Standardizing Government Standard-Setting Policy for Electronic Commerce[1]

Mark A. Lemley[2]

The Magaziner Report[3] contains strong language concerning the proper development of technological standards for electronic commerce. Consistent with its general anti-government tenor, the Report takes a strong position against government standard-setting in its section on Technical Standards.[4] Somewhat more surprisingly, the Report also takes the position that technical standards should be open and promote interoperability,[5] and strongly suggests that the standards be set by industry groups rather than individual companies.[6]

Unfortunately, an examination of government policy towards electronic commerce reveals that the government's actual approach to standard-setting is internally inconsistent. Further, the broad general endorsement of open standards in the Report

---

[2] Professor of Law, University of Texas School of Law; of counsel, Fish & Richardson, P.C. Thanks to Rose Hagan and the participants in the Berkeley Center for Law and Technology conference on the Legal and Policy Framework for Global Electronic Commerce for comments on an earlier draft.

[3] WILLIAM J. CLINTON & ALBERT GORE, JR., A FRAMEWORK FOR GLOBAL ELECTRONIC COMMERCE (1997), available at <http://www.ecommerce.gov/framewrk.htm> (visited March 13, 1999) (hereinafter MAGAZINER REPORT or simply the REPORT).

[4] *See id*. §9 ("The United States believes that the marketplace, not governments, should determine technical standards . . . "); *see also id*. Background (referring to governmental control over standards development as a "[p]otential area[] of problematic regulation").

[5] *See id.* ("Standards are critical . . . as they can allow products and services from different vendors to work together"; "the marketplace . . . should determine technical standards and other mechanisms for interoperability"; "Numerous private sector bodies have contributed to the process of developing voluntary standards that promote interoperability.").

[6] *See id.* ("we urge industry driven multilateral fora to consider technical standards in this area"). The REPORT also endorses the standards model of the Internet Engineering Task Force (IETF), *see id*., more on this later. On the other hand, the REPORT does note that "in some cases, multiple standards will compete for marketplace acceptance." *Id.*

leaves a number of important issues unaddressed, including the role of intellectual property and antitrust law in standard setting. How these questions are dealt with in practice will have a significant impact on the way in which electronic commerce develops.

I. Network Effects and the Need for Standards

The Magaziner Report does not speak of standards for electronic commerce in a vacuum. Rather, it identifies a number of different areas where some sort of standard is necessary for electronic commerce to flourish. These areas include electronic payment systems (electronic funds transfers, ecash, smart cards and the like), security infrastructure (encryption standards), contract infrastructure (standards for authentication, integrity, and non-repudiation), telecommunications, and data interchange.[7]

Virtually all of these issues arise in markets characterized by network effects, usually fairly strong ones.[8] Thus, the interoperability of global telecommunications systems is obviously a precondition to international electronic commerce; if data from a buyer's system can never reach a seller's system, there can be no transaction. Similarly, electronic commerce between a particular buyer and a particular seller requires them to

[7] *Id.*

[8] Network effects occur when the value to each consumer of a particular product is in part a function of how many other consumers buy that product. A good example is the telephone, which has no value to consumers unless it connects them to other people, preferably as many as possible. For a detailed discussion of network effects and law, see Mark A. Lemley & David McGowan, *Legal Implications of Network Economic Effects*, 86 CAL. L. REV. 479 (1998) [hereinafter Lemley & McGowan, *Network*].

agree on a method of payment, a method of assuring performance, a method of security, and a method of product delivery.[9]

It is possible, of course, to design such agreements for each transaction on an ad-hoc basis. Early electronic commerce has sometimes taken this form. In the absence of a widely used email encryption program, for example, particular parties in an ongoing business relationship (say, lawyers and clients) will sometimes agree on an encryption mechanism for communications between them. But there are strong social benefits to having most parties use the same system, just as there are strong benefits to having most computer users work on the same operating system or word processing program. If everyone used the same encryption system, or the same standards for data downloads, electronic commerce would be cheaper and easier than in a world without a dominant standard. The benefits are even more stark where there is not much intrinsic difference between competing standards. There may be no inherent reason to prefer one brand of smart cards to another, for example, but there are certainly strong benefits to having a smart card that works in a large variety of vendors' machines.

