Fordham University School of Law

Research Paper 41

January 2004

States and Internet Enforcement

Joel R. Reidenberg

1 UNIV. OTTAWA L. & TECH. J. (2004)

INAUGURAL SYMPOSIUM
1 UNIV. OTTAWA L. & TECH. J.

States and Internet Enforcement

Joel R. Reidenberg*

The debate over Internet jurisdiction has focused largely on the continued relevance of territorial borders and on the authority of states to prescribe rules for online conduct.[1] Some academics have argued that the Internet creates a space beyond territorial regulation.[2] This view maintains that the Internet evades or escapes national regulation. Others scholars have persuasively argued that states retain important regulatory authority through prescriptive and personal jurisdiction.[3] These conflicting views

---

 Professor of Law, Fordham University School of Law; Visiting Professor of Law, Université de Paris I (Panthéon-Sorbonne). Many thanks to the participants at the University of Ottawa Comparative IP and Cyberlaw Symposium for remarks on an earlier draft and especially to Michael Geist, Jane Bailey, Jennifer Chandler, Stephanie Perrin, Peggy Radin and Jon Zittrain for their thoughtful comments. A Fordham Law School Faculty Research Grant and a Fordham University Faculty Fellowship supported work on this paper.

[1] The term "state" in this essay refers to nation-state.

[2] David R. Johnson & David Post, Law and Borders—The Rise of Law in Cyberspace, 48 Stan. L. Rev. 1367 (1996); Henry H. Perrit, Jr. Jurisdiction in Cyberspace, 41 Vill. L. Rev. 1 (1996);

[3] Michael Geist, Cyberlaw 2.0, 44. B.C. L. Rev. 323 (2003); Justin Hughes, The Internet and the Persistence of Law, 44 B.C. L. Rev. 359 (2003); Jack Goldsmith, Against Cyberanarchy, 65 U. Chicago L. Rev. 1199 (1998) ; Jack Goldsmith, The Internet and the Abiding Significance of Territorial Sovereignty, 5 Indiana J. Global Legal Studies 475 (1998); Jack Goldsmith, Unilateral Regulation of the Internet: A Modest Defense, 11 E.J.I.L. 135 (2002); Michael Birnhack & Niva Elkin-Koren, The Invisible Handshake: The Reemergence of the State in the Digital Environment, 8 Va. J. L. & Tech. 6 (2003)

appeared dramatically in the case of Yahoo's auction web site. Yahoo's site allowed the display of Nazi memorabilia around the world. In France, the display violated democratically chosen rules against racial, religious and ethnic hatred and a French court ordered Yahoo to block access to French web users.[4] In the United States, where the servers were located, Yahoo won an injunction barring the enforcement of the French decision in the United States.[5]

Traditionally, a standoff would exist if as Jack Goldsmith argued: "offshore users with no local assets are generally beyond the regulating nation's enforcement jurisdiction."[6] However, for the online world, the situation is much more complex. The lack of local assets and the assistance of foreign courts no longer constrain state enforcement powers. States can enforce their decisions and policies through Internet instruments. Online mechanisms are available and can be developed for such pursuits.

This essay addresses the enforcement of decisions through Internet instruments. The starting point is a brief justification of Internet enforcement as the obligation of democratic states. Next, the essay argues that the movement to re-engineer the Internet infrastructure by public and private actions also facilitates state enforcement of legal and policy decisions. The essay maintains that states will increasingly try to use network intermediaries such as payment systems and Internet service providers as enforcement instruments. Finally and most importantly, the essay focuses on ways that states may harness the power of technological instruments such as worms, filters and packet interceptors to enforce decisions and sanction malfeasance.

---

http://www.vjolt.net/vol8/issue2/v8i2_a06-Birnhack-Elkin-Koren.pdf ; Michael Geist, Is There a There There? Toward Greater Certainty for Internet Jurisdiction, 16 Berkeley Tech. L.J. 1345 (2001); Neil Weinstock Netanel, Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory, 88 Calif. L. Rev. 397 (2000)

[4] TGI Paris, Ord. en référé du 20 nov. 2000 available at <http://www.foruminternet.org/telechargement/documents/tgi-par20001120.pdf>

[5] Yahoo! v. La ligue contra le racisme et l'anti-sémitisme, 169 F. Supp. 2d 1181 (N.D.Ca, 2001)

[6] Jack Goldsmith, Unilateral Regulation of the Internet: A Modest Defense, 11 E.J.I.L. 135, 140 (2000).

I. The Justification for State Enforcement Against Remote Parties

Democracy is founded on the principle of popular sovereignty. For liberal democracies, citizens agree to collective governance in order for government to protect their security and property. [7] At the same time, the 'social compact' emphasizes limits on state power.[8] For other democracies, the citizenry may make a more general and absolute delegation of power to the state in order to promote public liberty.[9] In each instance, government is expected to sustain the rule of law and thereby guarantee the protection of the rights of citizens. The democratic state, thus, has an obligation to assure security, order and the rule of law.

To fulfill the state's obligation to its citizens, democracies accord enforcement authority to the state. Traditionally, this authority includes three principle powers: the power to award money damages for wrongdoing by members of the society; the power to grant injunctive relief; and the power to incarcerate. The failure of a democratic state to use these powers to enforce policies and decisions adopted by the democracy is, in effect, an abdication of the responsibilities of the state.

For states to meet their responsibilities in the online world, states must find ways to transpose the powers of enforcement to the Internet. For example, the dueling French and American court decisions in the Yahoo case illustrate both the profound obligation of states to execute their democratically chosen policies and the need for states to transpose enforcement powers online. The French court ruling that ordered Yahoo to block French users' access to the company's promotion of Nazi memorabilia was

---

[7] See e.g. John Locke, The Second Treatise of Government 70-85 (Thomas P. Peardon ed., Liberal Arts Press 1952)(1690)

[8] Id.

