2005

Technology and Internet Jurisdiction

Joel R. Reidenberg
Fordham University School of Law, jreidenberg@law.fordham.edu

TECHNOLOGY AND INTERNET JURISDICTION

JOEL R. REIDENBERG[†]

The current Internet technology creates ambiguity for sovereign territory because network boundaries intersect and transcend national borders. At one level, this technologically-created ambiguity challenges sovereign jurisdiction. Yet, the evolution of the Internet's technological infrastructure is intertwined with sovereign jurisdiction because the relationship between technology and law is dynamic.[1] As sovereign states grapple with the challenges of existing technologies, they still must protect their citizens in the online environment.

The debates over Internet jurisdiction,[2] however, mask deep and fundamental objections to state authority. Jurisdiction fits within a broader struggle over the respect for the rule of law in the Information Society. In effect, jurisdiction over activities on the Internet has become one of the main battlegrounds for the struggle to establish the rule of law in the Information Society.[3]

 Professor of Law, Fordham University School of Law. A.B. Dartmouth, J.D. Columbia, Ph.D Université de Paris I-Sorbonne. The author would like to thank participants at the University of Pennsylvania Law Review Symposium, "Current Debates in the Conflict of Laws," for their thoughtful comments on these reflections and would also like to thank Lodewijk Asscher, Lee Bygrave, Julie Cohen, Michael Froomkin, Sir Marrack Goulding, Bernt Hugenholtz, Mark Lemley, Kalypso Nicholaides, and Peter Swire for their vigorous debate and comments on the points relating to state enforcement powers.

[1] *See, e.g.*, Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553, 554-55 (1998) (describing the regulatory role of "[t]echnological capabilities and system design choices"); R. Polk Wagner, *On Software Regulation*, 78 S. CAL. L. REV. 457 (2005) (arguing for a symbiotic relationship between code and law in Internet regulation).

[2] *See* Michael Geist, *Cyberlaw 2.0*, 44 B.C. L. REV. 323, 332-35 (2003) (describing the increasingly "bordered" nature of the Internet); Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199, 1200 (1998) (challenging the notion that regulation is not applicable to the Internet); David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1367 (1996) (arguing that "[c]yberspace requires a system of rules quite distinct from the laws that regulate physical, geographically-defined territories"); Joel R. Reidenberg, *Yahoo and Democracy on the Internet*, 42 JURIMETRICS J. 261, 261 (2002) (arguing that "the policy rules embedded in the technical infrastructure must recognize values adopted by different statutes").

[3] Dan Hunter makes an interesting critique of the open source movement that suggests a similar political battle for the control of intellectual property rights. *See* Dan

Parts of the Internet community have long sought to divorce the applicability of sovereign law from their online activities.[4] While the days of Internet separatism have waned, many technology players continue to advocate in favor of legal immunity for online activities. Yahoo! exemplifies this view. As a proponent of technological immunity, Yahoo! believes that democratically chosen laws should not apply to its online activities. In the now famous French case, the U.S. company transmitted images of Nazi objects that were constitutionally protected in the United States, but illegal to display in France where the users were located and where Yahoo! targeted advertising.[5] Yahoo! unsuccessfully argued that France did not have personal jurisdiction over the U.S. company because it was operating on the Internet from the United States and that French law did not apply to the images because they were stored on a server in the United States.[6] Yahoo! also argued that the technology offered it no means to comply with French law.[7] When the French courts rejected the technology-based defenses and ruled against Yahoo!, the company went forum shopping and sought to deny enforcement of the French order by suing for a declaratory judgment in federal court in California.[8] In essence, the U.S. Internet company wanted to avoid the application and enforcement of a law it did not like in a country where it did business over the Internet. Although Yahoo! found a willing accomplice at the U.S. district court in the company's effort to obtain immunity from financial liability, the U.S. court of appeals overturned the lower court decision and held that the California court had no personal jurisdiction over the French parties and that France had every right to hold Yahoo! accountable in France.[9]

Hunter, Culture War (Aug. 10, 2004) (unpublished manuscript, *available at* http://ssrn.com/abstract=586463).

[4] *See, e.g.*, Johnson & Post, *supra* note 2; John Perry Barlow, A Declaration of the Independence of Cyberspace (Feb. 8, 1996), *at* http://homes.eff.org/~barlow/Declaration-Final.html.

[5] T.G.I. Paris, Nov. 20, 2000, *available at* http://www.juriscom.net/txt/jurisfr/cti/tgiparis20001120.pdf (last accessed May 2, 2005).

[6] *Id.* at 3.

[7] *Id.*

[8] Yahoo!, Inc. v. La Ligue Contre Le Racisme Et L'Antisemitisme, 169 F. Supp. 2d 1181 (N.D. Cal. 2001).

[9] Yahoo!, Inc. v. La Ligue Contre Le Racisme Et L'Antisemitisme, 379 F.3d 1120, 1126 (9th Cir. 2004). The Ninth Circuit has just agreed to rehear this appeal en banc. Yahoo!, Inc. v. La Ligue Contre Le Racisme Et L'Antisemitisme, 399 F.3d 1010 (9th Cir. 2005).

This Essay argues that the initial wave of cases seeking to deny jurisdiction, choice of law, and enforcement to states where users and victims are located constitutes a type of "denial-of-service" attack against the legal system. Internet separatists use technology-based arguments to deny the existence of sufficient contacts for jurisdiction and the applicability of rules of law interdicting certain behavior. From this perspective, the attackers seek to disable states from protecting their citizens online.

The Essay next shows that innovations in information technology will undermine the technological assault on state jurisdiction. This counterintuitive effect is born out of the fact that more sophisticated computing enlists the processing capabilities and power of users' computers. This interactivity gives the victim's state a greater nexus with offending acts and provides a direct relationship with the offender for purposes of personal jurisdiction and choice of law. Some of these same innovations also enable states to enforce their decisions electronically and consequently bypass the problems of foreign recognition and enforcement of judgments.

Finally, the Essay argues that the exercise of state power through assertions of jurisdiction can and should be used to advance the development of more granular technologies and new service markets for legal compliance. Technologies should be available to enable Internet participants to respect the rule of law in states where their Internet activities reach. Assertions of state jurisdiction and electronic enforcement are likely to advance this public policy.

I. THE TECHNOLOGICAL DENIAL OF LAW: A DENIAL-OF-SERVICE ATTACK

Internet enthusiasts embrace the wonder of the Internet's global electronic reach, but often reject the burden and responsibility of a global presence. The defenses for hate,[10] lies,[11] drugs,[12] sex,[13] gam-

[10] *See* T.G.I. Paris, Nov. 20, 2000, at 4 (finding that Yahoo! could not avoid the French ban on the display of Nazi symbols in France when Yahoo! served content to France).

