Data Directive, *supra* note 27.

[53] See, e.g., PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW: A STUDY OF UNITED STATES DATA PROTECTION (1996), (detailing origins of the EU personal data directive); Graham Greenleaf, *Stopping Surveillance: Beyond 'efficiency' and the OECD*, 3 PLPR 148 (1996) *available at* <http://www2.austlii.edu.au/itlaw/articles/efficiency.html> (Personal Data Directive grew out of the OECD privacy Guidelines and the Council of Europe privacy Convention).

U.S. purports to support the OECD privacy guidelines, information industry organizations in the U.S. have thus far blocked new privacy legislation, except as to online gathering of information from children.[54] While some commentators predict that technology (e.g., anonymizing browsers) can help to solve the cyberspace privacy problem,[55] others believe the law will have to play a role.[56] The law might, for example, need to require the use of anonymizing technologies to protect intellectual privacy in the future.[57]

Another information policy area in which preservation of social values is at stake is encryption policy.[58] A recent lawsuit, *Bernstein v. United States,* seeks to protect and even extend societal free speech values.[59] Bernstein is a computer scientist who wrote an encryption program which he wanted to share with his students and colleagues and post on his website. The U.S. government has insisted that these acts would "export" a "munition" in violation of U.S. export control laws.[60] Bernstein challenged the constitutionality of these laws as applied to his software, claiming that he has free speech rights under the First Amendment to the Constitution to express himself by writing and sharing his encryption software with others.[61] So far the courts have agreed with him (although an appellate decision was later withdrawn and the case has now been remanded to the trial court to consider the implications of the government's recent liberalization of encryption regulations).[62] Outside the United States, as well as inside, the possible role of encryption in protecting the privacy of electronic correspondence means that encryption policies should be especially important to those countries, such as the members of the E.U., who value privacy as a fundamental human right.[63]

A third policy area posing preservation of societal value challenges is the struggle over preserving fair use rights when copyright owners use technical protection systems to guard digital versions of their works from unauthorized copying.[64] Some, including this author, interpret the U.S. Digital Millennium Copyright Act (DMCA) as allowing

---

[54] Children's Online Privacy Protection Act of 1998, Pub. L. No. 105-277, 112 Stat. 2681-728 (1998).
[55] See, e.g., Developments in the Law—The Law of Cyberspace, 112 HARVARD L. REV. 1574, 1644-1648 (1999), *available at* <http://www.harvardlawreview.org/issues/download/5-99-DEVO.pdf>.
[56] See, e.g., Reidenberg, *supra* note 29.
[57] See, e.g., Julie E. Cohen, *The Right To Read Anonymously: A Closer Look at Copyright Management in Cyberspace*, 28 CONN. L. REV. 981 (1996) (suggesting that the law may need to require anonymizing features in copyright management systems).
[58] Michael Froomkin, *The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. Pa. L. Rev. 709 (1995).
[59] 176 F.3d 1132 (9th Cir. 1999).
[60] Export Administration Regulations, 15 C.F.R. Pts. 730-74.
[61] *Bernstein*, *supra* note 59 at 1139-41 (discussing the status of encryption software as 'speech').
[62] Bernstein v. U.S. Dept. of State, 974 F.Supp. 1288 (N.D.Cal. 1997), *aff'd*, 176 F.3d 1132 (9th Cir. 1999), *reh'g granted, withdrawn*, 192 F.3d 1308 (9th Cir. 1999). The rehearing en banc was later withdrawn in favor of rehearing by the original panel in the dispute.
[63] See, e.g., Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, art. 8(1), Europ. T.S. No. 5 *available at* < http://www.coe.fr/eng/legaltxt/5e.htm> ("Everyone has the right to respect for his private and family life, his home and his correspondence."). The Convention has 41 ratifications and entered into force on September 3, 1953.
[64] See, e.g., Digital Agenda, *supra* note 24.

circumvention of a technical protection system in order to engage in fair use,[65] although it is less clear whether fair use circumventors have an implied right to make software necessary to accomplish fair use circumventions.[66] However, one recent decision takes the view that fair use does not apply in cases involving anti-circumvention regulations because the purpose of the DMCA is to prevent the circumvention of technical protection measures and has nothing to do with guarding against copyright infringement.[67]

A similar struggle is occurring over fair use rights and contract law. One of the most contentious issues in the U.S. debate over UCITA has been whether courts should enforce terms of mass-market licenses when the terms prohibit activities that would otherwise be considered fair uses under U.S. copyright law. UCITA seems to presume that such terms are enforceable, but some commentators believe that copyright policy should override contract law in this situation.[68] Behind both of these struggles are concerns about preserving the public sphere, in which information is accessible to all, and in which learning, speech and thought can occur without the threat of private control or censorship.