[9] See e.g. Laurent Cohen-Tanugi, Le droit sans l'état: Sur la démocratie en France et en Amérique 10 (1985)

necessary to support French public policy.[10] Any other decision would have negated the democratically chosen law in France on hate speech. At the same time, the U.S. court's refusal to recognize the French decision in the United States rested on the court's desire to find a conflict with the First Amendment and its fundamental policies for the American democracy.[11] While Yahoo had assets in France and ultimately chose to remove Nazi material from its auction site, the conflict shows the importance of online enforcement.

States confront a challenge for the transposition of legal and physical powers to the online world, particularly the powers of injunction and incarceration. *Lex informatica* or "code", the catchier phrase popularized by Larry Lessig,[12] provide useful tools for states in this area.

II. Enforcement through Network Engineering

The engineering of the Internet is itself an important enforcement tool. Infrastructure design empowers the automatic enforcement of policies and decisions.[13] At its origin, the engineering of the Internet responded to the first obligation of

---

[10] See Joel R: Reidenberg; Yahoo and Democracy on the Internet; 42 Jurimetrics 261 (2002); Joel R. Reidenberg, L'affaire Yahoo! et la démocratisation internationale de l'Internet, Juris Classeur : Communication, Commerce électronique, chron. 12 (Mai 2001)

[11] Yahoo! v. La ligue contra le racisme et l'anti-sémitisme, 169 F. Supp. 2d 1181 (N.D.Ca, 2001)

[12] See Joel R: Reidenberg; Governing Networks in Cyberspace, 45 Emory L. J. 911, 929-30 (1996)(first using the term *lex informatica* to describe governance through the interaction of state rules and technological choices); Joel R: Reidenberg; Lex Informatica and The Formulation of Information Policy Rules through Technology, 76 Texas L. Rev. 553 (1998); Lawrence Lessig, Code and other laws of cyberspace (1999)(using the term "code" to describe rules established through technological decisions)

[13] See e.g. Joel R. Reidenberg, Lex Informatica: The Formulation of Information Policy Rules through Technology, 76 Texas L. Rev. 553, 580-81 (1998); Joel R. Reidenberg, Rules of the Road for Global Electronic Highways: Merging the Trade and Technical Paradigms, 6 Harv. J. L. & Tech. 287, 300 (1993)("The technical choices… set the parameters directly in global network architecture.")

democratic states: the protection of national security. The U.S. government initiated the construction of the Internet in the context of military policy. The Department of Defense first funded the creation of the ARPANET to link civilian and academic research scientists with the military.[14] As the project evolved, "the military wanted to retain the advantages of specialized networks, but it wanted universal communication among them."[15] Ultimately, the Internet design sought to assure reliable transmission of data even if links in the telecommunications routing system failed through error or damage in a war.[16]

During the 1990s, however, the U.S. government responded to the Internet euphoria and the promise of electronic commerce with the privatization and self-regulation of network activities.[17] After the burst of the Internet bubble in 2000, the public and private sectors each began to focus on network architecture to enforce their policies. Public and private efforts sought to redesign critical features of online activity. This movement to re-engineer the Internet increasingly facilitates the enforcement of public policy choices and legal decisions.

---

[14] See Milton Mueller, Ruling the Root, 74 (2002)

[15] Id., at 75.

[16] ACLU v. Reno, 929 F. Supp. 824, 831 (E.D. Pa. 1996) ("From its inception, the network was designed to be a decentralized, self-maintaining series of redundant links between computers and computer networks, capable of rapidly transmitting communications without direct human involvement or control, and with the automatic ability to re-route communications if one or more individual links were damaged or otherwise unavailable. Among other goals, this redundant system of linked computers was designed to allow vital research and communications to continue even if portions of the network were damaged, say, in a war.")

[17] See White House, A Framework for Global Electronic Commerce (July 1997) http://web.archive.org/web/20000815054938/http://www.ecommerce.gov/framewrk.htm; Symposium: The Legal and Policy Framework for Global Electronic Commerce: A Progress Report, 14 Berkeley Tech. L. J. (1999) http://www.law.berkeley.edu/journals/btlj/articles/vol14/index.htm

A. Public re-engineering

Infrastructure design offers the state an *ex ante* means to assure that policy decisions are enforced. States can require that rules for the treatment of information be embedded within the technical system architecture. By "hard-wiring" particular rules within the infrastructure, states preclude violations and automate the enforcement of public decisions. Three recent actions illustrate the public sector's trend toward a re-engineering of the Internet. These examples show three different ways that the state may facilitate automated enforcement.

1. Engineering Products

The first example shows how regulators may compel developers of technology to build policy-enforcing designs into their products. In 2002, Microsoft sought to commercialize an online authentication service, " .NET Passport." The product was to be "an Internet-scale authentication service providing single sign-in across multiple participating websites in order to help users to save time and avoid repetitive data entries when surfing on the Internet."[18] More specifically:

> "The .NET Passport architecture uses a single authentication server, which is operated by Microsoft. The Passport contains some identification and authentication information plus some profiling information.... A user who has logged on to Passport has a unique identifier, a PUID. If the user wants to log on to a service provider, he instructs the Passport server to provide the PUID in a form that is readable by the service provider, currently symmetrically encrypted."[19]

---

[18] See Eur. Comm. Art. 29 Working Group, Working Document on On-line Authentication Services, Jan. 29, 2003, Eur. Doc. 10054/03/EN WP68, at p. 5 http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp68_en.pdf.

