

CYBERLAW 2.0

MICHAEL GEIST*

Abstract: This Article outlines two versions of cyberlaw. The first, characteristic of the scholarship of the late 1990s, is typified by a borderless Internet and national laws that cease to have effect at their real-space borders, the regulatory power of code, and the virtue of self-regulatory solutions to Internet and e-commerce issues. In Cyberlaw 2.0, the borderless Internet becomes bordered, bordered laws become borderless, the regulation of code becomes regulated code, and self-regulation becomes industry consultation, as government shifts toward a more traditional regulatory approach. The Article assesses each of these changes, calling attention to recent developments in copyright law, domain name dispute resolution, privacy, and Internet governance. At the heart of each is the question of the appropriate governmental role in Internet regulation and the need for cyberlaw to reconcile how government and regulation fit within the tensions of ever-changing technologies.

The private sector should lead. Though government played a role in financing the initial development of the Internet, its expansion has been driven primarily by the private sector. For electronic commerce to flourish, the private sector must continue to lead.

—President William J. Clinton and Vice President Albert Gore, Jr.,
Framework for Global Electronic Commerce, October 1997¹

* Canada Research Chair in Internet and E-commerce Law, University of Ottawa, Faculty of Law and Technology Counsel, Osler, Hoskin & Harcourt LLP. The author would like to thank the Social Sciences and Humanities Research Council of Canada for its support through the Initiative on the New Economy grant program; Goldie Bassi, William Karam, and Candice Teitlebaum for their research assistance; Rene Geist, and the participants at the Boston College Symposium on Intellectual Property, the Internet, and Electronic Commerce; the National Law School of India; Yale Law School; Ottawa Centre for Research and Innovation's 45th Circuit; and the Ontario Bar Association E-commerce law section for comments on earlier versions of this paper. Any errors or omissions remain the sole responsibility of the author.

¹ President William J. Clinton & Vice President Albert Gore, Jr., Framework for Global Electronic Commerce (July 1, 1997), at <http://www.ta.doc.gov/digeconomy/framework.htm> (last visited Feb. 3, 2003); see Memorandum on Electronic Commerce, 2 PUB. PAPERS 898, 899 (1997); see also U.S. INFO. AGENCY, A Framework for Global Electronic Commerce, GLOBAL ISSUES, Oct. 1997, at 33, 34 (summarizing principles outlined in the Framework), available at <http://usinfo.state.gov/journals/itgic/1097/ijge/ijge1097.pdf>.

INTRODUCTION

The 1990s was a time of unlimited possibility for the Internet. Fuelled by the seemingly insatiable appetite for anything "cyber," the globe was abuzz over the new economy and the race to replace bricks with clicks. From e-commerce to e-mail, the Internet stood ready to transform society's commercial and communications fabric.

For many, the Internet was also primed to create a sea-change in the law, with many maintaining that fitting traditional regulatory mechanisms into the online environment was the equivalent of squeezing a square peg into a round hole. Governments around the world became early adherents to this belief. Citing the convergence of borderless networks, laws that ended at national borders, and the regulatory power of computer code, governments willingly yielded Internet policy development to private-sector-led, self-regulatory initiatives.²

Today the Internet still represents a medium of great potential but the shine is clearly off the apple. The dot-com crash has led to a reexamination of the impact of the Internet, with many now acknowledging that the opportunity to purchase pet food or CDs online does not a revolution make.³ For many companies and consumers, the Internet is a supplement—not a replacement—to their daily commercial and communication activities.

And what of cyberlaw? It too is undergoing a reevaluation as the new challenges of Internet regulation may not be as insurmountable as we had been led to believe. Version 1.0 of cyberlaw is rapidly giving way to version 2.0, and with it, the emphasis is shifting from a borderless network to borderless law, from code that regulates to code that is regulated, and from self-regulation to government regulation.

This Article explores these two versions of cyberlaw. It argues that we must take note of this metamorphosis because it provides clear signs of the future of Internet regulation. At the core of this examination of cyberlaw is the role of government in the online world. Whether government is characterized as a willing bystander, a powerless policymaker, or a proactive regulatory force that knows no boundaries, cyberlaw must reconcile how government and regulation fit within the tensions of ever-changing technologies.

² See Clinton & Gore, *supra* note 1.

³ See Miguel Helft, *Dog Days for Pet Sites*, STANDARD, Jun. 12, 2000, at <http://www.the-standard.com/article/display/0,1151,15692,00.html>.

I. CYBERLAW 1.0

A. *Borderless Internet, Bordered Laws*

Although no single event or work can lay claim to capturing the early essence of cyberlaw, one e-mail comes close. John Perry Barlow's e-mail, known as the "Declaration of the Independence of Cyberspace,"⁴ served as a clarion call for a new regulatory approach to the Internet, and gave a voice to thousands of "netizens" who watched with increasing anxiety as seemingly overnight the Internet was transformed into a commercial, regulated space. Barlow penned his declaration one day after the U.S. Congress enacted the Communications Decency Act of 1996 (CDA),⁵ the first national U.S. attempt at Internet content regulation. Although relatively unremarkable by today's standards, the CDA galvanized the Internet community into action, culminating with the 1997 U.S. Supreme Court ruling that declared the CDA unconstitutional.⁶ Barlow's declaration left little doubt about his view of the appropriate role for government in cyberspace:

Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather . . . Governments derive their just powers from the consent of the governed. You have neither solicited nor received ours. We did not invite you. You do not know us, nor do you know our world. Cyberspace does not lie within your borders.⁷

The Barlow declaration was soon followed by what is likely the most cited cyberlaw article yet written: David Post and David John-

⁴ John Perry Barlow, A Declaration of the Independence of Cyberspace (Feb. 8, 1996), at <http://www.eff.org/~barlow/Declaration-Final.html>.