### E. Transnational Cooperation

One obvious fact about the Internet is the global character of its reach. While it is unquestionably true that a great deal of trade is international, the physicality of tangible goods, such as automobiles, vacuum cleaners, and television sets, makes it easy to apply territorially based rules to them. German law, for example, can easily be applied to a transaction involving bicycles that takes place entirely on German soil, but what law applies if unlawful information (e.g., pornography or copyright infringement) is uploaded to a computer in Germany and downloaded in the U.S. or in Belgium? If two electronic agents, one representing a German client and one representing a U.S. client, "meet" in cyberspace, exchange messages, and the U.S. electronic agent thinks a contract has been formed, whose law will be used to judge the validity and terms of the contract? It is well known that laws vary from nation to nation on such issues. Variations in national laws may interfere with the growth of electronic commerce, as well as other desired objectives. The question is: how can nations work together to find enough common ground on the private law of the Internet to promote e-commerce and other beneficial exchanges of information?

As desirable as complete harmonization of laws may seem in the abstract, achieving harmonization is likely to be a tediously slow process. Consider, for example, that almost a decade of meetings preceded the diplomatic conference which produced the WIPO Copyright Treaty adapting copyright rules as to digital works.[69] When

---

[65] See Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to be Revised,* 14 BERKELEY TECH. L. J. 519, 538-43 (1999).
[66] *Id*. at 547-57.
[67] Universal City Studios Inc. v. Reimerdes, No. 00 Civ. 0277 (LAK) (S.D.N.Y. February 2, 2000).
[68] See UCITA, *supra* note 40, § 105; Mark A. Lemley, *Beyond Preemption: The Law and Policy of Intellectual Property Licensing*, 87 CALIF. L. REV. 111 (1999) (suggesting that contractual overrides to fair use rights should sometimes be considered a misuse of copyright).
[69] See, e.g., Digital Agenda, *supra* note 24 at 375.

harmonization is infeasible (or perhaps as a step toward harmonization) nations may agree on policy guidelines to inform the legal rules nations eventually develop. The OECD has been active in promoting this form of international cooperation.[70] Guidelines may not lead to uniformity, however, in part because countries that endorse guidelines sometimes do not actually implement them.[71] Guidelines may also be implemented in inconsistent ways. Yet even inconsistent implementations of rules based on guidelines may be better than the chaos of complete disharmony.

Differences in national culture and legal traditions may make it difficult to attain consensus on the fine details of legal rules on an international basis. Nevertheless, numerous international efforts, such as those undertaken by the United Nations Commission on International Trade Law (UNCITRAL), offer some promise for evolving harmonized rules to promote electronic commerce over the Internet.[72]

Another way to achieve harmony on a global scale may be for one nation to propose legal rules that it urges other nations to adopt. This may be a faster path to harmonization than the laborious consensus process that typifies treatymaking. Both the U.S. and the E.U. have used this approach to international lawmaking for the Internet, in particular as to global electronic commerce. The U.S. White Paper on Intellectual Property and the National Information Infrastructure, for example, proposed digital copyright rules virtually identical to the treaty proposals the Administration submitted to WIPO at more or less the same time.[73] The Clinton Administration's proposed rules became the baseline for discussion, even if they were ultimately transformed in the course of the U.S. legislative and international treatymaking process.[74]

The E.U. has sought to persuade other nations to adopt its database and personal data protection regimes through the "stick" of reciprocity-based rules. The E.U. will not protect the databases of non-E.U. nationals unless other countries adopt the same or a very similar law.[75] And unless other nations provide what the E.U. considers to be "adequate" protection to personal data, the E.U. has announced its intent to stop transnational data flows into and out of the offending country. Reciprocity-based provisions as a means to achieve harmonization have been the subject of heated debate, much of it emanating from the U.S.[76] The E.U. has, of course, a legitimate interest in attempting to ensure that the objectives of its laws will not be subverted by computer

---

[70] See, e.g., Cryptography Policy: The Guidelines And The Issues, The OECD Cryptography Policy Guidelines And The Report On Background And Issues Of Cryptography Policy, March 1997, OECD Doc. OCDE/GD(97)204; and O.E.C.D., Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, O.E.C.D. Doc. C58 (final) (Oct. 1, 1980), reprinted in 20 I.L.M. 422 (1981), available at <http:// www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.htm> [hereinafter OECD Guidelines].

[71] See, e.g., Reidenberg, *supra* note 29 at 773-4 (Clinton administration has cited the OECD Guidelines, *supra* note 70, as the basis for all American privacy laws, but American legislators have refused to implement comprehensive or meaningful standards).