In short, much of the infrastructure of electronic commerce would benefit from uniform standards. There are three basic ways to produce such standards. First, the government can mandate the choice of a particular standard, as happened historically in telecommunications and broadcasting. Second, industry players can come together in a standard-setting organization to select a single standard on which they will base their

[9] Parties can and do conduct electronic commerce without agreeing on all of these things expressly, but that simply means either that there is implicit acquiescence to a particular standard (the use of a credit card number, for example, or an "agreement" that the transaction will not be encrypted) or that the parties haven't considered the issue yet. For an argument that electronic cash has been unsuccessful largely because credit cards are being used online with great frequency, see John D Mueller, *Selected Developments in the Law of Cyberspace Payments*, 54 BUS. LAWYER 403, 406-07 (1998).

products. Finally, if the economic incentives for standardization are strong enough, no one needs to "choose" a standard at all: the market will "tip" to favor one particular product (a new *de facto* standard) at the expense of competing products.[10] Each approach has advantages and disadvantages.[11]

II. Government Participation in Setting Electronic Commerce Standards

The Magaziner Report takes a strong position against government-imposed standard setting for electronic commerce. It includes strong rhetoric on the importance of standards being set in the marketplace, not by a bureaucracy. This rhetoric seems to be directed abroad more than at home. Indeed, the First Annual Report of the U.S. government's Working Group on Electronic Commerce touts as a major accomplishment a resolution it pushed at the Global Standards Conference in 1997 in which participants agreed to let the private sector lead in standard-setting.[12] While there is talk of a limited role for government science agencies in facilitating development of open standards,[13] a reader of the Magaziner Report could be forgiven for thinking that the major project of the government in setting Internet standards will be to get out of the way.

Despite this strong rhetoric, the Administration has shown no hesitation in jumping into the standard-setting process when doing so would further its substantive

[10] For a discussion of tipping, see Michael L. Katz & Carl Shapiro, *Network Externalities, Competition, and Compatibility*, 75 AM. ECON. REV. 424 (1985).

[11] For a fuller explanation, see Mark A. Lemley, *Antitrust and the Internet Standardization Problem*, 28 CONN. L. REV. 1041 (1996) [hereinafter Lemley, *Standardization*]; *see generally* Lemley & McGowan, *Networks supra* note 8 (discussing the implications of network effects for law).

[12] U.S. GOVERNMENT WORKING GROUP ON ELECTRONIC COMMERCE, FIRST ANNUAL REPORT, at Executive Summary (Nov. 1998) [hereinafter ANNUAL REPORT].

goals. The most glaring example involves encryption policy. The government has for many years tried every means at its disposal, short of an outright ban, to prevent industry from coalescing around a strong encryption standard.[14] The Report claims that it is "encouraging the development of a voluntary, market-driven key management infrastructure," or at least that "in partnership with industry, [it] is taking steps to promote the development of market-driven standards."[15] This is nonsense. For several years, the government has "encouraged" key escrow encryption by refusing to let industry export anything else[16] and by refusing to buy products that don't meet its idea of a proper standard.[17] Even today, in a period of liberalization, the government still prohibits general commercial export of strong encryption products.[18] One can agree or disagree with the government's arguments against strong encryption and in favor of a back door for law enforcement. I, for one, am largely agnostic on the subject. However, it is clear that government has hardly left voluntary standard setting to take its course.

---

[13] *Id.* at Progress on the Presidential Directive (discussing several facilitative roles for the National Institute of Standards and Technology).

[14] For an early description of this fight, see A. Michael Froomkin, *The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709 (1995); *see also* A. Michael Froomkin, *It Came From Planet Clipper: The Battle Over Cryptographic Key "Escrow,"* 1996 U. CHI. LEGAL F. 15.

[15] MAGAZINER REPORT, *supra* note 3, §9.

[16] For cases discussing the government's regulation of encryption under the International Trafficking in Arms Regulations, *see* Bernstein v. U.S. Dept. of State, 945 F. Supp. 1279 (N.D. Cal. 1996); Junger v. Daley, 8 F. Supp. 2d 708 (N.D. Ohio 1998); Karn v. U.S. Dept. of State, 925 F. Supp. 1 (D.D.C. 1996).