[11] *See* Dow Jones & Co. v. Gutnick, (2002) 210 C.L.R. 575 (Austl.) (holding that a party cannot avoid prosecution for defamation via the Internet in the jurisdiction where the material was downloaded), *available at* http://www.4law.co.il/582.htm; Blumenthal v. Drudge, 992 F. Supp. 44, 48-53 (D.D.C. 1998) (accepting an assertion of immunity by a service provider for online defamation based on infrastructure arrangement); English Sports Betting v. Tostigan, 2002 WL 461592 (E.D. Pa. Mar. 15, 2002) (holding that Internet publication allegedly defaming Pennsylvania owner of offshore gambling website was insufficient to justify jurisdiction in Pennsylvania).

bling,[14] and stolen music[15] are in essence that technology justifies the denial of personal jurisdiction, the rejection of an assertion of applicable law by a sovereign state, and the denial of the enforcement of decisions. As Internet technologies enable global activities from remote locations, these claims rely on the technical infrastructure choices that parties make to conduct their online activities and on the assumption that existing technologies are static. In the face of these claims, legal systems engage in a rather conventional struggle to adapt existing regulatory standards to new technologies and the Internet.[16] Yet, the underlying fight is a profound struggle against the very right of sovereign states to establish rules for online activity.

A. *Personal Jurisdiction*

Some of the earliest attempts to reject state authority relate to personal jurisdiction. In the United States, courts have had great trouble figuring out how to apply traditional jurisdiction principles to Internet activities. To satisfy the Due Process Clauses of the U.S. Constitution,[17] a defendant must have sufficient minimum contacts with the forum "such that the maintenance of the suit does not offend 'traditional notions of fair play and substantial justice.'"[18] The Supreme Court, in *Asahi Metal Industry Co. v. Superior Court*, was more exacting, and lim-

---

[12] *See* United States v. Yates, 391 F.3d 1182 (11th Cir. 2004) (holding that criminal liability applies to the sale of prescription drugs over the Internet).

[13] Reno v. ACLU, 521 U.S. 844 (1997) (basing the decision to invalidate portions of the Communications Decency Act, in part, on the quality of existing filtering technology); Voyeur Dorm, L.C. v. City of Tampa, 265 F.3d 1232, 1236-37 (11th Cir. 2001) (finding that local zoning law was not violated because adult shows were "provided" online from the local venue, and were not "consumed" in person at the local site).

[14] *See* People v. World Interactive Gaming Corp., 714 N.Y.S.2d 844, 851 (Sup. Ct. 1999) (holding that an offshore Internet site does not avoid New York gambling interdiction).

[15] *See* Metro-Goldwyn-Mayer Studios, Inc. v. Grokster Ltd., 380 F.3d 1154 (9th Cir. 2004) (refusing to find distributors of software that enabled users to exchange digital media liable for copyright infringement), *cert. granted* 125 S. Ct. 686; *In re* Aimster Copyright Litig., 334 F.3d 643, 648-56 (7th Cir. 2003) (determining that a file-sharing provider could not avoid an injunction); A&M Records, Inc. v. Napster, Inc., 284 F.3d 1091, 1099 (9th Cir. 2002) (same).

[16] Andreas Manolopoulos, *Raising Cyberborders: The Interaction Between Law and Technology*, 11 INT'L J.L. & TECH. 40, 55 (2003) (noting that changing technological standards confound legal texts).

[17] U.S. CONST. amends. V, XIV.

[18] Int'l Shoe Co. v. Washington, 326 U.S. 310, 316 (1945) (quoting Milliken v. Meyer, 311 U.S. 457, 463 (1940)); *see also* Calder v. Jones, 465 U.S. 783, 788 (1984); World-Wide Volkswagen Corp. v. Woodson, 444 U.S. 286, 297 (1980).

ited personal jurisdiction to cases in which the defendant "purposely avail[s]" himself of the forum.[19] In essence, as the Supreme Court also held in *World-Wide Volkswagen v. Woodson*, personal jurisdiction is subject to a test of reasonableness.[20] Similar standards exist in foreign states where a court's competence to hear the case depends on the defendant's nexus with the forum state.[21] For example, the Brussels and Lugano Conventions on jurisdiction for intra-European disputes look to various forms of contact between defendants and the state asserting jurisdiction.[22]

In the Internet context, defendants have generally claimed that a remote forum is precluded from jurisdiction because the contacts are only established through a server that is not within the forum. Defendants assert that their activities are not directed at the forum state.[23] This type of argument challenges the very ability of sovereign states to protect their citizens within their borders from online threats. Among the early U.S. cases, the Western District of Pennsylvania in *Zippo Manufacturing v. Zippo Dot Com, Inc.* distinguished between active and passive web sites and held that remote, passive web sites did not accord personal jurisdiction to the forum.[24] More recently, courts have looked to online targeting and to deleterious effects within the forum to determine if personal jurisdiction is appropriate.[25] The effects ap-

---

[19] 480 U.S. 102, 112 (1987).

[20] 444 U.S. 286, 297 (1980) (holding that a defendant needs to have "conduct and connection with the forum State . . . such that he should reasonably anticipate being haled into court there").

[21] For example, the French requirement is discussed in YVES LOUSSOURAN & PIERRE BOUREL, DROIT INTERNATIONAL PRIVÉ (6th ed. 1999).

[22] *See* Convention 88/592/EEC on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters, 1988 O.J. (L 319) 9, 10-11 (Lugano Convention); Convention on Jurisdiction and Enforcement of Judgments in Civil and Commercial Matters, 1978 O.J. (L 304) 77, 79-80 (Brussels Convention).

[23] *See* Barrett v. Catacombs Press, 44 F. Supp. 2d 717 (E.D. Pa. 1999) (holding that posting to a listserv is too passive for personal jurisdiction); Machulsky v. Hall, 210 F. Supp. 2d 531 (D.N.J. 2000) (finding that a buyer's single transaction on eBay did not confer specific jurisdiction on the seller's forum state).

[24] 952 F. Supp. 1119, 1124 (W.D. Pa. 1997).

[25] Geist, *supra* note 2, at 332-47; *see also* Gator.com Corp. v. L.L. Bean, Inc., 341 F.3d 1072, 1078 (9th Cir. 2003) (finding that an interactive web site with advertising targeted at Californians and with relationships with California vendors and customers creates sufficient contacts for general jurisdiction), *reh'g en banc granted*, 366 F.3d 789 (9th Cir. 2004); ALS Scan, Inc. v. Digital Serv. Consultants, Inc., 293 F.3d 707, 714 (4th Cir. 2002) (holding that information transmitted into the jurisdiction over the Internet that causes harm within the jurisdiction provides minimum contacts); Panavision Int'l, L.P. v. Toeppen, 141 F.3d 1316, 1322 (9th Cir. 1998) (finding jurisdiction where a domain name was registered to divert Internet traffic away from the forum); Cy-

proach is also gaining currency outside the United States. In *Dow Jones & Co. v. Gutnick*,[26] the High Court of Australia subjected Dow Jones to suit in Australia for defamation in that country under Australian law arising from a web posting on a U.S.-based server.[27] Likewise, the High Court of Justice in the United Kingdom found that Governor Arnold Schwarzenegger's campaign manager could be sued for defamation in the British courts as the result of statements about a U.K. resident that appeared on a newspaper website in the United States.[28]

The maturation of the analysis reflects an evolution from a somewhat naïve view of the Internet to a rejection of the Internet activists' simple denial of law. The Internet became popular precisely because of the promise of a global audience. But, this promise could not absolve online activities of legal responsibility. While online technologies were initially designed for geographically indifferent access, nothing fixed the technology in stone. Commercial pressures and the dynamic nature of the Internet have resulted in geolocation and the re-creation of geographic origin and destination.[29] This design feature and its malleability mean that Internet activity is "purposely availing" throughout the Internet whenever content is posted without geolocation filtering. In gravitating toward an effects doctrine, sovereign states promoted submission to the rule of law rather than capitulation to an Internet attack.