⁵ Pub. L. No. 104-104, 110 Stat. 133 (codified as amended in scattered sections of 47 U.S.C.).

⁶ See *Reno v. ACLU*, 521 U.S. 844, 874 (1997) (holding the CDA lacked the precision required by the First Amendment to regulate the content of speech); Electronic Privacy Information Center, EPIC Hails Supreme Court Internet "Indecency" Decision: Opinion "Preserves Both Free Speech And Personal Privacy" (June 26, 1997) (noting that "EPIC joined with the American Civil Liberties Union and 18 other plaintiffs in challenging the law on February 8, 1996, the day it was signed by President Clinton"), at http://www2.epic.org/cda/epic_sup_ct_statement.html.

⁷ Barlow, *supra* note 4.

son's *Law and Borders: The Rise of Law in Cyberspace*.⁸ The Post and Johnson article added legal clout to the passion of the Barlow declaration, positing that cyberspace was cut off from the rule-making institutions of the physical world.⁹ The authors argued that geographic, physical borders are a necessary precondition for effective and legitimate law making because it is within those borders that rules are enforced and legitimated by the general public.¹⁰ They maintained that the Internet undermines this dynamic, suggesting that it operates independent of real space and with no identifiable borders.¹¹ Given this dilemma, Post and Johnson advocated considering cyberspace as a separate "place," governed by its own legal framework.¹² The sole border would be one dividing the virtual from the physical; by entering cyberspace, a person would literally enter a new jurisdiction.¹³ The inhabitants would govern this new space, and the authors advocated a decentralized, self-regulatory model in which Internet users created rules best suited to their needs.¹⁴

Although the Post and Johnson article generated immediate challenges from some scholars with many dismissing the "cyberspace as a place" school of thought,¹⁵ the belief in the virtually insurmountable legal complications created by bordered laws mapped onto a borderless Internet became a truism amongst many observers.¹⁶ In fact, many courts accepted this notion, which is reflected by the reluctance to even consider the possibility of mapping geographic borders to the online world. For example, in *American Library Ass'n v. Pataki*, a

⁸ See generally David R. Johnson & David Post, *Law and Borders: The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996).

⁹ See *id.*

¹⁰ *Id.* at 1368-70.

¹¹ *Id.* at 1370.

¹² *Id.* at 1378-81.

¹³ Johnson & Post, *supra* note 8, 1379.

¹⁴ *Id.* at 1379-81. Post and Johnson have revisited and enhanced their proposal for rule-making in cyberspace. See generally David R. Johnson & David G. Post, *And How Shall the Net Be Governed? A Meditation on the Relative Virtues of Decentralized, Emergent Law*, in COORDINATING THE INTERNET 62 (Brian Kahin & James Keller eds., 1997). Post has also discussed the advantages of rule-making by those using the Internet. See David G. Post, *Anarchy, State and the Internet: An Essay on Law-Making in Cyberspace*, 1995 J. ONLINE L. art. 3, par. 4, at 20-27.

¹⁵ See, e.g., Jack Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199, 1200-01 (1998).

¹⁶ See, e.g., Paul Schiff Berman, *The Globalization of Jurisdiction*, 151 U. PA. L. REV. 311, 314-17 (2002); Adria Allen, Comment, *Internet Jurisdiction Today*, 22 NW. J. INT'L L. & BUS. 69, 69-70 (2001); Timothy B. Nagy, Comment, *Personal Jurisdiction and Cyberspace: Establishing Precedent in a Borderless Era*, 6 COMM'LAW CONSPICUOUS 101, 101 (1998).

Commerce Clause challenge to a New York state law targeting Internet content classified as obscene, the court characterized geography on the Internet in the following manner:

The Internet is wholly insensitive to geographic distinctions. In almost every case, users of the Internet neither know nor care about the physical location of the Internet resources they access. Internet protocols were designed to ignore rather than document geographic location; while computers on the network do have "addresses," they are logical addresses on the network rather than geographic addresses in real space. The majority of Internet addresses contain no geographic clues and, even where an Internet address provides such a clue, it may be misleading.¹⁷

B. *The Regulatory Power of Code*

The second defining principle of cyberlaw was the regulatory power of code—that is, "how the software and hardware that makes cyberspace what it is regulate cyberspace as it is."¹⁸ Although Lawrence Lessig is most closely associated with this principle, due in large measure to his seminal work, *Code and Other Laws of Cyberspace*,¹⁹ others such as Joel Reidenberg were also early advocates.²⁰ As Lessig argued in one of his early pieces, *The Constitution of Code*,

[C]ode . . . regulates behavior in cyberspace. The code, or the software that makes cyberspace as it is, constitutes a set of constraints on how one can behave in cyberspace. The substance of these constraints vary, but they are experienced as conditions on one's access to cyberspace. In some places, one must enter a password before one gains access; in other places, one can enter whether identified or not. In some places, the transactions that one engages produce traces that link the transactions (the mouse droppings) back to the individual; in other places, this link is achieved only if one wants. In some places, one can select to speak a language that only the recipient can hear (through encryption); in

¹⁷ 969 F. Supp. 160, 170–71 (S.D.N.Y. 1997).

¹⁸ LAWRENCE LESSIG, *CODE AND OTHER LAWS OF CYBERSPACE* 6 (1999).