[17] For a discussion of the government procurement policies related to key escrow encryption, see Howard S. Dakoff, Note, *The Clipper Chip Proposal: Deciphering the Unfounded Fears that Are Wrongfully Derailing Its Implementation*, 29 JOHN MARSHALL L. REV. 475, 482-84 (1996). Of course, supporting a standard in the marketplace is not the same as mandating choice of a particular technology. *See* Lemley & McGowan, *Networks*, *supra* note 8, at 544-45.

[18] *See* Stewart A. Baker, *Security and the Infrastructure for Electronic Commerce*, 14 BERKELEY TECH. L.J. __ (1999).

Two other examples help illustrate this point. First, the Administration pushed Congress for years to enact some sort of criminal copyright statute regulating the development of so-called "circumvention devices" that facilitate copying.[19] Indeed, its support for such a law is one of the centerpieces of the Magaziner Report.[20] The Administration finally succeeded in 1998, when Congress passed the Digital Millennium Copyright Act (DMCA).[21] The primary purpose of the DMCA is to intervene in the innovation marketplace, by imposing what one might call "unilateral technological disarmament" on designers of encryption-breaking systems.[22] Not only has the government once again intervened in the technological marketplace to promote its agenda, but it did so here in a way that is almost diametrically opposed to its efforts to push key escrow. One can perhaps discern a consistent government policy here -- something along the lines of "the U.S. government should have the means to break encryption, but no one else should" -- but it is hardly one consistent with the overarching principle that "the private sector should lead."[23]

---

[19] A circumvention device is one that effectively bypasses or disables a technological protection system designed to encrypt or restrict access to a piece of data, particularly a copyrighted work. *See generally* 17 U.S.C. § 1201(a)(1) (1998).

[20] MAGAZINER REPORT, *supra* note 3, §4.

[21] Digital Millenium Copyright Act, Pub. L. No. 105-304, 105th Cong., 2d Sess. (1998)

[22] For a superb analysis of this labyrinthine law, see Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to be Revised*, 14 BERKELEY TECH. L.J. __ (1999).

[23] MAGAZINER REPORT, *supra* note 3, §1.

Indeed, government policy in this area is sufficiently schizophrenic that Congress had to amend the original draft DMCA to provide an exception for law enforcement officials, who otherwise would be committing a crime by attempting to do what key escrow would allow them to do. 17 U.S.C. § 1201(e) (1998).

Finally, it is worth considering the Report's approach to telecommunications regulation. True, the government has pushed quite strongly for telecommunications deregulation both here and abroad. But the Report also indicates that government telecommunications policy must be founded in part on "guaranteeing open access to networks on a non-discriminatory basis."[24] I happen to think this is sound policy,[25] and it does leave a good deal of room for private companies to maneuver. But a policy of open interconnection certainly contemplates government setting, if not the actual technical standards for telecommunications companies, at least the framework for those standards.

III. Open vs. Closed Standards

The Mazaginer Report's commitment to open, interoperable standards in telecommunications raises a more general issue for technical standard setting: the role of intellectual property in standards. Computer software is eligible for patent, copyright, trademark and trade secret protection, as well as protection by contract.[26] While there is some debate over the scope of some of these rights as applied to industry standards, particularly copyright,[27] there seems no question today that a single company can at least

[24] MAGAZINER REPORT, *supra* note 3, §7.

[25] *See* Joseph Farrell, *Creating Local Competition*, 49 FED. COMM. L.J. 201, 211 (1996); Lemley & McGowan, *Networks*, *supra* note 8, at 551.

[26] *See generally* PETER S. MENELL ET AL., LEGAL PROTECTION FOR COMPUTER TECHNOLOGY (forthcoming 1999).