B. *Choice of Law*

The next type of attack against sovereign authority seeks to deny the applicability of the substantive law if it is not the law of the place

---

bersell, Inc. v. Cybersell, Inc., 130 F.3d 414, 419-20 (9th Cir. 1997) (finding a passive home page insufficient to establish jurisdiction); *Zippo*, 952 F. Supp. at 1124 (setting out the test for passive jurisdiction); Bensusan Restaurant Corp. v. King, 937 F. Supp 295, 301 (S.D.N.Y.1996) (determining that there is no personal jurisdiction when web site is passive).

[26] (2002) 210 C.L.R. 575 [Austl.], *available at* http://www.4law.co.il/582.htm.

[27] *Id.* at 263-64; *see also* Ari Weinberg, *Australia to Dow Jones: Stay Awhile*, FORBES.COM, Dec. 10, 2002, *at* http://www.forbes.com/2002/12/10/cx_aw_1210 dowjones.html.

[28] Richardson v. Schwarzenegger, 2004 EWHC 2422 (Q.B. Oct. 29, 2004), *available at* http://portal.nasstar.com/75/files/Richardson-v-Schwarzenegger%20QBD%2029% 20Oct%202004.pdf.

[29] *See, e.g.*, Akamai: How it Works, *at* http://www.akamai.com/en/html /services/edge_how_it_works.html ("EdgeScape enables the enterprise to customize content based on the following data: . . . Country . . . City . . . Latitude and Longitude . . . Time zone").

where the Internet activity was launched, such as the place where the server is located. This blanket denial of prescriptive jurisdiction undermines the basic objective of conflict of laws jurisprudence, which is to avoid forum shopping and promote an efficient resolution of disputes when cases have international dimensions. Network technology pushes the localization of activities for choice-of-law purposes toward the transmission end-points. However, the attack against the law where users are located encourages forum shopping, to locate the infrastructure for the conduct of Internet activities within legal safe havens.[30]

Sovereign authority, nevertheless, asserts itself against Internet activists. In *Twentieth Century Fox Film Corp. v. iCrave TV*, a film studio fought successfully to apply U.S. copyright law to streaming video on the Internet and obtained an injunction against a Canadian service that could legally stream video in Canada from servers in Canada.[31] In France, the *Yahoo!* court determined that the French penal code applied to Yahoo!'s activities because the illegal content could be visualized in France.[32] The United Kingdom recently followed the same approach in a libel case, finding the place of downloading dispositive for the choice of law.[33] For privacy, the Children's Online Privacy Protection Act[34] in the United States contains a choice of law provision in its definitions that applies the protections of the American statute to any website, regardless of its place of origin, that collects personal information from children.[35] The European Directive on data privacy contains a similarly expansive choice of law rule that purports to apply European substantive law to any organization that uses means within the European Union to collect personal data.[36]

---

[30] *See, e.g.*, A. Michael Froomkin, *The Internet as a Source of Regulatory Arbitrage*, *in* BORDERS IN CYBERSPACE 129, 142 (Brian Kahin & Charles Nesson eds., 1997) (arguing that Internet actors will locate in safe havens).

[31] Nos. Civ.A. 00-121, Civ.A. 00-120, 2000 WL 255989, at *3 (W.D. Pa. Feb. 8, 2000).

[32] T.G.I. Paris, Nov. 20, 2000, *available at* http://www.juriscom.net/txt/jurisfr/cti/tgiparis20001120.pdf.

[33] Lewis v. King, [2004] EWCA (Civ) 1329 (Eng. C.A.), *available at* http://www.courtservice.gov.uk/judgmentsfiles/j2844/lewis-v-king.htm.

[34] Pub. L. No. 105-277, 112 Stat. 2681 (1998) (codified at 15 U.S.C. §§ 6501-6506).

[35] 15 U.S.C. § 6501(2) (2000).

[36] *See* Council Directive 95/46/EC of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, art. 4, § 1(c), 1995 O.J. (L 281) 31, 39; JOEL R. REIDENBERG & PAUL M. SCHWARTZ, DATA PROTECTION LAW AND ON-LINE SERVICES: REGULATORY RESPONSES 126-28 (1998), *available at* http://europa.eu.int/comm/internal_market/privacy/

The attempt by Internet separatists to deny the application of local law creates a stark challenge to public order rules. Online hate speech, for example, is generally prohibited outside the United States.[37] However, the First Amendment provides constitutional protection[38] and may therefore make the United States a haven for those wishing to spread such hate speech on the Internet. Similar issues are raised by the recognition that Internet pornography receives constitutional protection within the United States[39] and data privacy is a fundamental political right outside the U.S.[40] These legal differences encourage participants in illicit activities to launch their Internet activities from states that provide a legal safe haven.[41]

C. *Enforcement of Judgments*

The recognition of foreign judgments in these attack cases will often be problematic. As the *Yahoo!* case illustrated, public order rules at the place where Internet activity is launched may conflict with those of the place where the activity has its effects. Even the international conventions on recognition of foreign judgments provide an exception to enforcement when there is a conflict with the public order of the enforcing state.[42]

---

docs/studies/regul_en.pdf.

[37] *See, e.g.*, European Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, art. 10, 312 U.N.T.S. 221 (subjecting the right to freedom of expression to restrictions necessary in a democratic society); T.G.I. Paris, Nov. 20, 2000, at 4("[L]a simple visualisation en France de tels objets [nazis] constitue une violation de l'article R.645-1 du Code penal."), *available at* http://www.juriscom.net/txt/jurisfr/cti/tgiparis20001120.pdf; *see also* T.G.I. Paris, Feb. 11, 2003, *at* http://www.legalis.net/jurisprudence-decision.php3?id_article=1043 (applying the French hate speech law, but determining that Yahoo! and its chief executive Timothy Koogle had satisfied their obligations under a separate telecommunications safe harbor provision).

[38] *See, e.g.*, R.A.V. v. City of St. Paul, 505 U.S. 377, 391 (1992) (invalidating a city ordinance which criminalized cross-burning and offensive graffiti).

[39] *See* U.S. CONST., amend. I ("Congress shall make no law . . . abridging the freedom of speech . . . ."); Reno v. ACLU, 521 U.S. 844, 849 (1997) (holding that the First Amendment protects indecent sexual material on the internet).