[19] See Id., at pp. 3-4.

From the start, Microsoft's plans appeared to conflict with European data privacy law and faced regulatory scrutiny to assure that the authentication services could be used in a fashion compatible with European data protection requirements. [20]

The consortium of European data protection supervisory authorities, known as the Article 29 Working Party, pursued an investigation of the compatibility of .NET Passport with European law. Microsoft worked with the European supervisory authorities and negotiated an agreement that included modifications to the product.[21] Among the changes, Microsoft separated the creation of a .NET Password account from the collection of personal information and agreed to include greater user controls related to the disclosure of personal information.[22] These changes decreased the surveillance aspects of the original product design. Interestingly, Microsoft announced that these privacy-enhancing measures would be applied on a worldwide basis, even though only European law required them.[23]

In essence, the Article 29 Working Party obliged Microsoft to build European data privacy protections directly in the company's technology. This embedding of privacy rules in the technical design assures enforcement of certain principles required by the European Directive.[24] Like an injunction, this re-engineered product design compels compliance with privacy principles.

---

[20] See Id.

[21] See European Commission, Press Release-- Data protection: Microsoft agrees to change its .NET Passport system after discussions with EU watchdog, Doc. IP/03/151, Jan. 30, 2003; Microsoft, Building Trust in Internet Privacy: The new .NET passport (undated) available at http://www.microsoft.com/europe/content/downloads/BuildingTrust.pdf.

[22] Microsoft Building Trust in Internet Privacy: The new .NET Passport, 3 (undated) available at http://www.microsoft.com/europe/content/downloads/BuildingTrust.pdf (visited Sept. 23, 2003)

[23] See Helen Jung, Microsoft Agrees to Changes in Passport, InformationWeek, Jan. 30, 2003, http://www.informationweek.com/news/IWK20030130S0004

[24] Directive 95/46/EC of the European Parliament and of the Council 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. (L281) 31 (Nov. 23, 1995) http://europa.eu.int/comm/internal_market/privacy/law_en.htm.

2. Engineering Market Access

The second interesting case demonstrates how the state may re-engineer network systems to prevent illegal activities from taking place within the state's jurisdiction. As in many places, gambling is illegal in New York.[25] New York courts have enjoined Internet gambling sites that took bets from New Yorkers.[26] Yet, in 2002, the New York State Attorney General pursued a noveler approach to the elimination of online gambling in New York. Attorney General Elliot Spitzer sought to redesign the online payment network to prevent Internet gambling in New York. Spitzer reached agreements with Paypal[27] and Citibank[28] to stop the processing of payments for Internet casinos by blocking transactions according to merchant codes embedded in the payment system's network. Within a few months, the majority of credit card issuers in New York signed agreements with the N.Y. Attorney General to block cardholders from using their credit cards to gamble at Internet casinos.[29]

By cutting off the payment mechanisms for recreational gamblers, these agreements effectively shut down the major Internet casinos in New York and prevented them from gaining access to the New York market. New York re-engineered the payment system to achieve *ex ante* enforcement of the state ban on

---

Similarly, the Privacy Protection Commissioner of Canada compelled an airline to reconfigure its web site so that Internet users could access the site without having to accept "cookies." Privacy Comm'n of Canada, PIPED Case Summary #162 (Apr. 16, 2003) http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030416_7_e.asp

[25] NY Gen. Oblig. § 5-401; N.Y. Pen. L. § 225

[26] See People of the State of New York v. World Interactive Gaming Corp., 714 N.Y.S.2d 844 (Sup. Ct. 1999).

[27] N.Y. Attorney General, Press Release: Agreement Reached with Paypal to Bar New Yorkers from Online Gambling (Aug. 21, 2002) available at http://www.oag.state.ny.us/press/2002/aug/aug21a_02.html

[28] N.Y. Attorney General, Press Release: Financial Giant Joins Fight Against Online Gambling (June 14, 2003) http://www.oag.state.ny.us/press/2002/jun/jun14a_02.html

[29] N.Y. Attorney General, Press Release: Ten Banks End Online Gambling with Credit Cards (Feb. 11, 2003) http://www.oag.state.ny.us/press/2003/feb/feb11b_03.html

gambling. In effect, this type of re-engineering resembles the traditional power of an injunction. New York was able to preclude offshore Internet sites from taking bets from New Yorkers. Although New York clients of online casinos might still circumvent this injunctive action, legal systems do not pretend to achieve perfect compliance. Regulations that can substantially reduce proscribed actions are legitimate and effective.[30] Indeed, the overall impact of the New York agreements will certainly be a successful prevention of online gambling in New York. The payment network, thus, enforces the New York ban on gambling by preventing market access to offshore gaming web sites.

3. Engineering Network Access

The last example demonstrate how states may compel a re-engineering of the access to network infrastructure in order to enforce behavioral rules. States are particularly concerned about the control of pornography and obscenity on the Internet. In the United States, the Supreme Court in *ACLU v. Reno*[31] struck down the first attempt to modify access to the Internet—the rejected law, the Communications Decency Act, would have modified access to the Internet in order to limit minors' exposure to offensive content. Not to be deterred, Congress subsequently enacted the Children's Internet Protection Act.[32] This statute imposes a ban on federal funding of libraries that do not use filters to prevent children from accessing pornography. This time, Congress was more successful and the Supreme Court upheld the statute.[33] Similarly, Pennsylvania enacted a net blocking law that enables the state Attorney General to order the blocking of web sites by Internet

---

[30] See e.g. Lawrence Lessig, The Zones of Cyberspace, 48 Stanford L. Rev. 1403, 1405 (1996) cited in Michael Geist, Cyberlaw 2.0, 44 B.C. L. Rev. 323, fn.42 (2003).
[31] 117 S. Ct. 2329 (1997)
[32] 20 U.S.C. § 9134.
[33] See U.S. v. Amer. Library Assoc., 123 S. Ct. 2297 (2003)(upholding the constitutionality of the Children's Internet Protection Act.)

service providers.[34] The constitutionality of the Pennsylvania statute is under challenge.[35]

In each of these instances, the laws sought to create an architecture of network access that would enforce the state policy for the protection of children.[36] CIPA's success before the Supreme Court now means that funded libraries must adopt an infrastructure design that enforces the state policies on the protection of children against harmful content on the Internet.