[27] Some courts, notably the First Circuit in *Lotus Dev. Corp. v. Borland Int'l*, 49 F.3d 807 (1st Cir. 1995), have held that standard protocols may be entirely ineligible for copyright protection. Even if an interface protocol is eligible for copyright protection, it may still lose protection against all but the most literal copying if a court concludes during its filtration analysis that virtually all of the elements of the interface are unprotectable. For example, in *Mitel*, the Tenth Circuit concluded that the arbitrary selection of code numbers in the operation of telephone call controllers was not sufficiently original to qualify for

own patent rights that dominate a standard[28] and probably copyright rights in a standard as well.[29] Recent developments make possible intellectual property ownership not merely of technical standards, but of entire business models in the electronic commerce environment.[30] The Magaziner Report generally endorses strengthening intellectual property rights in the electronic commerce environment.[31]

---

copyright protection. Mitel v. Iqtel, 124 F.3d 1366, 1373-74 (10th Cir. 1997). *But see* Atari Games Corp v. Nintendo of America, 975 F.2d 832, 840 (Fed. Cir. 1992) (holding that the arbitrary string of numbers in a lock-out device was not dictated by function and therefore could be copyrighted); American Dental Ass'n v. Delta Dental Plans, 126 F.3d 977 (7th Cir. 1997) (concluding that the listing of code numbers assigned to each element was a copyrightable part of a taxonomy of information, because different numbers could have been chosen).

Program interface elements will also be uncopyrightable if they are dictated by external factors, such as the requirements of compatibility with a particular hardware or software platform. Thus, the Tenth Circuit concluded that the selection of values matched to codes in Mitel's call controllers, while sufficiently original to qualify for copyright protection, could not be protected because they were dictated by the needs of the industry. *Mitel, supra*, 124 F.3d at 1366. *See also* Computer Assoc. Int'l, Inc. v. Altai, Inc., 982 F.2d 693, 707-09 (2nd Cir. 1992). On the other hand, other courts have found similar program elements to be copyrightable. *E.g. Atari*, 975 F.2d at 845*;* Engineering Dynamics, Inc. v. Structural Software, Inc., 26 F.3d 1335, 1347 (5th Cir. 1994); CMAX/Cleveland, Inc v. UCR, Inc., 804 F. Supp. 337, 355-56 (M.D. Ga. 1992).

[28] For a general discussion of patents that confer market control on software standards, see Julie E. Cohen, *Reverse Engineering and the Rise of Electronic Vigilantism: Intellectual Property Implications of "Lock-Out" Technologies*, 68 S. CAL. L. REV. 1091 (1995).

[29] For example, Microsoft's copyright in its operating system has served to give it effective control over the standards contained therein, despite questions as to whether Microsoft's applications program interfaces (APIs) are themselves copyrightable. *See* Mark A. Lemley & David McGowan, *Could Java Change Everything? The Competitive Propriety of a Proprietary Standard*, 43 ANTITRUST BULL. 715 (1998) [hereinafter Lemley & McGowan, *Java*]. In part, this results from uncertainty about the copyrightability of the APIs themselves. In part, however, it also reflects the technical difficulty of designing a compatible operating system given the constraints of copyright law. *See* Lemley & McGowan, *Networks*, *supra* note 8, at 527-30.

[30] *See* State St. Bank & Trust Co. v. Signature Fin. Group, 149 F.3d 1368 (Fed. Cir. 1998); *see also* U.S. Patent No. 5,790,793 (covering all Internet "push" technology); U.S. Patent No. 5,715,314 (covering electronic "shopping carts"); U.S. Patent No. 5,724,424 (covering a system of secure real time online payment); U.S. Patent No. 5,794,207 (covering buyer-priced auctions); U.S. Patent No. 5,794,210 (covering the concept of paying consumers to view ads).

[31] *See* MAGAZINER REPORT, *supra* note 3, §4 (endorsing the concept behind the DMCA, and encouraging patent protection for software and telecommunications inventions). *See also id.* §3 (supporting the development of U.C.C. article 2B (now the draft Uniform Computer Information Transactions Act), which would effectively provide new and broader forms of intellectual property-like protection). On the other hand, the Report does shy away from maximal protection in some areas: it is neutral on database protection, for example, and it encourages tougher reviews of software patent applications by the PTO. *Id.* §4.

It should be evident, however, that the goal of strengthening intellectual property protection is in some tension with the goal of promoting open standards for electronic commerce. While some intellectual property owners might choose to open their standards to competition -- Sun Microsystems has done so with Java, for example[32] -- as a rule intellectual property ownership in a de facto standard is inimical to open standard setting.[33] The way to achieve a truly open, interoperable standard is to put the standard itself in the public domain. TCP/IP and HTML are good examples of public domain standards that nonetheless inspire both collaborative work to improve the standards (in the Internet Engineering Task Force (IETF), among other places) and the development of proprietary content for and extensions to the standards. One can imagine a world in which Microsoft owned the intellectual property rights in both TCP/IP and HTML, but it is hard to believe that the course of Internet development would have been the same.