[40] *See* Council Directive 95/46/EC, *supra* note 36 (protecting the right to privacy with respect to the processing of personal data); Council of Europe (COE), Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, 20 I.L.M. 317 (1981) (establishing the fundamental right to data protection).

[41] *See* Froomkin, *supra* note 30, at 142 (arguing that the Internet encourages routing around restrictive laws).

[42] *See supra* note 22 and accompanying text (discussing intra-European enforcement conflicts).

Courts are also especially ill-equipped to evaluate the nuances of foreign public order decisions. The *Yahoo!* case illustrates this difficulty particularly well. At the district court level, Yahoo! introduced a misleading translation of the French decision.[43] The key passage of the order in the French version was translated word-for-word with the exception of a qualifying phrase. This qualifying phrase was simply omitted in the English translation. The original court decision ordered Yahoo!: "de prendre toutes les mesures *de nature* à dissuader et à rendre impossible toute consultation sur Yahoo.com du service de ventes aux enchères d'objets nazis."[44] This was translated as "to take all *necessary* measures to dissuade and render impossible any access via Yahoo.com to the Nazi artifact auction service . . . ."[45] Instead of properly translating *mesures de nature* as either "available measures" or "the type of measures," the translation for the U.S. court ignored "*de nature*" and added the word "*necessary*," a term that does not appear at all in the original language. The effect of this distorted translation is to convert the filtering obligation from one of good faith efforts that is found in the original to one of successful results in the translation. At the same time, the translation distorted the term "Nazi objects" by translating it as "Nazi artifacts." This distortion creates an implication not found in the original text that the items had historical value. Such distortions in translation can serve to increase the sense of conflict over public order values. Indeed, the display of Nazi artifacts with historical connotations is expressly permitted by the French law.[46]

---

[43] The translation of the French opinion was prepared for the U.S. court by one of the French attorneys representing Yahoo!'s French subsidiary in the French proceeding. Yahoo!, Inc. v. La Ligue Contre Le Racisme Et L'Antisemitisme, 169 F. Supp. 2d 1181, 1185 (N.D. Cal. 2001) ("translation attested accurate by Isabelle Camus, February 16, 2001"), *rev'd* 379 F.3d 1120 (9th Cir. 2004), *reh'g en banc granted* 399 F.3d 1010 (9th Cir. 2005).

[44] T.G.I. Paris, May 22, 2000 (emphasis added), *at* http://www.legalis.net/jurisprudence-decision.php3?id_article=175. Note that this language comes from the original interim order that Yahoo! translated. This exact language was then repeated by the French court in the confirmation of the interim order. *See* T.G.I. Paris, Nov. 20, 2000, at 2, *available at* http://www.juriscom.net/txt/jurisfr/cti/tgiparis20001120.pdf. The U.S. proceeding challenged the enforceability of the confirming order, but Yahoo! used the earlier translation in the U.S. proceeding.

[45] *Yahoo!, Inc.*, 169 F. Supp. at 1185 (emphasis added).

[46] The relevant provision of the Code Pénal prohibits:

> The act, except for the needs of a film, performance or exhibit that has an historical connotation, the wearing or display or exhibit in public of a uniform, insignia, or sign resembling the uniforms, insignias, or signs that were worn or exhibited either by members of an organization declared criminal by application of Article 9 of the Statutes of the International Military Tribunal annexed to the Treaty of London of August 8, 1945, or by a person found

Since states are understandably concerned with playing a role in regulating illicit Internet activity, they are unlikely to remain passive when those activities conflict with public order rules. Faced with enforcement difficulties at the primary source, state authorities will look to second-order means for the enforcement of public policies. Online intermediaries are at the front lines.[47] In the New York gambling case *People v. World Interactive Gaming*, for example, the state succeeded in obtaining a conviction against an offshore Internet casino,[48] though this victory did not appear to stem the flow of illegal Internet gambling in New York. Consequently, the state sought to prevent Internet gambling by striking at the payment system.[49]

II. THE TECHNOLOGICAL EMPOWERMENT OF STATES: INNOVATION

Ironically, just as the Internet attack uses technological infrastructure to challenge jurisdiction, technological innovation also empowers sovereign states to assert their rules on Internet activity. The evolution of sophisticated information processing and information technologies provides states with greater contacts that justify personal jurisdiction and a stronger claim to prescriptive jurisdiction. At the same time, these technologies offer states important means to enforce their decisions.

---

guilty by a French or international court of one or more crimes against humanity as found in Articles 211-1 to 212-3 or specified by Law No. 64-1326 of December 26, 1964.

CODE PÉNAL [C. PÉN], art. R.645-1, *available at* http://www.legifrance.gouv.fr/WAspad/RechercheSimpleCode?commun=CPENAL&code=r645-1.

[47] *See* Associated Press, *Paypal To Impose Fines for Breaking Porn, Gambling, Drug Bans* (Sept. 13, 2004), *at* http://www.siliconvalley.com/mld/siliconvalley/9654085.htm (discussing PayPal's decision to fine users who violate the site's terms of service to pay for gambling, pornography or pharmaceuticals from non-certified online pharmacies).

[48] 714 N.Y.S.2d 844, 848-50 (Sup. Ct. 1999) (holding that New York State had jurisdiction over an offshore company offering internet gambling to residents of New York).

[49] Press Release, Office of New York State Attorney General, Ten Banks End Online Gambling with Credit Cards (Feb. 11, 2003), *at* http://www.oag.state.ny.us/press/2003/feb/feb11b_03.html (announcing the success of Eliot Spitzer's initiative to obtain agreements from banks to block cardholders from using their cards for online gambling).

A. *Personal Jurisdiction*

At present, the Internet relies on a technical design concept called "end-to-end."[50] This means that the infrastructure operates merely to transmit information from one point to another and any sophisticated processing takes place at the end point. The transmission protocols of the Internet were also designed to be geographically independent. But, users and technologies exist within physical borders and these end points provide justification and capability for sovereign states to assert their authority.

The increasing reliance on end-point processing for sophisticated Internet uses such as multimedia services creates significant interactivity behind the scenes. For example, streaming video purposefully avails itself of the user's computing capability at the user's location. The sophistication of the technology denies the attack against jurisdiction suggested by some Internet separatists precisely because the technical infrastructure depends on interactivity. In *Media3 Technologies, LLC v. Mail Abuse Prevention System, LLC*, Mail Abuse Prevention System (MAPS) created a blacklist of servers that proliferated spam and allowed Internet participants to query the blacklist stored on a server in California.[51] The Massachusetts court found that the availability and query action sufficed for personal jurisdiction in Massachusetts.[52] Similarly, the ubiquitous use of JavaScript, pop-up windows, and fetch commands each enlist resources where the user is located by creating an interaction between a remote web service and the processing resources of the user's computer. These interactions target users at the users' locations.