¹⁹ See generally *id.*

²⁰ See Joel R. Reidenberg, *Governing Networks and Rule-Making in Cyberspace*, in *BORDERS IN CYBERSPACE* 84 (Brian Kahin & Charles Nesson eds., 1997)

other places encryption is not an option. The code or software or architecture or protocols set these features; they are features selected by code writers; they constrain some behavior by making other behavior possible, or impossible. They too are regulations.²¹

Lessig's argument, developed in several other articles prior to the release of *Code and Other Laws of Cyberspace*,²² noted that not only could technology influence the regulatory framework, but that it could be the regulatory framework.²³ Reidenberg also called attention to the power of technology, suggesting that traditional American and European approaches to regulatory policy making are ineffective when applied to the Internet.²⁴ Instead, Reidenberg noted that "a network governance paradigm must emerge to recognize the complexity of regulatory power centers, [and] utilize new policy instruments such as technical standardization to achieve regulatory objectives."²⁵

Lessig identified not only the power of the underlying computer code, but foreshadowed the next stage of cyberlaw development: the need for government to "harness" it.²⁶ In *Code and Other Laws of Cyberspace*, Lessig claimed that "not only can the government take . . . steps to reassert its power to regulate, but that it should. Government should push the architecture of the Net to facilitate its regulation, or else it will suffer what can only be described as a loss of sovereignty."²⁷

C. The Virtue of Self-Regulation

In the late 1990s, Lessig's call for government to regulate code went largely unheeded. Buoyed by the perceived potential of e-commerce and claims that governmental intervention would serve only to stifle the development of the Internet, governments were generally all too happy to adopt self-regulatory frameworks that left policy leadership to the private sector. For example, on July 1, 1997, President Clinton released a report entitled *Framework for Global Electronic*

²¹ Lawrence Lessig, *The Constitution of Code: Limitations on Choice-Based Critiques of Cyberspace Regulation*, 5 *COMMLAW CONSPICUOUS* 181, 183 (1997) (citations omitted).

²² See generally Lawrence Lessig, *Constitution and Code*, 27 *CUMB. L. REV.* 1 (1996-97); Lawrence Lessig, *Reading the Constitution in Cyberspace*, 45 *EMORY L.J.* 869 (1996); Lawrence Lessig, *The Zones of Cyberspace*, 48 *STAN. L. REV.* 1403 (1996) [hereinafter Lessig, *Zones*].

²³ See LESSIG, *supra* note 18, at 6.

²⁴ See Reidenberg, *supra* note 20, at 96-95, 100.

²⁵ *Id.* at 96-100.

²⁶ See LESSIG, *supra* note 18, at 231-34.

²⁷ *Id.* at 199.

Commerce, articulating guiding policy principles, including private sector leadership; avoidance of undue governmental restrictions on e-commerce; the enforcement of a predictable, minimalist, consistent, and simple legal environment for commerce; the recognition of the unique qualities of the Internet; and the facilitation of electronic commerce on a global basis.²⁸ The European Union declaration, released one week after the U.S. framework, followed the United States' lead and called for, among other things, a key role for the private sector, the development of a clear and predictable regulatory framework, and the recognition of the special characteristics and fundamentally transnational nature of the Internet.²⁹

Not surprisingly, global corporations encouraged the self-regulatory approach. For example, the Global Business Dialogue on E-Commerce (GBDe), an e-commerce corporate policy and lobbying group with dozens of multinational corporations among its membership, maintained,

[T]he pace and scope of change requires business to play a leadership role in working with governments, governmental organizations, business groups, consumer organizations and other stakeholders to develop an effective e-commerce framework that is global, market-driven and flexible. . . . [E]-commerce policy solutions should be market-driven and based on industry self-regulation wherever possible.

....

. . . Conventional regulatory structures seem to be less capable of coping with the challenges of converging markets. The GBDe believes priority must be given to self-regulation and policy cooperation rather than over-regulation. Only in providing for continued market dynamism will a policy framework enable the converging process to realize its full potential, as well as allowing electronic commerce to reap the largest benefit from the convergence melting pot.³⁰

²⁸ See *supra* note 1 and accompanying text.

²⁹ See Ministerial Declaration from European Ministerial Conference (Bonn, Germany), Global Information Networks: Realising the Potential (July 6–8, 1997) [hereinafter Ministerial Declaration], at http://europa.eu.int/ISPO/bonn/Min_declaration/i_finalen.html.

³⁰ GLOBAL BUS. DIALOGUE ON ELEC. COMMERCE, GBDE 2000 BROCHURE 2, 7 [hereinafter GBDE 2000 BROCHURE] (on file with the author). Current information on the GBDe is available at <http://www.gbde.org> (last visited Mar. 2003).

Even with the most contentious policy matters, governments frequently seemed willing to oblige industry and the private sector. The Deputy Chairman of Australia's Broadcast Authority, one of the few government agencies among Organisation for Economic Co-operation and Development (OECD) member states actively to enforce an online content regulatory framework,³¹ noted in a 1998 speech,

It is clear that there is a broad level of international consensus emerging about some basic principles for the governance of cyberspace. These have been articulated in North America, Europe and the Asia Pacific region, including Australia The use of the terminology "Legal Framework for Cyberspace" might best be avoided, carrying as it does unnecessary and inappropriate overtones of heavy-handed interference, when what is really being proposed is simply a body of broad principles largely based on the notion of international cooperation, national responsibility and industry self-regulation.³²

Similarly, the European Commission, in conjunction with the European Parliament and the European Council—bodies not known for regulatory reticence—developed an overtly self-regulatory "Action Plan" in 1997.³³

³¹ See Gareth Grainger, *Freedom of Expression and Regulation of Information in Cyberspace: Issues Concerning Potential International Cooperation Principles for Cyberspace*, Address Before the UNESCO International Congress, INFOethics '98: Ethical, Legal and Societal Challenges of Cyberspace and Expert Meeting on Cyberspace Law 15–21 (Sept. 1, 1998) (transcript available at http://www.aba.gov.au/abanews/speeches/online_serv/pdftrf/ggmon98.pdf).