Standard-setting organizations do offer a potential way to preserve open standards despite the presence of intellectual property. Many standard-setting organizations, including the IETF, have by-laws that restrict the ability of members to own or assert intellectual property rights in standards adopted by the group. These rules take a variety of forms. Some groups ban the ownership of intellectual property rights in standards altogether. Other groups may impose rules forbidding a member from asserting intellectual property rights in the standard altogether, or at least from asserting them against another member. Both of these approaches amount in effect to a royalty-free

---

[32] *See* Lemley & McGowan, *Java*, *supra* note 29, at 750-753.

[33] Indeed, even in the case of Java one might reasonably be concerned that if the standard prevails, Sun will assert its intellectual property rights in the standard to close it to others. *See id.* at 769-772 (raising this concern, and suggesting ways to deal with it).

compulsory license. Still other groups allow members to retain intellectual property rights in a standard, but require that the intellectual property be licensed on "reasonable, nondiscriminatory terms" to those who wish to use the standard. Finally, some standard setting organizations merely require advance disclosure by members of any intellectual property rights that might cover a potential standard, so that the organization can use that information in deciding whether to adopt the proposed standard.

Such by-laws offer the possibility of preserving open standards even in a world of strong intellectual property rights. The by-laws are not without their limitations, however. First, their enforceability is limited. Standard-setting organization by-laws obviously cannot bind companies who are not members of the organization; a company that is large enough (or that has a strong enough intellectual property portfolio) may simply choose to go it alone and develop a proprietary standard. Further, there is some question as to how internal rules will be enforced against members that violate those rules. Will agreeing to license a patent on nondiscriminatory terms actually bar a patent owner from filing suit for infringement? Will it simply limit her remedies? Or is such an agreement simply a contractual obligation enforceable only in a separate suit? Similarly, how can members of a standard-setting organization enforce a by-law that requires only disclosure of intellectual property rights, but not relinquishment or licensing of those rights? These are complex questions, and the law so far doesn't have entirely satisfactory answers.[34] This uncertainty may make it hard to keep a standard open in the face of a determined effort by an intellectual property owner to close it.

[34] Figuring out what the answers should be would take far more space than I have here. I hope to embark on this project in the near future.

Furthermore, the antitrust laws may restrict the rules standard-setting organizations can impose and enforce. A number of recent cases suggest that standard-setting organizations may not be free to compel members to license their intellectual property rights. One case, *Addamax v. Open Software Foundation,*[35] went so far as to hold that the collective action of competitors in a standard-setting organization might itself violate the antitrust laws. While this case seems wrongly decided,[36] it may serve to deter standard-setting organizations from regulating member behavior at all. Further, standard-setting organizations which negotiate with patent owners on behalf of their members risk being characterized as a buyer's cartel trying to coerce a license at an artificially low price. The Antitrust Division has even taken action against the European Telecommunications Standards Institute for compelling members to relinquish claims of ownership in the standards it promulgates.[37] Finally, the Federal Trade Commission and a private company recently filed actions against Intel alleging that Intel wrongfully retaliated against intellectual property owners that sued it by barring their access to Intel's

---

[35] 888 F. Supp. 274, 281, 284 (D. Mass. 1995).

[36] *See* Lemley, *Standardization*, *supra* note 11, at 1080-90 (arguing that standard setting organizations should not be subject to antitrust liability in network markets unless they restrict rather than promote access to a standard).

[37] In a series of negotiations regarding rules promulgated by the European Telecommunications Standards Institute (ETSI), the United States put substantial pressure on ETSI to back down from its original rule requiring disclosure and nondiscriminatory licensing of member intellectual property rights embodied in ETSI standards. For discussions of the evolution of ETSI intellectual property rules, see Cortien Prins & Martin Schiessl, *The New Telecommunications Standards Institute Policy: Conflicts Between Standardization and Intellectual Property Rights*, 8 EUR. INTELL. PROP. REV. 263 (1993); Mark Shurmer & Gary Lea, *Telecommunications Standardization and Intellectual Property Rights: A Fundamental Dilemma?*, in STANDARDS POLICY FOR INFORMATION INFRASTRUCTURE 391-96 (Brian Kahin & Janet Abbate eds., 1995).