B. Private Re-engineering

Beyond the public re-engineering efforts, private actors also recognized that rules could be 'hard wired' into the infrastructure to advance commercial interests. Not surprisingly, the private sector has likewise sought to re-engineer the Internet in ways that facilitate enforcement. A few examples illustrate the trend for the private sector to search for such enforcement aids.

1. Engineering Intellectual Property Protection

The difficulty protecting intellectual property online has led major content providers to seek infrastructure changes that will advance the enforcement of proprietary rights. The U.S. copyright law gives very broad protection to content providers and to the technical protection of digital works.[37] While the scope of the Digital Millennium Copyright Act's protections is controversial,[38] digital rights management techniques allow intellectual property rules to be embedded directly in the infrastructure of online content distribution. Current DRM technologies seek to foreclose violations of intellectual property rights by restricting users'

---

[34] 18 Pa. C.S. § 7626

[35] See Center for Democracy and Technology v. Fisher, E.D. Pa. No. 03-5051 (Sept. 9, 2003)

[36] Other countries, too, impose filter obligations on those providing network access. See e.g. France. Loi no. 96-659 du 26 juillet 1996, art. 15 (requiring service providers to offer content filtering tools to users)

[37] 17 U.S.C. § 1201

[38] See e.g., Julie Cohen, DRM and Privacy, 18 Berkeley Tech. L.J. 575 (2003); Dan Burk and Julie Cohen, Fair Use Infrastructure for Copyright Management Systems, 15 Harv. J.L. & Tech. 41 (2001) .

interactions with online content.[39] This private use of technology, in effect, empowers *ex ante* private enforcement of intellectual property rights.

Similarly, content providers have taken steps to reduce the Internet's architecture of anonymity. The Internet communications protocol, TCP/IP, does not require that parties communicating with each other be personally identified. As commercial activities emerged on the Internet, this anonymity confronted a business desire to identify users. At first, 'phone home' technologies enabled content providers to track product usage.[40] Manufacturers such as Sony announced that all new products would contain a unique IP address,[41] thereby facilitating surveillance programs. More recently, content providers targeted anonymous file sharing. Since transaction records leave digital traces embedded in communication routing, the infrastructure may be 'reverse engineered' to identify or profile users. Now, content providers seek to use these infrastructure capabilities and resources to identify file sharers who illegally swap copyrighted works.

Whether or not one agrees with the scope of the Digital Millennium Copyright Act, the law may entitle content providers to compel the identification of Internet users.[42] For example, the Recording Industry Association of America successfully sued Verizon, an Internet service provider, in federal district court for the identities of subscribers.[43] By forcing Verizon to match log files with client records, the RIAA sought to unmask illegal traders

---

[39] See e.g., Microsoft, Windows Media Rights Manager 9 Series, http://msdn.microsoft.com/library/default.asp?url=/library/en-us/wmrm/htm/quickstart.asp

[40] See e.g. Adam Cohen, Spies among us, Time Europe, July 31, 2000 http://www.time.com/time/europe/magazine/2000/0731/cover.html ("More than 20 million people have downloaded programs that secretly snoop inside their PCs.")

[41] Sony to Assign IP Addresses to All Products, NE Asia Online, (Apr. 27, 2001) http://www.nikkeibp.asiabiztech.com/wcs/frm/leaf?CID=onair/asabt/news/129248

[42] See 17 U.S.C. § 512(h)

[43] Recording Industry Assoc. of America v. Verizon, 240 F. Supp. 2d 24 (D.D.C., 2003)

of copyrighted works.[44] While this particular decision was reversed on appeal, the court did make clear that hosting services would have obligations to divulge the identities of alleged copyright infringers; Verizon did not have to reverse engineer the identities because the appellate court found that the service provider's specific activities—those of a transmission conduit, rather than a hosting service-- were outside the statutory clause.[45] As a result, more cases will certainly explore the scope of this clause in the DMCA. These efforts, though, demonstrate a movement to re-engineer of the infrastructure in ways that prevent anonymous file sharing and that enforce intellectual property rights.

2. Engineering Commercial Protection

Private organizations have similarly pursued the re-engineering of network information flows to enforce commercial policies. Perhaps the most visible example comes from VeriSign. This company has a monopoly on the management of the ".com" domain name registry for the Internet. In September 2003, VeriSign initiated a program called "SiteFinder" that redirected mistyped domain names to an advertiser supported web site at VeriSign.[46] VeriSign sought to exploit its monopoly position and generate advertising revenue from these redirects built directly into the Internet routing infrastructure. The move was particularly controversial and faced substantial opposition from the Internet community.