³² *Id.* at 44.

³³ See Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: Action Plan on Promoting Safe Use of the Internet (Nov. 26, 1997), at <http://www.midas.gr/info2000/lab/internetact.doc> (last modified Feb. 17, 2000).

As noted by the Communication:

The European Parliament has stated the need for self-regulation and urged Member States and the Commission to promote co-operation among industry (access and service providers), political decision-makers and users' associations.

The Council requested Member States to encourage and facilitate self-regulatory systems including representative bodies for Internet service providers and users, effective codes of conduct and hot-line reporting mechanisms available to the public. The Commission was requested to foster co-ordination at Community level of self-regulatory and representative bodies and promote and facilitate the exchange of information on best practice in this area.

Implicit in emerging cyberlaw principles was the limited role for government in the regulation of the Internet.³⁴ The borderless Internet perspective suggested that traditional governmental organizations lacked the moral authority to exert regulatory control over the online environment because the relationship between citizen and state changed dramatically given the ability for the "governed" to move freely between online spaces without regard to national borders.³⁵ With the reach of national laws ending at national borders, the right of states to regulate online conduct, which frequently occurred outside national borders, was diminished.

Proponents of regulatory code argued that government was increasingly powerless to regulate the online environment. In the battle between East Coast Code (traditional regulation, which directs behavior) and West Coast Code (regulation, by the software code, of cyberspace), initially West Coast Code would prevail, leaving government without its customary methodology for regulating online behavior.³⁶ Although Lessig acknowledged that government could seek to regulate code, he maintained that its ability to do so was directly related to the type of code or architecture of the Internet in question; thus, open source code is far less regulable than proprietary software code.³⁷

Advocates of self-regulation promoted the view that government was an inefficient and ineffective regulator of the online environment. This was a vision of government as too slow and too removed from the realities of the Internet marketplace—in a sense too Lud-

In the Bonn Declaration, ministers stressed the role which the private sector can play in protecting the interests of consumers and in promoting and respecting ethical standards, through properly-functioning systems of self-regulation in compliance with and supported by the legal system.

Id. (citations omitted). See Ministerial Declaration, *supra* note 29, for the Bonn Declaration referenced above.

³⁴ See Barlow, *supra* note 4.

³⁵ See LESSIG, *supra* note 18, at 190–91.

³⁶ See *id.* at 53, 99, 220–21. East Coast Code has been so-named because in the United States much of traditional regulation originates in Washington, D.C.; the tax code is an example of such traditional regulation. *Id.* at 53. West Coast Code, on the other hand, references the regulation of behavior by the "instructions imbedded in the software and hardware that make cyberspace work." *Id.* Software and hardware code generally originate from programmers located on the West Coast of the United States. *Id.*

³⁷ See *id.* at 107. For an explanation of open source software, see Marshall Brain, What Does Open Source Mean?, HowStuffWorks.com, at <http://computer.howstuffworks.com/question435.htm> (last visited Mar. 24, 2003) (noting that with open source software, the source code to the software is readily available, which allows for modification and customization).

dite—to regulate effectively.³⁸ Far better, self-regulation advocates would argue, to allow those parties who “get it” to set the rules unconstrained by government and guided by self-interest and the market.³⁹

II. CYBERLAW 2.0

Government may have been willing to step aside during the commercial Internet's nascent years, but no longer. With every aspect of the Internet regulatory environment undergoing renewed analysis, the next generation of cyberlaw looks to be dramatically different from its predecessor. In Cyberlaw 2.0, the borderless Internet becomes bordered, bordered laws become borderless, the regulation of code becomes regulated code, and self-regulation becomes industry consultation, as government shifts toward a more traditional regulatory approach. This vision of cyberlaw exacerbates competing policy tensions, pitting government against government, government against industry, and government against citizen.

A. *Bordered Internet, Borderless Laws*

1. Bordered Internet

The vision of a borderless Internet riding roughshod over laws that stop at national borders may have captured the imagination of many in the Internet community in the mid-1990s,⁴⁰ but today it has become increasingly clear that the reverse may actually be true. Supported by businesses unwilling to abandon longstanding business models based on traditional geographic borders, several companies are rapidly creating new tools that allow for effective (though imperfect) geographic identification on the Internet. Governments, meanwhile, unwilling to concede that national laws are limited to national borders, are increasingly turning to explicitly extra-territorial legislation.

The result is an emerging legal framework that threatens the national sovereignty of many smaller countries, though not for reasons one would expect. Version 1.0 of cyberlaw was highlighted by the inability to enforce national laws against activities with local effects occurring outside the jurisdiction, which served as the primary threat to

³⁸ See Donna Wentworth, *Deadline Time*, FILTER 1.3 (1998), at <http://cyber.law.harvard.edu/filter/100198/ifwp.html>.

³⁹ See GBDE 2000 BROCHURE, *supra* note 30, at 3, 4.

⁴⁰ See generally Johnson & Post, *supra* note 8.

national sovereignty. In version 2.0, the greater challenge is proving to be aggressive extra-territorial statutes that hamper states' ability to enforce national law and policy inside the jurisdiction.