The most telling example comes from filtering. Web sites and Internet service providers often design or filter content based on user location. RealNetworks, for instance, only streams soccer games to users in particular countries, and some web sites display prices in currencies matched to the user's location.[53] Similarly, Yahoo! offered banner advertisements in French to visitors to a California web site screened as originating in France. Verizon, on the other hand, re-

---

[50] *See* Mark A. Lemley & Lawrence Lessig, *The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era*, 48 UCLA L. REV. 925, 930-31 (2001) (discussing the end-to-end infrastructure).

[51] No. 00-CV-12524-MEL, 2001 WL 92389, at *2 (D. Mass. Jan. 02, 2001).

[52] *Id.* at *4-5.

[53] Associated Press, *Geolocation: Don't Fence Web In*, WIRED NEWS (July 12, 2004), *at* http://www.wired.com/news/infostructure/0,1377,64178,00.html (describing technology that allows websites to tailor content based on the location of access).

fused to accept all email originating in Europe in an effort to combat spam.[54] This geolocation of users demonstrates that Internet participants actively target the user's jurisdiction or, as Verizon did, refrain from interacting with users located in particular places.

The result of the technological innovations that make the Internet experience seamless for users is that sovereign states are presented with a stronger basis for the assertion of personal jurisdiction. The technological attack against jurisdiction cannot be justified where information processing resources within the sovereign state are enlisted by remote Internet participants and where sophisticated Internet participants can, if they desire, avoid the global scope of their online activities. In effect, the technological choice either to filter or not to filter becomes a normative decision to "purposefully avail" of the user's forum state. Technological innovation that enhances interactivity also shifts the burden from demonstrating that a jurisdiction was targeted to showing that reasonable efforts were made to avoid contact with the jurisdiction.

B. *Choice of Law*

Technological innovation also supports sovereign states in the claim for prescriptive jurisdiction and the application of their laws to online activity. An infrastructure that takes advantage of facilities or processing capabilities in a state implicates that state's interests. The technical attack that seeks a global benefit from Internet activity without the global burden of responsibility does not.

The European directive on data privacy illustrates this effect. The choice of law provision declares that:

> Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where: . . . (c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.[55]

---

[54] John Leyden, *Verizon Persists With European Email Blockade*, REGISTER (Jan. 14, 2004), *at* http://www.theregister.co.uk/2005/01/14/verizon_email_block/.

[55] Council Directive 95/46/EC, art. 4(1), 1995 O.J. (L 281) 31, 39, *available at* http://europa.eu.int/comm/internal_market/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf.

While the official versions in other languages seem to impose a lesser standard based on the use of "means" within the member state,[56] the consequences of technical innovations that rely on the power of a user's computer to process data appear to justify the application of the law of the user's member state.[57]

In the American context, the Anticybersquatting Consumer Protection Act[58] provides for an in rem action against a domain name even when a U.S. trademark holder asserts a claim against foreign acts by a foreign party. The basis for this assertion of U.S. law is the technical infrastructure that places the registry of domain names in the United States.[59]

As technology increases the points of involvement or attachment in various countries and at the user's location, each of these countries and the user's state has a greater interest in the Internet activity and a greater interest in applying its substantive law to that activity.

C. *Technological Enforcement*

Technological innovations also mean that states can impose liability on those who do not comply with local rules. Technology empowers sovereign states with very potent electronic tools to enforce their policies and decisions even in the absence of a wrongdoer's physical presence or tangible assets.[60] States can use filters and packet interceptors as well as hacker tools like viruses and worms to enforce decisions and sanction malfeasance. These electronic tools might establish electronic borders that prevent offending material and foreign

---

[56] The English and French versions do not use the same terminology. *Compare id.* (using the term "equipment" in the English version) *with* Council Directive 95/46/CE, art. 4(1)(c) (using the term "moyens," or means, in the French version), *available at* http://europa.eu.int/comm/internal_market/privacy/docs/95-46-ce/dir1995-46_part1_fr.pdf.

[57] *See* Peter P. Swire, *Of Elephants, Mice, and Privacy: International Choice of Law and the Internet*, 32 INT'L LAW. 991, 999 (1998) ("Actual enforcement will thus take place under the law of a particular Member State.").

[58] Anticybersquatting Consumer Protection Act of 1999, Pub. L. No. 106-113, 113 Stat. 1501A-545 (1999) (codified as amended in scattered sections of 15, 16, and 28 U.S.C.).

[59] *See* 15 U.S.C. § 1125(d)(2)(A) (2000) (providing for an in rem action by the owner of a mark against a domain name "in the judicial district in which the domain name registrar, domain name registry, or other domain name authority that registered or assigned the domain name is located").

[60] *See* Joel R. Reidenberg, *States and Internet Enforcement*, 1 U. OTTAWA L. & TECH. J. 213, 225-29 (2003) (addressing the enforcement of decisions through Internet instruments).

wrongdoers from entering the state's electronic zone, like the firewall established by China; electronic blockades that prevent offenders from transmitting outside the borders of the wrongdoer's state; or electronic sanctions such as a denial-of-service attack to take down an offender's site.[61]

For democratic societies, adherence to the rule of law means that the use of any technological enforcement instrument necessitates carefully prescribed authorization criteria. Each mechanism implicates important civil, political, and sovereign rights. As with other police powers of the state, legal authority is a prerequisite for the exercise of coercive powers. As a threshold matter, states must have a legal process in place that authorizes the use and choice of technological enforcement tools. This is analogous to the ordinary civil procedure process that requires a winning party to return to court for a subsequent enforcement order if a violator refuses to comply with the initial judgment. Like traditional enforcement instruments, the use of technological tools must be framed by constitutional and public policy limits as well as constraints of international norms.

The basic principle guiding the choice to use a technological instrument or to deploy a specific type of instrument should be that a state only uses the least intrusive means to accomplish the rule enforcement.[62] 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 must be considered. If continuing rule violations pose imminent danger to a state's public order, a state will have stronger justification to take 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 activity, the

---

[61] *Id.*

[62] The principle of "least restrictive means" appears in many areas of U.S. law, particularly in First Amendment cases, as well as in other legal systems. *See, e.g.*, Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n, 447 U.S. 557, 566 (1980) (defining the approach for First Amendment analysis); Turner Broad. Sys., Inc. v. FCC, 520 U.S. 180, 217 (1997) (applying the approach to cable television rules); *see also* Alan O. Sykes, *The Least Restrictive Means*, 70 U. CHI. L. REV. 403, 403-04 (2003) (discussing the approach in the context of the WTO).

technological enforcement tool may be different than if the goal is to compel a violator to pay monetary damages.

The legal pre-conditions for the deployment of technological instruments must satisfy internal constitutional and public policy limits on the use of state power. In the United States, the Due Process Clause of the Fifth Amendment states that "[n]o person shall . . . be deprived of life, liberty, or property, without due process of law,"[63] and the Fourteenth Amendment applies the same standard to actions of the separate states.[64] These limitations necessarily frame the use of technological instruments. Just as due process protections apply to the arrest and incarceration of suspects and the seizure of property,[65] a state cannot escape accountability by conducting an enforcement action online. Similar standards exist in the traditions of other democracies.[66] This means that prior to the deployment of technological instruments, the state must have an adjudicatory process to justify the use of the particular tool.