Other companies also redirect Internet traffic to respond to powerful commercial interests. For example, Google redirects

---

[44] Christopher Stern, Verizon Identifies Download Suspects, Wash. Post, June 6, 2003, p. E05 http://www.washingtonpost.com/wp-dyn/articles/A21198-2003Jun5.html

[45] R.I.A.A. v. Verizon, 2003 U.S. App. LEXIS 25735 (D.C. Cir., Dec. 19, 2003) http://pacer.cadc.uscourts.gov/docs/common/opinions/200312/03-7015a.pdf

[46] See Declan McCullagh, VeriSign stands firm on domain redirect, C/Net News.com, Sept. 22, 2003 http://news.com.com/2100-1032-5080384.html?tag=nl

any request by a French user to http://www.google.com, a US-based server, to http://www.google.fr, a French server.[47]
The burgeoning spam problem on the Internet has likewise prompted companies to install spam blocks and filters. These technical devices seek to prevent communications that might otherwise harm service providers' email servers or their clients.

Thus, for commercial reasons, companies are looking to infrastructure designs as a means to execute and enforce their commercial policies.

III. Enforcement through Intermediaries

Even with a re-engineering of the Internet in ways that empower state enforcement capabilities, the proliferation and dispersion of Internet participants may still make direct enforcement against rule breakers difficult and expensive. States cannot ignore and are likely to pursue additional means of enforcement through intermediaries or proxies. Various points in the network infrastructure serve as gateways that in effect re-centralize access to the Internet. These gateways might be access providers, hosting services, or major switching hubs that are located within the jurisdiction of the interested state. The existence of these gateway points in an otherwise decentralized network entices states to focus efforts and find enforcement mechanisms that operate through the intermediaries at these points.

A. Progressive Responsibility

During the initial Internet euphoria, policy-makers gave network intermediaries important immunities for data transiting their systems. In the United States, the Telecommunications Act of 1996[48] exculpated ISPs from liability for the content of

[47] Apparently, Google filters URL requests originating from French ISPs and redirects them to Google's French site. For example, all of the author's requests to http://www.google.com from the Free.fr dial up Internet service and from the Noos.fr cable Internet service are each redirected automatically to http://www.google.fr.
[48] Pub. L. 104-104, 110 Stat. 56 (Sept. 30, 1996)

transmitted data.[49] Congress adopted this policy initially to provide an incentive for the development of Internet communications. The subsequent major U.S. intellectual property legislation, the Digital Millennium Copyright Act of 1998,[50] also generally exonerated web hosting services from liability for copyright infringements of hosted content.[51] But, the DMCA did not create an absolute immunity. Under the DMCA, liability for copyright infringement could attach if the hosting service failed to remove allegedly infringing material once the copyright owner provided the service with a notice of the infringement.[52] This difference in treatment of intermediaries reflects in part the economic importance of intellectual property rights and the relative value that the state places on protecting those rights.

As other state values become more significant, corresponding reductions in the scope of immunity for online intermediaries are enacted. For example, the value of security rose to critical importance after the terrorist attacks of September 11, 2001. The legislation that quickly followed, the USA Patriot Act,[53] facilitated government access to customer data held by service providers. The new provisions entitle the government to obtain data from service providers for law enforcement purposes under more relaxed legal standards than under prior law. At the same time the new provisions grant service providers immunity from damages if they volunteer information to the government on their clients' activities.[54] While couched as an immunity from damages, this provision transforms the intermediary into a law

---

[49] 47 U.S.C. § 230(c). See Jonathan Zittrain; Internet Points of Control, 44 B:C. L. Rev. 653 (2003)(noting the shift toward control through intermediaries on the Internet) http://www.bc.edu/schools/law/lawreviews/meta-elements/journals/bclawr/44_2/10_FMS.htm

[50] Pub. L. 105-304, 112 Stat. 2860 (Oct. 28, 1998).

[51] 17 U.S.C. § 512

[52] Id. See Alfred C. Yen, Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Liability, and the First Amendment, 88 Georgetown L. J. 1833 (2000)(discussing the "jousting" in the United States over the imposition of liability on ISPs for copyright infringement by subscribers.)

[53] Pub. L. 107-56, 115 Stat. 272 (Oct. 21, 2001)

[54] Id., at §§ 210-212.

enforcement agent and breaks down pre-existing barriers between service providers and law enforcement. Service providers now a have greater incentive and responsibility to assist the state in its law enforcement mission. In other words, the state has begun building a statutory regime that imposes greater responsibility on intermediaries.

B. Attractive Agents

Just as legal responsibility is likely to turn progressively toward intermediaries, intermediaries become ever more attractive as agents for rule enforcement. The temptation to use intermediaries arises from the confluence of two factors. To the extent that actual wrong-doers are numerous and dispersed, the state will require substantial resources to pursue each wrong-doer and such pursuits are likely to encounter practical obstacles. By contrast, to the extent that the activities of dispersed wrongdoers are channeled through gateway points, these intermediaries are easier to reach and offer more efficient results. The centralization of activity through gateways provides state authorities with new enforcement opportunities.[55]

Illegal transactions, for example, illustrate a growing attractiveness for states to pursue law enforcement through intermediaries. In New York, the direct legal fight against online casinos was difficult and did not give the state's Attorney General satisfactory results. New York's first attempt to block an illegal gambling web site earned an important injunction against an off-shore casino site.[56] But, the proliferation and decentralized nature of such sites defied the efficacy of sequential direct enforcement actions. In effect, New York was stymied in its efforts to reach the illegal gambling sites themselves. Similarly, individual actions against illegal gamblers, the users of such sites, could not easily be undertaken due to the expense and difficulty of

---

[55] But, "DarkNets" may still try to mask nefarious actions. See Heather Green, The Underground Internet, Business Week Online, Sept. 15, 2003, http://www.businessweek.com/magazine/content/03_37/b3849089_mz063.htm

[56] People of the State of New York v. World Interactive Gaming Corp., 714 N.Y.S.2d 844 (Sup. Ct. 1999).

identifying the wrongdoers. The New York Attorney General then targeted the payment system.[57] Payment intermediaries were easy to identify and attractive instruments for enforcement because they would both prevent sites from operating in New York and prevent New Yorkers from engaging in illegal gambling. New York found that enforcement against payment intermediaries within its jurisdiction was more efficient and effective. Likewise, New York City asked eBay to remove World Trade Center items hosted on the company's auction web site.[58] The city claimed that the sale of particular items violated police and fire department trademarks. Yet, rather than directly challenging the sellers, New York enlisted the intermediary, eBay, to police the behavior of auction sellers.