Because both business and government share a vested interest in bringing geographic borders to the online environment (albeit for different reasons), it should come as little surprise that technologies facilitating geographic identification have so quickly arrived onto the marketplace. Although critics often point to the inaccuracy of these technologies,⁴¹ few users of the technology actually require perfection.⁴² Businesses either want to target their message to consumers in a specific geographic area or to engage in "jurisdictional avoidance."⁴³ Governments, on the other hand, often want to engage in geographic identification so that they can more easily identify when laws are triggered. For example, the State of Nevada recently enacted legislation that paves the way for the Nevada State Gaming Commission to legalize online gambling.⁴⁴ Jurisdictional identification is central to the new legislation:

The commission may not adopt regulations governing the licensing and operation of interactive gaming until the commission first determines that:

(a) Interactive gaming can be operated in compliance with all applicable laws;

(b) Interactive gaming systems are secure and reliable, and provide reasonable assurance that players will be of lawful age and communicating only from jurisdictions where it is lawful to make such communications.⁴⁵

⁴¹ See Information Technology Association of America, E-Commerce Taxation and the Limitations of Geolocation Tools, at <http://www.ita.org/taxfinance/docs/geolocationpaper.pdf> (last visited Jan. 30, 2003).

⁴² See Anick Jesdanun, *The Potential and Peril of National Internet Boundaries*, S.F. EXAMINER, Mar. 4, 2001, available at <http://www.examiner.com/business/default.jsp?story=b.net.0107>. Following from economic theory, Lessig noted that "[a] regulation need not be absolutely effective to be sufficiently effective." See Lessig, *Zones*, *supra* note 22, at 1405. The same applies to bordering technologies: whether used for targeted marketing or to ensure legal compliance, it need not be perfect. See *id.*

⁴³ See Stephanie Olsen, *Tracking Web Users into European Territory*, CNET NEWS.COM, Apr. 3, 2001, at <http://news.com.com/2100-1023-836361.html>; Bob Tedeschi, *E-Commerce: Borders Returning to the Internet*, NYTIMES.COM, Apr. 2, 2001, at <http://www.nytimes.com/2001/04/02/technology/02ECONOMY.html>.

⁴⁴ Reuters, *Nevada Governor Signs Online Gambling Bill*, CASINO CITY NEWSL., June 19-25, 2001, at <http://newsletter.casinocity.com/Issue41>.

⁴⁵ 2001 Nev. Stat. 3075, 3076.

Geographic identification has actually been utilized on the Internet on a relatively primitive scale for some time. For example, Internet Protocol (IP) lookups, which determine approximate user locations by referencing the user's IP address against databases listing Internet Service Provider (ISP) server locations, had been used by Microsoft until last year to comply with U.S. regulations prohibiting the export of strong-encryption Web browser software.⁴⁶ Although imperfect, the process was viewed as sufficiently effective to meet the standards imposed by the regulations.⁴⁷

Recently, several companies have begun offering more sophisticated versions of these technologies. Akamai, an e-business service and software provider, provides a geographic identification service called EdgeScape, which maps user IP addresses to their geographic location and network point of origin.⁴⁸ This information is then assembled into a database and made available to EdgeScape customers. Each time a user accesses a client's Web site, EdgeScape provides data detailing the country from which the user is accessing the site, the geographic region within that country (i.e., state or province), and the name of the user's origin network.⁴⁹ Similarly, Quova, a California-based company, has developed GeoPoint, which boasts ninety-eight percent accuracy in determining Web users' country of origin and eighty-five percent accuracy when drilling down to the city level.⁵⁰

Businesses are implementing these technologies with increasing frequency as they seek to replicate offline business models online. For example, CinemaNow Inc., a California-based online distributor of feature-length films, uses the technology to limit distribution of the films to ensure compliance with distribution-license agreements that

⁴⁶ See Jesdanun, *supra* note 42; see also Jeff Tyson, *How Internet Infrastructure Works*, at <http://computer.howstuffworks.com/internet-infrastructure.htm> (last visited Mar. 24, 2003) (overview of how the Internet works).

⁴⁷ See *id.*

⁴⁸ For the company's Web site, see Akamai.com; for company facts and figures, see http://www.akamai.com/en/html/about/facts_figures.html (last visited Mar. 2003). For information on Akamai's Edgescape offering, see Products & Services, Edgescape, at <http://www.akamai.com/en/html/services/edgescape.html> (last visited Jan. 30, 2003).

⁴⁹ Edgescape can identify a customer's physical location (country, region, city, area code, zip code, etc.), network (connection type, e.g., dial-up; network name, e.g., AOL; actual connection speed), and corporate identity (company name, domain name). See How It Works, Akami, at http://www.akamai.com/en/html/services/edge_how_it_works.html (last visited Jan. 30, 2003).

⁵⁰ See Stephanie Olsen, *Tracking Web Users into European Territory*, CNET NEWS.COM, Apr. 3, 2001, at <http://news.com.com/2100-1023-836361.html>. For Quova's product description, see GeoPoint, at <http://www.quova.com/description/services/geopoint.html> (last visited Jan. 30, 2003).

vary by country.⁵¹ Similarly, Internet users accessing Movielink.com, a U.S. Internet movie rental Web site, who are identified as coming from outside the United States are advised that the site is not available to non-U.S. residents and denied further access to the Web site.⁵² Even Google, the world's most popular search engine, has acknowledged using these technologies to meet variations in local laws by delivering different search results to users in different countries.⁵³

The power to map geography onto the Internet calls into question claims of a borderless Internet. Although many Internet users do indeed experience a "borderless" Internet as they effortlessly visit sites worldwide at the click of a mouse, users themselves are not borderless. They are located in physical places that with increasing frequency can be identified by the Web sites they visit. As Web sites filter content or alter user experiences based on geographic origin, they begin the process of bordering the Internet.⁵⁴ Although previously the same network for all users whether accessed in Atlanta or Auckland, the Internet is fast becoming a bordered medium that varies noticeably depending upon geographic location of the user.