Ironically enough, the Federal Trade Commission has taken the opposite position, bringing action against a member of a standard setting group that asserted patent rights in a group standard in violation of the organization's by-laws. *See In re* Dell Computer Corp., No. 931-0097 (F.T.C. 1996). It seems odd to argue both that standard setting rules violate the antitrust laws, and that failing to comply with those rules violates the antitrust laws.

own intellectual property.[38] While these last cases don't directly concern standard setting organization rules, they may give such groups some hesitation about attempting to coerce compliance with their rules.

In short, we cannot be confident that standard-setting organizations can maintain open standards in the face of strong intellectual property rights governing those standards. As the number of companies that claim to own part or all of a standard increases, so does the likelihood that the standard produced by the marketplace will be owned by one competitor or another. The chance that a standard will truly be open correspondingly decreases.

IV. Lessons for Electronic Commerce

It is certainly possible to overstate the importance of group standard setting to electronic commerce. Electronic commerce can occur without a universal open standard set by a standards body. Indeed, the phenomenal growth now occurring has taken place largely without the benefit of universal standards.[39]

---

[38] Intergraph Corp. v. Intel Corp., 3 F. Supp. 2d 1255 (N.D. Ala. 1998); *In re* Intel Corp., FTC Dock. 9288 (complaint filed June 8, 1998), available at (visited on March 12, 1999) <http://www.ftc.gov/os/9806/intelfin.cmp.htm>. The FTC case was recently settled by consent decree. Intel agreed not to cut off its supply of chips and technology to plaintiffs who sued it, provided they met certain conditions. *See* (visited on April 14, 1999) <http://www.ftc.gov/os/1999/9903/d09288intelagreement.htm>.

[39] This is not to say there are no such standards under development. *See* Mueller, *supra* note 9, at 412 ("In the midst of the vigorous competition among various companies and consortia to establish their proprietary payment methods, many leading financial services and technology companies are also participating in efforts to develop open technology standards."). Among these putative group standards are BIPS, *see* (visited on Mar. 12, 1999) <http://www.fstc.org/projects/bips/>; the Account-Based Secure Payment Objects Standard, *see* (visited on Mar. 12, 1999) <http://www.commerce.net/resources/lists/open.html>; the Internet Open Trading Protocol, *see* (last modified on Feb. 16, 1999) <http://www.ietf.org/html.charters/trade-charter.html>; the Payment Facility Object Framework, *see* (visited on Mar. 12, 1999) <http://www.omg.org/schedule/Electronic_Payment_RFP.htm>; and the XML standard for extending HTML to enable machine-driven commerce, *see* (visited on Mar. 12, 1999) <http://www.veosys.com/xml/white_papers/whitepapers2.html>.

Nonetheless, there seems no question that the growth of electronic commerce could be both faster and more efficient if a number of the infrastructure problems noted in the Magaziner Report were dealt with. A number of commentators in particular have noted that the widespread deployment of electronic payment systems -- particularly smart cards and electronic cash -- has been delayed by the lack of a single, interoperable standard for their use.[40] This is a classic network problem. Consumers won't invest in smart cards until they are widely accepted, and merchants won't accept them unless they expect consumers to use them. The problem is exacerbated by the fact that competitors' cards work on different standards, and so there is no guarantee that a given consumer's card will work with a given merchant's machine. The problem may be solved eventually if one competitor's card gains a dominant share of the market, but the uncertainty of the intervening period will delay widespread adoption of electronic commerce tools. [41] Further, the fact that one company owns the resulting standard may limit total market penetration of the standard in the medium run even once the company has won a *de facto* standards competition. Consumers and vendors locked in to the losing standard, or who are prevented by exclusive dealing arrangements from dealing with the victor, will not be