Intermediaries also become attractive targets for states to use in the pursuit of the enforcement of public order. For example, India recently ordered ISPs to block access to a Yahoo newsgroup that offended Indian public policy.[59] Similarly, the European Directive on Electronic Commerce expressly allows member state authorities to order the blocking of conduit transmissions that violate local law and allows member state authorities to impose liability for knowingly hosting third party content that violates law.[60] In the United States, the Computer Assistance for Law Enforcement Act[61] also enlists telecommunications service providers to develop infrastructures that assist law enforcement wiretaps.[62]

As the capabilities of intermediaries to identify and interdict malevolent actors increase, states will focus on options to use these intermediaries. States, for example, will find routing backbone gateways attractive enforcement agents. The scandal created by VeriSign's re-routing of Internet traffic for commercial

---

[57] See supra Part II A(2).
[58] Michael Cooper, eBay is Asked to Remove Trade Center Items, NY Times, Feb. 22, 2002. p. A13.
[59] India Blocks almost all Yahoo Forums, ABCNews.com, Sept. 29, 2003 http://abcnews.go.com/wire/Business/ap20030929_1278.html
[60] See European Directive 2000/31/EC, Eur. O.J. L178/1, July 17, 2000, Art. 12(3) http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_178/l_17820000717en00010016.pdf
[61] Pub. L. 103-414, 108 Stat. 4279 (Oct. 25, 1994).
[62] See 47 U.S.C. § 1002

gain illustrates the ease with which key intermediaries may be able to isolate Internet participants. [63] VeriSign controlled the main directory for Internet addresses. When VeriSign sought to direct users who mistyped Internet addresses to VeriSign's own advertiser-supported search page, SiteFinder, the Internet community was outraged and the company suspended the commercial venture.[64] Yet, if this capability can be used for commercial purposes, states will insist on using such capabilities for legitimate law enforcement.

IV Enforcement through Technological Instruments

The enforcement of policies and rules through the re-engineering of the Internet and through online intermediaries show that technological instruments may also offer extremely powerful tools for states to sanction Internet actors. States may harness the power of "lex informatica" and use technologies to implement law enforcement actions. Beyond infrastructure re-engineering for *ex ante* enforcement such as the .NET Passport changes,[65] techniques that create disruptive technologies have police powers that are also available for states to use in connection with law enforcement. These technologies offer several types of enforcement mechanisms. A state must, however, consider a variety of important factors in choosing among the different technological enforcement mechanisms.

A. The Police Power of Technologies

Widely proliferating viruses and worms illustrate the ease of exploiting technology to disrupt online interactions.[66] For

---

[63] See surpa Part II B(2); Elizabeth Olson, Disputes Erupt Over Service for Poor Internet Typists, NY Times, Sept. 18, 2003, p. C3.
[64] Elizabeth Olson, VeriSign agrees to suspend disputed Site Finder service, NY Times, Oct. 4, 2003, p. C14.
[65] See Part II A(1).
[66] See Steve Hamm, Epidemic: Crippling computer viruses and spam attacks threaten the information economy, Bus. Wk., Sept. 8, 2003, pp. 28-34.

example, CodeRed destroyed web pages of infected servers.[67] SoBig.F sought to direct traffic to particular web sites at specified times.[68] LoveBug flooded the Internet with email messages.[69] Blaster exploited a known flaw in the Microsoft operating system security and caused widespread service degradation for users across the Internet.[70]

These disruptive technologies have important police powers. Digital protestors and vigilantes have proven that disruptive technologies can be used as specific weapons against particular online organizations. Enemies of several online companies have successfully damaged the ability of companies to do business on the Internet. Denial of service attacks against Amazon, Yahoo, eBay and CNN seriously interrupted the operations of these major Internet companies and temporarily shut down the corporate web sites. [71] The more recent Blaster worm targeted Microsoft for criticism. Infected computers bore the legend "Billy gates why do you make this possible? Stop making money and fix your software."[72] The worm used a denial of service attack to overwhelm the web page for Windows updates and forced Microsoft to take the web page offline.[73] Similarly, advocates of spam have launched "zombie armies" to disable

---

[67] CERT Advisory CA-2001-19 "Code Red" Worm Exploiting Buffer Overflow In IIS Indexing Service DLL (July 19, 2001) http://www.cert.org/advisories/CA-2001-19.html

[68] CERT Incident Note IN-2003-03 (Aug. 22, 2003) http://www.cert.org/incident_notes/IN-2003-03.html

[69] CERT Advisory CA-2000-04 Love Letter Worm (May 4, 2000) http://www.cert.org/advisories/CA-2000-04.html

[70] CERT Advisory CA-2003-20 W32/Blaster worm (Aug. 11, 2003) http://www.cert.org/adivsories/CA-2003-20.html

[71] Ann Harrison, Cyberassaults hit Buy.com, Amazon, and CNN, ComputerWorld, Feb. 9, 2000 available at http://www.computerworld.com/news/2000/story/0,11280,43010,00.html

[72] John Ostik, Behind Microsoft's Latest PR Blitz, Wired (Sept. 24, 2003) http://news.com.com/2010-1002-5081234.html