2. Borderless Laws—Copyright

Although the bordered Internet deservedly garners increasing attention, the emergence of borderless digital laws deserves even greater scrutiny. Copyright law, for instance, though typically regarded as national legislation, is increasingly being extended beyond national borders. The case of Dimitri Sklyarov, a Russian software programmer, and his employer, Elcomsoft, illustrates the explicitly

⁵¹ See Patricia Jacobus, *CinemaNow Appeases Studios By Locating Web Surfers*, CNET NEWS.COM, Feb. 26, 2001, at <http://news.com.com/2100-1023-253169.html>.

⁵² See Movielink, at <http://www.movielink.com> (last visited Mar. 2003). Presently, the terms of use include the following:

11. NON-UNITED STATES RESIDENTS. The Services are available only to customers located in the United States of America, excluding its territories. If you are outside of the United States of America, kindly refrain from using the Services. Movielink makes no representation that the Services and any content or products offered on the Services and their copyrights, trademarks, patents, and licensing arrangements, are appropriate or available for use in locations other than in the United States of America.

Terms of Use, Movielink, at <http://www.movielink.com/commerce/help/terms.jhtml> (last visited Mar. 24, 2003).

⁵³ See Declan McCullagh, *Google Excluding Controversial Sites*, CNET NEWS.COM, Oct. 23, 2002, at <http://news.com.com/2100-1023-963132.html>.

⁵⁴ See, e.g., Tedeschi, *supra* note 43.

extra-territorial nature of the Digital Millennium Copyright Act (DMCA), the flagship U.S. digital copyright statute.⁵⁵

Sklyarov, the author of a software program that undermined the encryption used by Adobe in its e-book software, visited Las Vegas, Nevada in July 2001 to present a paper on the strengths and weaknesses of software used to protect electronic books.⁵⁶ When Adobe became aware of his planned appearance, it approached the FBI to seek its intervention into the matter.⁵⁷ Armed with information from the company about the piracy potential of the software program, the FBI prepared an arrest warrant and detained Sklyarov after he delivered his conference presentation.⁵⁸

Spurred by Sklyarov's arrest, the global online community mobilized into action. A "Boycott Adobe" Web site was hastily constructed outlining how Sklyarov's software program featured many legitimate uses, such as the ability to make backup copies of e-books or to read e-books on other devices owned by the same user.⁵⁹ Software programmers voiced their concern, indicating that the arrest would make many think twice before visiting the United States lest they suffer the same fate as Sklyarov (who faced up to twenty-five years in prison, and fines up to \$2.25 million).⁶⁰ Civil liberties groups also became involved, organizing protests at Adobe's offices and expressing dismay that it had become a criminal offense under U.S. copyright law merely to distribute information about a device that could be used to break technology protecting digital copyright.⁶¹

After a month in jail, Sklyarov was released on bail; charges were later dropped against Sklyarov, but charges remained against his em-

⁵⁵ See generally Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 286 (1998) (codified in scattered sections of 17 U.S.C.); Reuters, *Copyright Bill Clears Congress*, WIRED NEWS, Oct. 12, 1998, at <http://www.wired.com/news/politics/0,1283,15571,00.html>.

⁵⁶ Declan McCullagh, *Russian Adobe Hacker Busted*, WIRED NEWS, July 17, 2001, at <http://www.wired.com/news/politics/0,1283,45298,00.html>.

⁵⁷ Declan McCullagh, *Hacker Arrest Stirs Protest*, WIRED NEWS, July 19, 2001, at <http://www.wired.com/news/politics/0,1283,45342,00.html>.

⁵⁸ *Id.*; McCullagh, *supra* note 56.

⁵⁹ See Background & Status, at <http://www.freesklyarov.org> (last visited Jan. 31, 2003).

⁶⁰ See Michelle Delio, *Russian Hacker Charges Dropped*, WIRED NEWS, Dec. 13, 2001, at <http://www.wired.com/news/politics/0,1283,49122,00.html>; Robert Lemos, *Copyright Act Gags Programmers*, ZDNET UK NEWS, Sept. 7, 2001, at <http://news.zdnet.co.uk/story/0,,t269-s2094786,00.html>.

⁶¹ *Adobe E-Book Hacker Released*, WIRED NEWS, Aug. 6, 2001, at <http://www.wired.com/news/politics/0,1283,45870,00.html>; Electronic Frontier Foundation, *Free Dmitry! What You Can Do To Help Set Dmitry Sklyarov Free*, Action Alert (July 17, 2001), at http://www.eff.org/alerts/20010719_eff_sklyarov_alert.html.

ployer, Elcomsoft (which faced fines up to \$500,000).⁶² Elcomsoft's first legal response was to file a motion to dismiss on the grounds that they represented an extra-territorial application of U.S. copyright law against a Russian company that had acted in accordance with its own national law.⁶³ The motion argued,

[A]lthough the importance of regulating the activities prohibited under section 1201 may be significant to the United States, application of the law is not consistent with the traditions of the international system, as its application to a foreign corporation for activities that occurred in cyberspace would conflict with the laws of Russia. Elcomsoft is a Russian company that conducted its activities consistent with the laws of that country. Russian law permits the development and sale of the AEBPR [Advanced eBook Processor] program. If this court were to find that it has jurisdiction over Elcomsoft pursuant to an alleged violation of section 1201 of title 17 of the United States Code, this court would be subjecting Elcomsoft to a law that conflicts with the regulations of another sovereignty.⁶⁴