Since the deployment of any of the technological instruments will not be perfect, a state's constraints on enforcement error must also apply. If, for example, the police search the wrong house by mistake or a search warrant is obviously defective, the victim of the error will often be entitled to redress and the law enforcement officer may be personally liable to the victim.[67] The state should not be able to avoid the standards of liability for mistakes by deploying technological enforcement instruments. However, the conventional acceptance of some error, such as mistakes made on a reasonable basis, should also apply to the deployment of technological instruments.

Beyond mistakes, enforcement error may arise against third-party interests because each technological instrument has a risk of collateral harm or damage. Electronic borders may over-block and prevent third parties' licit activities from entering the state. Electronic block-

---

[63] U.S. CONST. amend. V.

[64] *See id.* amend. XIV, § 1 ("nor shall any State deprive any person of life, liberty, or property, without due process of law").

[65] *See* Denmore v. Hyung Joo Kim, 538 U.S. 510, 531 (2003) (finding that due process was satisfied for detention of alien pending removal hearing); U.S. CONST. amend V (setting forth, in the Takings Clause, due process requirements for the seizure of property).

[66] *See* Thomas M.J. Möllers, *The Role of Law in European Integration*, 48 AM. J. COMP. L. 679, 688-711 (2000) (discussing shared European legal principles).

[67] *See, e.g.*, Groh v. Ramirez, 540 U.S. 551, 563-65 (2004) (holding that an officer who used a clearly invalid warrant to conduct a search was not entitled to qualified immunity).

ades may inadvertently capture non-wrongdoers and will, in any case, block access to the blockade target from third parties in states. Electronic sanctions against a wrongdoer's web server may also simultaneously destroy services for third parties such as email and Internet access.

When an electronic enforcement action prevents third parties from communicating, these types of errors confront basic constitutional protections on free speech and communications. In the United States, the powerful First Amendment jurisprudence will require the state to be able to justify any harm caused by the deployment of technological enforcement instruments under careful scrutiny.[68] Similar principles, though not as expansive as the First Amendment, exist outside the United States. For example, the European Convention for the Protection of Human Rights and Fundamental Freedoms establishes a right to receive information.[69] Article 10(1) of the Convention defines freedom of expression to include the "freedom . . . to receive and impart information and ideas without interference by public authority and regardless of frontiers."[70] This right is not absolute and may be circumscribed for a number of reasons, including "for maintaining the authority and impartiality of the judiciary."[71] In effect, the protections for third parties' freedom of speech and communication force the state to choose technological instruments that are narrowly tailored and that can be justified as essential to achieve the mandated enforcement objective.

Lastly, to the extent that the state uses intermediaries as enforcement agents, overreaching by such "deputized" private actors can violate civil liberties and be imputed to the state. Civil libertarians may also be concerned about the abuse of intermediaries by the state when intermediaries are pressed into law enforcement functions. These objections, however, are not insurmountable obstacles. The response lies in legislation that protects against overreaching and that protects against abuse of intermediaries.

Public international law may constrain states' use of electronic blockades and electronic sanctions. To the extent that these instruments are hostile acts, the U.N. Charter provides:

---

[68] Whether a court should apply a "strict scrutiny" or "intermediate scrutiny" test ought to depend on the type of speech that is harmed.

[69] Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, art. 10, 1 Europ. T.S. No. 5, 213 U.N.T.S. 221.

[70] *Id.* art. 10(1).

[71] *Id.* art. 10(2).

> All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.[72]

However, the deployment of electronic blockades and sanctions against identified wrongdoers hardly seems to be a "use of force" as currently contemplated by the U.N. Charter.[73] The instruments do not attack the foreign state as such nor the foreign state's infrastructure; they attack a wrongdoer located in the foreign state. As noted by the *Restatement (Third) of the Foreign Relations Law of the United States*, "[a] state's law enforcement officers may exercise their functions in the territory of another state only with the consent of the other state, given by duly authorized officials of that state."[74] However, no international human rights convention clearly prohibits "forcible abduction or irregular extradition."[75]

Where electronic blockades and sanctions are the equivalent of seizure and incarceration, customary international law is at best unsettled and therefore not yet mature enough to limit the deployment of online enforcement tools. Furthermore, the U.N. Charter's right of self-defense is also conditioned on an "armed attack."[76] An online enforcement action, even a denial-of-service attack, against a specific private wrongdoer seems very hard to qualify as an "armed attack."

---

[72] U.N. Charter art. 2, para. 4.

[73] *See, e.g.*, Jason Barkham, *Information Warfare and International Law on the Use of Force*, 34 N.Y.U. J. INT'L L. & POL'Y 57, 79 (2001) (noting that information warfare appears to be outside the traditional prohibitions on the use of force in international law); Christopher C. Joyner & Catherine Lotrionte, *Information Warfare as International Coercion: Elements of a Legal Framework*, 12 EUR. J. INT'L L. 825, 834-39 (2001) (arguing that contemporary international law does not have clear restrictions on information warfare); Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885 (1999) (expressing skepticism that even a state attack against another state's network system would be within the U.N. Charter prohibition); Sean P. Kanuck, Recent Development, *Information Warfare: New Challenges for Public International Law*, 37 HARV. INT'L L.J. 272 (1996) (arguing that current international law will need to adapt rules to restrict information warfare).

[74] RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 432(2) (1987).

[75] *Id.* § 432 reporter's note 1.

[76] U.N. Charter art. 51.

The recent Council of Europe Convention on Cybercrime[77] may even provide an international legal obligation for states to use online enforcement tools. The convention provides that signatories "shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences . . . are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty."[78] The official explanatory note indicates that the provision "leaves open the possibility of other sanctions or measures reflecting the seriousness of the offences . . . [and] leaves to the Parties the discretionary power to create a system of criminal offences and sanctions that is compatible with their existing national legal systems."[79]

International economic law, however, may impose limits on the use of an electronic border for enforcement purposes. The Agreement Establishing the World Trade Organization[80] sets out substantive obligations for signatory states to allow cross-border services and information flows. Antigua's recent case against the United States, though, suggests that the WTO constraints will affect the legitimacy of the underlying rules rather than the choice of enforcement mechanisms themselves.[81] Antigua was a haven for Internet gambling operations that faced a substantial loss of business in the United States as a result of U.S. legislation outlawing non-U.S.-licensed operations. Antigua filed a complaint with the WTO against the United States alleging that U.S. laws restricting Internet gambling were in violation of

---

[77] Council of Europe Cybercrime Convention, Convention on Cybercrime, *opened for signature* Nov. 23, 2001, S. TREATY DOC. NO. 108-11 (2003), Europ. T.S. No. 185, *available at* http://conventions.coe.int/Treaty/en/Treaties/Word/185.doc.

[78] *Id.* art. 13 § 1.