---

[40] *See, e.g.*, Elizabeth Judd, *BITS CEO Tells E-Money About the Group's Upcoming Initiatives*, E-MONEY, July 1998, at 26 (quoting Catherine Allen); John D. Muller, *Selected Developments in the Law of Cyberspace Payments*, 54 BUS. LAWYER 403, 410 (1998) ("Interoperability among different smart card systems is crucial to the development of smart cards, and industry leaders continue to work towards establishing worldwide open standards."); Richard Poynder, *Today's Technology: Understanding E-Money and E-Commerce*, E-MONEY, July 1998, at 18, 21; Cynthia Weaver, *Smartcards in the United States: What is Holding Up the Show?*, E-MONEY, Aug. 1998, at 3, 4.

[41] *See* Weaver, *supra* note 40, at 4: "The worldwide problem of insufficient interoperability is another major hindrance to smartcard acceptance . . . [The major vendors] are still waging a war over standards for their disparate electronic purse specifications . . . . Not until a universal standard for financial services applications is adopted by the international community will the United States forge ahead with smartcard open systems." *See also* Poynder, *supra* note 40, at 21 ("Until and unless a globally accepted purse architecture appears, or the main purse products are modified to be interoperable, then this situation [the prevalence of "proprietary, fragmented," standards that aren't interoperable] will do much to prevent the successful international proliferation of e-commerce . . . ").

able to use the dominant standard.[42] In a network market, if participants are excluded from the standard, then *everybody* loses.

The right choice between open and closed standards is a complex one. Factors that go into determining social welfare include the technical quality of the standards, the possibility of improving those standards over time, the variety and price of products that embody the standards, and the size of the market that will result, as well as the speed of adoption and durability of the winning standard. But in the context of electronic payment systems or transaction security, where the most important consideration is getting everyone speaking the same language, there are good reasons to think that open systems have a natural advantage. Certainly, the rhetoric of the Magaziner Report suggests the government is of that view.

If the government truly wants to promote open systems for electronic commerce, what should it do? Several possibilities come to mind. At a minimum, the government really should get out of the way of private standard setting organizations that promote open standards. The Administration's efforts to date have focused primarily on getting *foreign* governments not to intervene in the standard setting process.[43] But U.S. rules affect standard setting organizations as well. Antitrust challenges to organization rules that promote interoperability seem more likely to injure competition than to promote it. Also, the government should at least be aware that its efforts to block or alter a standard

---

[42] Thus, in both the PC market and the VCR market, the result of a standards competition was a minority of consumers and suppliers who were excluded from the network even years after it was clear which standard had won the competition. *See, e.g.,* Paul David, *Clio and the Economics of QWERTY*, 75 AM. ECON. REV. 332, Issue 2 (May 1985) (noting the risk of such suboptimal lock-in).

[43] *See* ANNUAL REPORT, *supra* note 12, at Progress on the Presidential Directive.

to achieve other policy goals -- as it has done in the encryption context -- will impose real costs on efforts to achieve a standard by consensus.[44]

But the government could take a more positive role in supporting the development of open standards. It could endorse interoperability in the marketplace in the same way it has endorsed key escrow: by refusing to buy or use products that rely on a closed proprietary standard. Alternatively, the government could simply require interoperability, particularly in markets that have historically been subject to regulation.[45] The Magaziner Report itself endorses just such a requirement where telecommunications standards are concerned; perhaps the government's historic role in regulating currency and payment systems[46] could justify a similar requirement there. Finally, Congress or the courts could promote interoperability by erecting some limits on the scope of intellectual property protection, for example by precluding ownership of industry standards altogether or by permitting the copying of APIs where necessary to achieve interoperability. Copyright law has already made some strides in this direction;[47] it may be that patent law should contain such an exception as well.[48]

---

[44] *Cf.* Jane Kaufman Winn, *Open Systems, Free Markets, and Regulation of Internet Commerce*, 72 TULANE L. REV. 1177 (1998) (arguing that government should not pass laws that favor particular technological choices before the technology is fully developed).

[45] Winn's caution against technology specific legislation, *see id.* at 1183, need not concern us overlong here. What I am suggesting is not a preference for a particular technical standard, but for a process of achieving that standard and for a particular set of rules regarding the use of whatever standard results.