Although presiding Judge Ronald M. Whyte denied the defense motion to dismiss, finding that the conduct in question occurred in the United States,⁶⁵ the response brief from the U.S. Attorney's Office

⁶² Defense Motion to Dismiss Indictment for Lack of Jurisdiction at 17–18, *United States v. Elcom*, No. CR 01-20183 RMW (N.D. Cal. filed Jan. 14, 2002) [hereinafter *Defense Motion*], available at http://www.eff.org/IP/DMCA/US_v_Elcomsoft/20020114_elcom_dismiss_juris_motion.pdf; Farhad Manjoo & Michelle Delio, *Adobe Hackers: We're Immune*, WIREN News, Mar. 4, 2002, at <http://www.wired.com/news/politics/0,1283,50797,00.html>. On December 17, 2002, a federal jury acquitted Elcomsoft on all criminal charges. Press Release, Electronic Frontier Foundation, Jury Acquits Elcomsoft in eBook Copyright Case (Dec. 17, 2002), at http://www.eff.org/IP/DMCA/US_v_Elcomsoft/20021217_eff_pr.html.

⁶³ Defense Motion, *supra* note 62, at 17–18; Manjoo & Delio, *supra* note 62.

⁶⁴ Defense Motion, *supra* note 62, at 16–17.

⁶⁵ *United States v. Elcom*, No. CR 01-20138 RMW (N.D. Cal. Mar. 27, 2002) (order denying Defense motion to dismiss for lack of jurisdiction), available at http://www.eff.org/IP/DMCA/US_v_Elcomsoft/20020327_dismiss_deny_order.html.

The court noted in the judgment:

The court need not reach the issue of whether the Digital Millennium Copyright Act has extraterritorial application because the trafficking conduct for which defendants have been charged occurred in the United States. The conduct which underlies the indictment includes Elcomsoft's offering its AEBPR program for sale over the internet, from a computer server physically located in the United States. Purchasers obtained copies of the program in

is instructive.⁶⁶ It argued that the plain language of the DMCA clearly applies extra-territorially, noting that section 1201(b), the section at issue, states that it is unlawful to "manufacture, *import*, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof."⁶⁷ According to the U.S. Attorney's Office, the inclusion of the word "import" within the statute demonstrates "Congress' intent to extend the DMCA beyond the borders of the United States."⁶⁸

The *Elcomsoft* jurisdictional issues are not an anomaly—in fact, the DMCA regularly influences behavior outside the borders of the United States, often to the consternation of other countries.⁶⁹ For example, Canada is currently engaged in a digital copyright reform process that is considering how to implement the World Intellectual Property Organization (WIPO) copyright treaties into national legislation.⁷⁰ As part of the reform process, Industry Canada and Canadian Heritage, the two ministries jointly responsible for Canadian copyright policy, sponsored a cross-country consultation involving "town hall" meetings in various cities across Canada in the spring of 2002.⁷¹

At the Ottawa meeting in March 2002, U.S.-based direct-to-home satellite provider DirecTV gave a detailed presentation on the response rate of Canadian ISPs to its DMCA "notice and takedown" no-

the United States. A copy of the program was sold to a purchaser in California. Payments were directed to, and received by, an entity in the United States.

There is sufficient conduct occurring within the United States for there to be subject matter jurisdiction over this matter on a territorial basis.

Id.

⁶⁶ See Government Opposition to Defense Motion to Dismiss for Lack of Jurisdiction at 10–12, *United States v. Elcom*, No. CR 01-20183 RMW (N.D. Cal. filed Feb. 8, 2002) (on file with author).

⁶⁷ *Id.* at 10.

⁶⁸ *Id.*

⁶⁹ See Matt Loney, *ISPs Buckle Under Copyright Cases*, ZDNet UK News, Dec. 10, 2002, at <http://news.zdnet.co.uk/story/0,,t269-s2127279,00.html> (Although anyone can demand the take-down of allegedly infringing material, an ISP's removal of content is "not a simple process" and can leave the "ISPs open to legal action," both "from the person giving notice and from their customers.").

⁷⁰ See GOV'T OF CAN., SUPPORTING CULTURE AND INNOVATION: REPORT ON THE PROVISIONS AND OPERATION OF THE COPYRIGHT ACT, at iv, 43–44 (Oct. 2002), available at <http://strategis.ic.gc.ca/pics/rp/section92eng.pdf>.

⁷¹ See Government of Canada, Consultation Meetings on Digital Copyright Issues, at <http://strategis.ic.gc.ca/SSG/rp00838e.html> (last visited Oct. 12, 2002).

tifications.⁷² DirecTV lamented that "only" forty-three percent of Canadian ISPs responded to its requests to remove content, seemingly oblivious to the fact that many Canadians might find it problematic that even one percent of ISPs, much less forty-three percent, would respond to legal requests that did not reflect Canadian copyright law or policy.⁷³ The response rate did not surprise many Canadian ISPs, however, who privately acknowledged that they had little alternative but to respond, lest they face the prospect of significant liability for copyright infringement in the United States.