[79] Council of Europe, Explanatory Report to the Convention on Cybercrime, ¶ 130 (Nov. 8, 2001), *at* http://conventions.coe.int/Treaty/en/Reports/Html/185.htm.

[80] Agreement Establishing the World Trade Organization, Apr. 15, 1994, 1867 U.N.T.S. 3, *available at* http://www.wto.org/english/docs_e/legal_e/04-wto.pdf.

[81] *See* WTO Panel Report on U.S. Measures Affecting the Cross-Border Supply of Gambling and Betting Services, WT/DS285/R (Nov. 10, 2004) (ruling on the substantive issue of whether the United States can prohibit offshore gambling), *available at* http://docsonline.wto.org/DDFDocuments/t/WT/DS/285R-00.doc. The U.S. has appealed the ruling to the WTO Appellate Body. *See* United States Trade Representative, Statement from USTR Spokesman Richard Mills Regarding the WTO Gambling Dispute with Antigua and Barbuda, Nov. 10, 2004 ("We will vigorously appeal this deeply flawed report . . . ."), *available at* http://www.ustr.gov/Document_Library/Spokesperson_Statements/Statement_from_USTR_Spokesman_Richard_Mills_Regarding_the_WTO_Gambling_dispute_with_Antigua_Barbuda.html; Matt Richtel, *Trade Group Says U.S. Ban on Net Gambling Violates Global Law*, N.Y. TIMES Mar. 26, 2004, at C5 (summarizing the case and noting the decision to appeal).

U.S. trade obligations relating to the cross-border supply of services.[82] The case is interesting because it addresses the legitimacy of the gambling laws themselves and whether the WTO rules bar the substantive provisions of U.S. law. If the final ruling in the case determines that U.S. substantive law contravenes the WTO obligations that the United States accepted, then any enforcement by the United States of the Internet gambling laws would not be a legitimate exercise of state power. International economic law, thus, constrains the state's underlying decisions on rules and policies rather than the choice of enforcement instruments if the decisions and policies are legitimate.

III. A PRESCRIPTIVE HIERARCHY FOR TECHNOLOGY: LEGAL SUPREMACY

The Internet attack on state jurisdiction advocates an important technological determinism that is problematic for the relationship between law and technology. In general, the advocates of denying state jurisdiction would effectively transfer rule-making power to technologists and technologies. Sovereign states, however, have an obligation to protect their citizens and to assure that technologies empower rules of law rather than undermine the protection of citizens; states must be able to assure their citizens' rights within their national territories. As technology enables noxious behavior online, states need ways to prevent and sanction Internet activities that violate their chosen rules of law. This means that states cannot allow technological attacks to defeat their citizens' politically chosen rights.

In effect, the rule of law as expressed by sovereign states must be supreme over technological claims. The rule of law must take precedence over technological choices in establishing the boundaries that society imposes on noxious online behavior. The supremacy of law, at the same time, must provide incentives for innovation and the development of technologies that can support public policy choices made by states.

A. *Prescribing Noxious Behavior*

The Internet attacks against sovereign jurisdiction arise most often when states face critical questions of public values and public order.

---

[82] WTO, Request for the Establishment of a Panel by Antigua and Barbuda, WT/DS285/2 (June 13, 2003), *available at* http://docsonline.wto.org/DDFDocuments/t/WT/DS/285-2.doc.

For example, many of the cases relate to the suppression of hate speech, defamation, pornography, gambling, and music thievery.[83] The technical community argues for its technical solutions rather than legal solutions. However, technology alone cannot resolve the problems of harmful and wrongful conduct online. In the absence of legal obligations, the development of technologies for public policy are typically stymied or rejected. After substantial hype, the technical protocol designed to support privacy policies and international privacy laws, the Platform for Privacy Protection,[84] failed to gain traction in the web community.[85] PICS technology, designed as a non-regulatory answer to the protection of children from Internet pornography, more or less died after the U.S. Supreme Court struck down the Communications Decency Act. Similarly, when technologies exist and are deployed for commercial purposes, they are typically not configured to support public policies. Yahoo!, for example, was already filtering French users to generate advertising revenue, but Yahoo! said it could not filter out those same users in order to comply with French law.[86]

The exponential growth and prevalence of spam, computer worms, and viruses on the Internet illustrate the need for a legal response. These scourges exist through the exploitation of technological innovations and inadequate responses by the technical community. In sovereign states, these noxious behaviors harm business, consumer, and citizen interests. More significantly, these growing security threats jeopardize the very utility of the Internet for communications upon which citizens now rely. As two-thirds of email traffic becomes spam,[87] users respond by reducing their reliance on the Internet for communications.

---

[83] *See supra* notes 10-15.

[84] For the history of P3P and a description of the protocol, see LORRIE FAITH CRANOR, WEB PRIVACY WITH P3P (2002).

[85] Few web sites code their web pages for use with P3P. In addition, the protocol raises a number of important legal issues that pose obstacles to wide deployment. *See* JOEL R. REIDENBERG & LORRIE CRANOR, CAN USER AGENTS ACCURATELY REPRESENT PRIVACY POLICIES? (TPRC 30th Research Conference Paper No. 65, 2002) (discussing legal concerns about privacy agreements, inadvertent deception, and liability related to the accuracy of P3P user agents), *available at* http://ssrn.com/abstract=328860.

[86] T.G.I. Paris, Nov. 20, 2000, at 3, *available at* http://www.juriscom.net/txt/jurisfr/cti/tgiparis20001120.pdf.

[87] *See, e.g.*, John E. Dunn, *Spam Growth Slowing at Last*, TECHWORLD, Jan. 12, 2005, *at* http://www.techworld.com/security/news/index.cfm?NewsID=2922 (reporting that spam represents 67% of all mail).

To counteract noxious online behavior, Internet participants and states will each look to create safe zones on the Internet that are more secure where policy rules apply and are enforced. Indeed, a wide-open, insecure Internet cannot cope with security problems for the average user/citizen, nor will that infrastructure resolve societal debates over hate, pornography, and other online vices.

In contrast to the Internet as a whole, safe zones become jurisdictional zones that are established through architectural designs.[88] Virtual private networks are an increasingly common example. For a zone to be safe, users will need to be authenticated and their interactions authorized by the network infrastructure.[89] Safe zones will by necessity dictate permissible network activities at each entry point and end point of the zone. These zones will consequently contain geographic indicators because wireless access, the new Internet addressing protocol known as Ipv6, and commercial pressure all require geographic localization. These zones then form a focus for the establishment by states of the rule of law. Participants will be located within the territory of states and will have contacts that can be localized within national territories. The design of the safe zones can give Internet participants the freedom of choice to select whether or not their activities give rise to contacts empowering states with personal jurisdiction and the application of local law. Technological innovation should create products and services to enable these participant choices.