[72] Boss, *supra* note 44.

[73] See, e.g., Digital Agenda, *supra* note 24.

[74] *Id*.

[75] Database Directive, *supra* note 22, Art. 11 and Declaration (56).

[76] See, e.g., SWIRE & LITAN, *supra* note 29.

processing of personal data outside its borders. However, reciprocity-based rules may not be an appropriate way to induce other countries to follow the lead of one country's law.[77] An "adequacy" approach may enable countries to develop their own means to achieve the same results.[78]

Perhaps nations should work towards achieving "policy interoperability" (that is, agreeing on goals a policy should achieve, while recognizing that nations may adopt somewhat different policy means to implement the goals). Policy interoperability, rather than reciprocity, may be especially important to those countries who seek to preserve the uniqueness of their social values within the framework of thriving global e-commerce. Policy interoperability also allows room for flexible approaches that can be tailored to the unique economic needs of each nation, while simultaneously avoiding the threat that incompatible national regulatory regimes will derail the unique benefits of convergence and globalization that the Internet offers. In addition, policy interoperability may foster a cooperative environment in which countries feel that their international obligations enhance, rather than erode, their valid national interests. Such an environment is less likely to lead countries to turn to the World Trade Organization (WTO) to determine whether attempts to force regulatory reciprocity represent non-tariff barriers to trade and are in violation of international trade agreements.[79] As some commentators have observed, it is not clear that settling such disputes before an organization concerned solely with international trade would result in policies that reflect the complex set of concerns that will create a livable Global Information Society.[80]

Despite the many international initiatives to develop international consensus on the law of the Internet,[81] some dangers clearly lurk in the international arena. Some arise from the ability of major multinational firms to engage in what Professor Froomkin describes as "regulatory arbitrage," in which firms play some nations off against others as a way to get acceptance of rules that the multinational firm prefers.[82] Also dangerous are potential races to the bottom (that is, contests over which nation will adopt the least restrictive rules and attract the most commercial activity as a result), or races to the top (who can adopt the toughest rules that will become a baseline for applying pressure to get international adoption by others?).[83] Much as countries may wish to take some time to think through what laws should be used to regulate the Internet, there is a sense of urgency about putting in place a legal and policy infrastructure to promote electronic

---

[77] Charles R. McManis, *Taking TRIPS on the Information Superhighway: International Intellectual Property Protection and Emerging Computer Technology*, 41 VILL. L. REV. 207 (1996).

[78] If the E.U. could be persuaded that U.S. firms would effectively self-regulate, it wouldn't matter if the U.S. did not implement a legislative solution, because adequate protection would still exist.

[79] SWIRE & LITAN, *supra* note 29 at 190-94.

[80] SWIRE & LITAN, *supra* note 29 at 194.

[81] See, e.g., U.S. GOVERNMENT WORKING GROUP ON ELECTRONIC COMMERCE, FIRST ANNUAL REPORT, at *iii-iv* and 5-8 (Nov. 1998) *available at* <http://www.doc.gov/ecommerce/E-comm.pdf> (referring to international meetings and working groups on e-commerce policy).

[82] See A. Michael Froomkin, *The Internet as a Source of Regulatory Arbitrage* in BORDERS IN CYBERSPACE (Brian Kahin & Charles Nessen, eds. 1997), *abstract available at* <http://personal.law.miami.edu/~froomkin/articles/arbitr.htm>.

[83] An example of the latter is the Clinton Administration's effort to persuade other countries to adopt the anti-circumvention rules of the DMCA as an appropriate implementation of the WIPO Copyright Treaty.

commerce and other exchanges of information via the Internet. The fear is that those who wait too long will be left behind in the global information economy. Perhaps this fear can have constructive consequences in motivating countries to work together to achieve the minimum level of consensus needed for electronic commerce to flourish.

## IV. Conclusion

The Internet has generated considerable interest not only among the millions of people who use it every day, but also among legal policy makers. The law of the Internet is still in the process of evolving. While ever more legal rules are being applied, adapted, and adopted to govern activities occurring via the Internet, there is every reason to expect that additional legal rules will need to be formulated (and reformulated) as technology advances to enable previously unimaginable activities, including new business models for producing and distributing products and services.

Information may be the principal commodity of an information economy in an information age, but policymakers need to realize that information is not just a commodity. It is also an essential input to innovation, knowledge creation, education, and social and political discourse. If information is commodified too much, these social values may be impaired. Policymakers need to realize that the information policies they adopt now in relation to the Internet will have profound effects on the information society that will result from these actions. Lawyers and legal scholars can help to formulate information policies that will produce an information society that we would actually like to live in.