[73] CERT Advisory CA-2003-20 W32/Blaster worm (Aug. 11, 2003) http://www.cert.org/advisories/CA-2003-20.html ("Lab testing has confirmed that the worm includes the ability to launch a TCP SYN flood denial-of-service attack against windowsupdate.com."

operators of spam-blocking lists.[74] Even digital warriors in furtherance of geo-political advantage are now using these technologies.[75] Last year, when Al-Jezeera launched an English language web site to disseminate propaganda at the time of the second Gulf War, the web site was forced off-line by a denial of service attack.[76]

Other forms of disruptive technologies further demonstrate that technological instruments can police data processing practices. For example, supermarket shoppers who were concerned about privacy turned to digital techniques to prevent a supermarket chain from gathering accurate profile information. The shoppers used cloned supermarket discount cards to frustrate the collection of personal information for customer profiling.[77]

In effect, private parties have shown that disruptive technological instruments are effective to enforce privately chosen rules and policies.[78]

B. Types of Technological Enforcement

Just as disruptive technologies embody police powers when used by private actors, these technologies can also be used by states to support law enforcement. Three key types of technological mechanisms are available for enforcement: (1) the creation of electronic borders around a state to secure compliance with laws and policies; (2) the imposition of electronic blockades

---

[74] Mike Brunker, Spam block list bombed to oblivion, MSNBC.com, Sept. 24, 2003, available at http://www.msnbc.com/news/95094.asp?0cv=TB10&cp1=1

[75] Michael Vatis, Cyberattacks during the War on Terrorism: A Predictive Analysis, Dartmouth Institute on Security Technology Studies Working Paper, at 5-9 (Sept. 22, 2001) http://www.ists.dartmouth.edu/ISTS/counterterrorism/cyber_a1.pdf

[76] See Al-Jazeera Web site under hacking attack, host says, HoustonChornicle.Com, Mar. 25, 2003 http://www.chron.com/cs/CDA/ssistory.mpl/special/iraq/1835732

[77] David Gallagher, The Man Who Would Buy Everything, Everywhere, N.Y. Times, Mar. 10, 2003, p. C3.

[78] One should note that many such private actions are likely to violate existing computer crime laws. An analysis of these issues is beyond this essay. Here the point is to show the power of technologies for police-like purposes.

to enjoin violations; and (3) the imposition of electronic sanctions to punish violators. Each of these instruments has important and varying consequences for states and third parties. Electronic borders have fewer extraterritorial implications than electronic blockades and electronic blockades are less hostile than electronic sanctions.

1. Electronic Borders

States may block outsiders from entering the state online through packet interception or filtering. Although currently available techniques may be rudimentary for these purposes, states may certainly develop more robust technologies to create electronic borders. A number of countries such as China and Saudi Arabia have already established the equivalent of online national borders by requiring service providers to filter Internet traffic.[79] These electronic borders replicate general national boundaries on the Internet. Yet, the erection of technical fences is not limited to autocratic states and general borders. Democracies such as France and India have imposed electronic borders against specific rule violators. France ordered Yahoo to block transmissions into France of illegal Nazi displays.[80] Similarly, India ordered Internet service providers to block entry into India of Yahoo discussion groups.[81]

By creating an electronic border, a state prevents communications with rule offenders and isolates those offenders outside the state. Such a border is like a self-enforcing injunction against violations of the state's rules. The electronic border does not directly effect redress, but may force the foreign party to remedy any harm as a condition of online re-entry into the state.

---

[79] See Jonathan Zittrain and Ben Edelman, Documentation of Internet Filtering Worldwide (Oct. 24, 2003) http://cyber.law.harvard.edu/filtering/ (visited Jan. 3, 2003); Shanthi Kalathil and Talyor C. Boas, Open Networks, Closed Regimes: The Impact of the Internet on Authoritarian Rule 13-42 (2003)

[80] TGI Paris Ordinance en référé (Nov. 20, 2000) http://www.foruminternet.org/telechargement/documents/tgi-par20001120.pdf

[81] See Dinesh C. Sharma, India bans a Yahoo group, C/Net, Sept. 23, 2003 available at http://news.com.com/2100-1028_3-5081021.html

Importantly, the creation of an electronic border requires a police action either through packet interception or filtering. While packet interception techniques may be initiated directly by law enforcement, filtering would require the use of intermediaries—Internet service providers or backbone routing hubs—as agents.

2. Electronic Blockades

As a corollary to an electronic Internet border, states may initiate a police action to stop a law offender's transmissions from going outside the offender's country. Packet interception techniques can be used or developed to capture the offender's transmissions when the destination is external to the offender's country. This type of blockade enjoins an offender from participating on the Internet outside the offender's home country and is the equivalent of incarceration or home confinement. In effect, the enforcing state creates an electronic prison that is co-extensive with the host country.

Since the electronic police action is targeted against a particular actor's activities outside the host country, an electronic blockade does not directly offend the territorial integrity of the host country. Nevertheless, a blockade is a hostile act. An electronic blockade imposes restraints on organizations and individuals within host countries. Correspondingly, the blockading state necessarily enlists intermediaries to assist in the creation of the electronic fence. Packet interception or other similar technologies will operate through the Internet's transmission intermediaries. In addition, an electronic blockade negatively affects other countries when the offender's access is blocked to the third country destinations.[82] Nevertheless, an electronic blockade appears as the online equivalent to incarceration and may also be used to force a foreign party to comply with state laws and policies.

[82] These restrictions on international communications are not likely to violate a state's obligations under the World Trade Organization rules because they are imposed for law enforcement purposes.