B. *The Normative Exercise of State Authority*

States have, as a result, a normative incentive to assert the supremacy of law over technological determinism. As a baseline, the rule of law and public values must drive technical capabilities. Indeed, examples already exist for the supremacy of law over technol-

---

[88] *See* Lawrence Lessig & Paul Resnick, *Zoning Speech on the Internet: A Legal and Technical Model*, 98 MICH. L. REV. 395, 399-404 (1999) (discussing Internet access controls); Andrea M. Matwyshyn, *A Network Theory Approach to Internet Jurisdiction Through Data Privacy*, 98 NW. U. L. REV. 493, 494 (2004) (arguing for a "trusted systems" approach to jurisdiction).

[89] *See, e.g.*, Ross Anderson, *'Trusted Computing' Frequently Asked Questions*, Ver. 1.1 (Aug. 2003) (discussing innovations in access controls), *at* http://www.cl.cam.ac.uk/users/rja14/tcpa-faq.html; CRAIG MUNDIE ET AL., TRUSTWORTHY PAPER 8 (Microsoft White Paper, Oct. 2002), *at* http://download.microsoft.com/download/a/f/2/af22fd56-7f19-47a-8167-4b1d73cd3c57/twc_mundie.doc ("Assertions of identity (that is, authentication) need to be robust, so that taking actions that depend on identity (that is, authorization) can be done reliably.").

ogy. In the United States, the Digital Millennium Copyright Act prohibits the sale and manufacture of devices that circumvent technological protections on digital works.[90] The Communications Assistance for Law Enforcement Act requires a wiretap-ready capability for new digital telecommunications infrastructure.[91] Outside the United States, other governments have experimented with a similar approach. The French Law for Trust in the Digital Economy requires service providers to inform their clients of the availability of filtering technologies and to include features enabling clients to report illicit content.[92] The 1997 German Teleservices Data Protection Act even had a rule that required special alerts for the use of "cookies" technology.[93]

By using public values to drive technical rules, the exercise of state jurisdiction promotes the development of more granular technologies. The assertion of state jurisdiction as hierarchically superior to technology provides an important incentive for technologists to create more refined technologies that allow communities to define their own rules. For example, content filtering technologies exist as a result of pressure from the U.S. Congress,[94] and the widely used e-commerce product, .NET Passport, was structured more carefully to enable compliance with European data privacy rules only after European regulators persuaded Microsoft to modify the product design.[95] To the ex-

---

[90] 17 U.S.C. § 1201(a)(2) (2000).

[91] 47 U.S.C. § 1002(a)(1) (2000).

[92] Loi no. 2004-575 du 21 juin 2004 pour la confiance dans l'economie numerique, J.O., 22 juin 2004, p. 11168, A.L.D., July 1, 2004, 1868, *available at* http://lexinter.net/lois4/loi_du_21_juin_2004_pour_la_confiance_dans_l'economie_numerique.htm.

[93] *See* Gesetz über den Datenschutz bei Telediensten (Teledienstedatenschutzgesetz—TDDSG), v. 22.7.1997 (BGB1. I S.1870), § 3(5) (requiring that teleservices users be informed about the nature and use of any personal data collected). This was enacted as Article 2 of Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations-und Kommunikationsdienste-Gesetz—IuKDG), v. 22.7.1997 (BGB1. I S.1870). An English translation of the statute is available at http://www.iuscomp.org/gla/statutes/TDDSG.htm. For a more detailed examination of section 3(5), see REIDENBERG & SCHWARTZ, *supra* note 36, at 71-72.

[94] *See, e.g.*, Paul Resnick & Jim Miller, *The CDA's Silver Lining*, WIRED, Aug. 1996, at 109, 109 (noting that "[t]he original goal [of PICS filtering technology] was to empower parents and teachers to provide kid-safe lenses. As a bonus, however, PICS provides a general labeling infrastructure that is now available for all kinds of uses."), *available at* http://www.wired.com/wired/archive/4.08/silver_pr.html.

[95] *See* ARTICLE 29 DATA PROTECTION WORKING PARTY, WORKING DOCUMENT ON ON-LINE AUTHENTICATION SERVICES, at 4, E.U. DOC. 10054/03/EN WP 68 (Jan. 29, 2003) ("As a result of this very open and fruitful dialogue Microsoft has committed itself to make changes to the system delivering improvements from the data protection perspective."), *available at* http://europa.eu.int/comm/internal_market/privacy

tent that granular technologies increase geolocation features and combine them with blocking capabilities, such technologies will enhance respect for sovereign states by empowering compliance with the rule of law in those states. In other words, these technologies enable Internet participants to respect the legal obligations in states where their Internet activities reach rather than prevent compliance with local law. As a corollary, the assertion of jurisdiction by states over Internet participants provides a powerful incentive for innovation in technical capabilities in precisely the manner that strengthens the authority of law in the face of technological attacks. This approach creates new markets for technologically-based compliance services and products.

In contrast, if the law accepts technological attacks, then there is little incentive for technical developers to innovate in ways that support public values. Two recent cases illustrate this problem of technologically dependent decision making. In *Reno v. ACLU*, Justice O'Connor noted that if technology were available that could offer less restrictive means to block access to minors, then the constitutional objections to the Communications Decency Act (CDA) might be more easily resolved.[96] Justice O'Connor assumes that the court's decision will have a neutral effect on technical developments and ignores whether the decision will undermine the incentives to develop technologies that might better protect children.

More recently, in the *Center for Democracy & Technology v. Pappert*,[97] a federal district court faced a constitutional challenge to the Pennsylvania statute that required web filtering to block children's access to pornography. The court took the same position:

> [T]he Court concludes that, with the current state of technology, the Act cannot be implemented without excessive blocking of innocent speech in violation of the First Amendment. . . . [G]iven the current design of the Internet, the Act is unconstitutional under the dormant Commerce Clause because of its affect[sic] on interstate commerce.[98]

/docs/wpdocs/2003/wp68_en.pdf.

[96] 521 U.S. 844, 891-92 (1997) (O'Connor, J., concurring) ("Although the prospects for the eventual zoning of the Internet appear promising, I agree with the Court that we must evaluate the constitutionality of the CDA as it applies to the Internet as it exists today.").

[97] 337 F. Supp. 2d 606 (E.D. Pa. 2004).

[98] *Id.* at 611.

Again, the federal court allowed the technological attack instead of requiring that the technology support a public policy of protecting children from pornography.

Both courts assumed that technologies were static or, at least, that technological developments were outside the law. This assumption is wrong. Technology is dynamic and reacts to legal jurisdictional claims. Had the courts imposed responsibility on Internet service providers, those providers would have had a strong incentive to rapidly develop technologies that would allow more refined filtering for users' geographic reach and content selection. Such developments would support important public values as defined by state legislatures. The opposite occurs when states do not insist on respect for their public values. Technologies attack state jurisdiction and there is little incentive to build in capabilities that can comply with state laws.

* * *

In summary, the assertion of sovereign jurisdiction to protect citizens is likely to advance the fundamental public policy that the rule of law should be supreme to technological determinism. At the same time, the multiplicity of states with jurisdiction over Internet activities is likely to stimulate creativity and new Internet services such as more accurate and selective filtering technologies, stronger security zones and more robust, customized compliance capabilities.