[46] For a discussion of the history of banking and payment system regulation in the United States, see Kerry Lynn Macintosh, *How to Encourage Global Electronic Commerce: The Case for Private Currencies on the Internet*, 11 HARV. J.L. & TECH. 733 (1998); Jane Kaufman Winn, *Clash of the Titans: Regulating the Competition Between Established and Emerging Electronic Payment Systems*, 14 BERKELEY TECH. L.J. __ (1999).

[47] Commentators have sharply divided on whether compatibility and/or standardization should justify reverse engineering or copying of parts of a plaintiff's computer program. Virtually all recent courts have endorsed reverse engineering in some circumstances. *See,* Alcatel USA, Inc. v. DGI Technologies, Inc., 166 F.3d 772 (5th Cir. 1999); DSC Communications Corp. v. DGI Technologies, Inc., 81 F.3d 597, 601 (5th Cir. 1996); Bateman v. Mnemonics, Inc., 79 F.3d 1532, 1539 n.18 (11th Cir. 1996); Lotus Dev. Corp.

Whether or not the government decides to stand behind the Magaziner Report's rhetoric in favor of open and private technical standards for electronic commerce, two things should be clear. First, the government is perfectly willing to intervene in the development of market standards when it has an interest in the outcome. Second, the choice between open and closed standards is an important one for the development of electronic commerce, and rhetoric alone won't produce the right outcome.

---

v. Borland Int'l, Inc., 49 F.3d 807, 819-22 (1st Cir. 1995) (Boudin, J., concurring); Atari Games Corp. v. Nintendo of America, Inc., 975 F.2d 832, 843-44 (Fed. Cir. 1992); Sega Enterprises, Ltd. v. Accolade, Inc., 977 F.2d 1510, 1527-28 (9th Cir. 1992); Vault Corp. v. Quaid Software Ltd., 847 F.2d 255, 270 (5th Cir. 1988); Mitel, Inc. v. Iqtel Inc., 896 F. Supp. 1050, 1056-57 (D. Colo. 1995), *aff'd on other grounds* 124 F.3d 1366 (10th Cir. 1997).

Most commentators have similarly endorsed such a reverse engineering right. *See, e.g.*, JONATHAN BAND & MASANOBU KATOH, INTERFACES ON TRIAL (1995); Julie E. Cohen, *Reverse Engineering and the Rise of Electronic Vigilantism: Intellectual Property Implications of "Lock-Out" Technologies*, 68 S. CAL. L. REV. 1091 (1995); Lawrence D. Graham & Richard O. Zerbe, Jr., *Economically Efficient Treatment of Computer Software: Reverse Engineering, Protection, and Disclosure*, 22 RUTGERS COMPUTER. & TECH. L.J. 61 (1996); Dennis S. Karjala, *Copyright Protection of Computer Documents, Reverse Engineering, and Professor Miller*, 19 U. DAYTON L. REV. 975, 1016-18 (1994); Maureen A. O'Rourke, *Drawing the Boundary Between Copyright and Contract: Copyright Preemption of Software License Terms*, 45 DUKE L.J. 479, 534 (1995); David A. Rice, *Sega and Beyond: A Beacon for Fair Use Analysis . . . At Least as Far as It Goes*, 19 U. DAYTON L. REV. 1131, 1168 (1994).

On the other hand, some early decisions rejected compatibility as a justification for copying. *See* Apple Computer v. Franklin Computer, 714 F.2d 1240 (3d Cir. 1983); Digital Communications Assoc. v. Softklone Distributing Corp., 659 F. Supp. 449 (N.D. Ga. 1987). And one current case suggests limits on the reverse engineering right. DSC Communications Corp. v. Pulse, 1999 WL 126067 (Fed. Cir. 1999). *See also* Anthony Clapes, *Confessions of an Amicus Curiae: Technophobia, Law and Creativity in the Digital Arts*, 19 U. DAYTON L. REV. 903 (1994) (arguing that no right to reverse-engineer software should exist) and Arthur Miller, *Copyright Protection for Computer Programs, Databases, and Computer-Generated Works: Is Anything New Since CONTU?*, 106 HARV. L. REV. 977 (1993) (same).

[48] Here again, the issue is complex, and there is no room to develop it fully. I hope to do so in a future paper.