3. Electronic Sanctions

Finally, states may electronically sanction rule offenders by using technologies to penalize or destroy the offenders' online presence.[83] To sanction offenders, a state might launch a 'denial of service' or a 'distributed denial of service' attack. This is an online death penalty and prevents an offender from interacting on the Internet. A state may also use hacking techniques to "seize" or paralyze rule-violating web pages just as the state might execute a seizure order for real or personal property. In other words, the state may use techniques similar to the MS Blaster worm for law enforcement purposes. [84] Yet, electronic sanctions may cause collateral damage to third parties. For example, while a state may launch a denial of service attack from state servers, a distributed DOS attack enlists the use of private computing power and both attacks cripple the offender's host server. Others who rely on the same server will face service interruption and be penalized without cause in the host country.

Electronic sanctions are the most aggressive and hostile type of technological enforcement. They are a police action that takes place on the foreign territory where the offender is located. For the offender's host country, an electronic attack is a hostile act because it violates the country's territorial integrity. Indeed, under the computer crime laws of many countries, the electronic attack against an offender might be illegal.[85] Sovereign immunity would nevertheless apply since the attacks are launched by a foreign state. But, in design, this type of police action is a form of information warfare. The use of these capabilities, thus, has serious

---

[83] Recent US proposals have also sought statutory authorization for private parties to engage in self-help measures that bear a resemblance to electronic sanctions. A discussion of the merits and objections to such a privatization of law enforcement is outside the scope of this essay and will have to wait for another day.

[84] See e.g. Matt Richtel, Spread of Attacks on Web Sites is Slowing Traffic on the Internet, NY Times, Feb. 10, 2000, p. A1.

[85] For an interesting discussion of the scope of US cybercrime statutes, see Orin Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes,* 78 N.Y.U. L. Rev. 1596 (2003).

implications for the launching state. Already, the Bush Administration reportedly has prepared guidelines for cyber-attacks designed to disrupt enemy computer networks.[86] According to Richard Clarke, former adviser to the President on cybersecurity, the technological capabilities presently exist.[87]

For serious rule violations that fundamentally threaten public order, states may decide that electronic sanctions are a necessary and justified last resort.

C. The Deployment of Technological Enforcement Mechanisms

For democratic societies, the use of any technological enforcement instrument necessitates carefully prescribed authorization criteria. Like other police powers of the state, legal authority is a pre-requisite for the exercise of coercive powers. Each mechanism implicates important civil, political and sovereign rights. As a threshold matter, states must have a legal process in place to authorize the use and choice of technological enforcement tools.

For the choice to use a technological instrument or to deploy a specific type of instrument, the basic principle guiding these decisions should be that a state only use the least intrusive means to accomplish the rule enforcement. Four factors must be considered to determine whether and how to use technologies for rule enforcement. First, a state must weigh the magnitude of any threat to public order. If a threat is significant, a state may be justified in taking more drastic measures such as an electronic blockade. Second, the urgency of any threat is significant. If continuing rule violations pose imminent danger to a state's public order, a state will have stronger justification to use more serious measures such as electronic sanctions. Third, a state must evaluate the effectiveness of the tool. If a tool will not be effective against the rule violation, then the collateral implications may outweigh any justificatory use. Lastly, a state must consider the ultimate enforcement goal. If the state seeks the cessation of offending

---

[86] Bradley Graham, Bush Orders Guidelines for Cyber-Warfare, Wash. Post, Feb. 7, 2003, p. A1.

[87] Id. ("We have capabilities, we have organizations; we do not yet have an elaborated strategy, doctrine, procedures.")

activity, the technological enforcement tool may be different than the choice to compel a violator to pay monetary damages.

V. Conclusions

As the Internet matures, network engineering, intermediaries and technologies all provide states with greater means to enforce legal decisions and policies. In fulfilling their responsibilities toward their citizens, states must harness "lex informatica" as an instrument for the enforcement of decisions and policies for online activity.

The evolution toward more frequent online enforcement seems inevitable and a number of observations and predictions can be made. Public objectives and commercial pressures will result in re-engineered networks that are designed in ways supporting online enforcement including greater geographic identification and diminishing anonymity. Gateways will increasingly find themselves in the middle of enforcement actions despite the initially strong immunities granted to Internet intermediaries; intermediaries offer the most efficient and attractive means to reach rule violators. The critical importance of technological tools means that new instruments will be developed for the purpose of law enforcement such as sophisticated means to intercept offender's data traffic. Lastly, the choices among technological enforcement instruments will ultimately rely on political calculations because the choices impose different levels of hostility against other countries ranging from the least offensive, an electronic border, to the most offensive, electronic sanctions.

We can expect to see three phases in Internet enforcement by states. The first use of new online enforcement instruments will cause international controversy just like the Chinese decisions to control the web at the border[88] and the French decision that required Yahoo to block access to French users.[89] But, the second use takes on a more routine character like the Indian decision to

---

[88] See Shanthi Kalathil and Talyor C. Boas, Open Networks, Closed Regimes: The Impact of the Internet on Authoritarian Rule 13-42 (2003)

[89] See TGI Paris Ordinance en référé (Nov. 20, 2000) http://www.foruminternet.org/telechargement/documents/tgi-par20001120.pdf

order the blocking of Yahoo newsgroups.[90] At the third phase, online enforcement with electronic blockades and electronic sanctions will cause serious international political conflicts. These conflicts arise because of the impact on territorial integrity. Such conflicts are likely to force negotiations toward international agreements that establish the legal criteria for a state to use technological enforcement mechanisms. This progression leads appropriately to political decisions that will define international legal rules.

[90] See Dinesh C. Sharma, India bans a Yahoo group, C/Net, Sept. 23, 2003 available at http://news.com.com/2100-1028_3-5081021.html