Much the same issue arose in Australia in early 2003. At least one Australian ISP received a demand letter from MediaForce, a U.S. digital copyright solutions company acting on behalf of Warner Bros., which listed several IP addresses it claimed were used illegally to access copyrighted material.⁷⁴ The letter proceeded to demand that the users of the IP addresses be denied access and that their accounts be terminated.⁷⁵

Digital copyright issues have proven to be the most contentious cyberlaw policy matter. Content creators, led by the movie and music industries, have sought greater control over their content in response to concerns over global piracy facilitated by the Internet. Despite widespread agreement on the importance of the issue, there is no consensus on the appropriate policy solutions. The export of U.S. law through a borderless DMCA limits the policy choices of other jurisdictions, because their local companies and citizens frequently face no viable alternative but to abide by the U.S. statute, even where it is inconsistent with local law.

3. Borderless Laws—Domain Names

The aggressive extra-territorial legislative approach is not limited to copyrights. A similar situation unfolded in the United States in the domain name sphere in 1999 with the enactment of the Anticybersquatting Consumer Protection Act (ACPA), which features a unique

⁷² See Michael Geist, *New Net Laws Reach Beyond Borders*, GLOBE & MAIL, June 27, 2002, at B17, available at <http://www.globeandmail.com/servlet/ArticleNews/printarticle/gam/20020627/TWGEIS>.

⁷³ See *id.*

⁷⁴ James Pearce, *US Firm Puts Pressure on Overseas ISPs*, ZDNET UK NEWS, Jan. 14, 2003, at <http://news.zdnet.co.uk/story/0,,1269-s2128644,00.html>.

⁷⁵ *Id.*

in rem jurisdiction provision that almost ensures its extra-territorial application.⁷⁶

The provision is designed to address instances in which the plaintiff, invariably a trademark holder, is unable to assert traditional personal jurisdiction principles because the domain name registrant has no ties to the jurisdiction.⁷⁷ The statute grants trademark holders the right to file a civil action against the domain name itself, which is treated as property based in the United States because the domain name root server resides there.⁷⁸

Several commentators have questioned the constitutionality of the ACPA's in rem provision,⁷⁹ though courts have thus far not hesitated to apply it. For example, the provision surfaced in a dispute between two Canadian parties over the Technodome.com domain name.⁸⁰ Heathmount was a Montreal-based company seeking to develop theme parks in both Canada and the United States.⁸¹ It claimed trademarks in the name "Technodome" in both countries.⁸² The owner of the technodome.com domain name was a Toronto teenager who worked at a local theatre company.⁸³ Heathmount, as the trademark holder, could have launched a trademark infringement action in Canada where courts have addressed cybersquatting issues on several occasions,⁸⁴ or it could have initiated an Internet Corporation for

⁷⁶ 15 U.S.C. § 1125(d)(2)(C) (2000).

⁷⁷ *Id.* § 1125(d)(2)(A)(ii); R. Polk Wagner & Catherine T. Struve, *Realspace Sovereigns in Cyberspace: Problems with the Anticybersquatting Consumer Protection Act*, 17 BERKELEY TECH. L. J. 989, 992 (2002), available at http://www.law.upenn.edu/fac/pwagner/wagner-struve_acpa.pdf.

⁷⁸ 15 U.S.C. § 1125(d)(2)(C). The provision stipulates that "[t]he owner of a mark may file an *in rem* civil action 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." *Id.*

⁷⁹ See generally Wagner & Struve, *supra* note 77.

⁸⁰ *Heathmount A.E. Corp. v. Technodome.com*, 106 F. Supp. 2d 860 (E.D. Va. 2000), motion to dismiss denied 2000 U.S. Dist. LEXIS 20316 (E.D. Va. 2000), appeal dismissed 2002 U.S. App. LEXIS 475 (4th Cir. 2002).

⁸¹ Electronic Frontier Foundation, *NSI Opposes EFF in Case Seeking Fairness in Where Such Disputes are Heard*, EFFECTOR, Aug. 3, 2001, at <http://www.eff.org/effector/HTML/effector14.17.html>.

⁸² *Heathmount*, 106 F. Supp. 2d at 861.

⁸³ Brief of Appellants at 1, *Heathmount*, No. 01-1153, 2002 U.S. App. LEXIS 475 (4th Cir. Jan. 10, 2002), available at http://www.eff.org/Cases/Heathmount_v_Technodome.com/20010329_appellant_brief.pdf.

⁸⁴ See Press Release, Electronic Frontier Foundation, EFF Argues Website Case Unfair—A Domain's Home Is Its Local Jurisdiction, Not in Virginia (Dec. 5, 2001), at http://www.eff.org/Cases/Heathmount_v_Technodome.com/20011205_eff_pr.html; see also *Saskatoon Star Phoenix Group v. Noton*, [2001] 206 Sask. R. 106; *itravel2000.com Inc.*

Assigned Names and Numbers (ICANN) Uniform Domain Name Dispute Resolution Policy (UDRP) action.⁸⁵ Instead, it chose to launch an ACPA action in Virginia. The Toronto teenager had absolutely no connection to Virginia.⁸⁶ The trademark owner successfully invoked the in rem jurisdiction clause by suing the domain name, rather than its owner.⁸⁷

The court considered the propriety of a U.S. court addressing a suit between two Canadian litigants and concluded:

Plaintiff may not be able to assert the same rights in Canada, which lacks a body of law equivalent to the ACPA and whose enforcement of its trademark laws cannot extend into the United States. Defendants suggest that Canadian intellectual property law, drawing upon recent English case law, might view the registration of a trademark-infringing domain name as an actionable trademark violation. This outcome is particularly likely, Defendants argue, in a case like the one at bar, involving both registration and use of the mark. However, Defendants' prediction of what the Canadian courts will do when presented with this issue is necessarily speculative and provides little support for the argument that Canada is a satisfactory alternative forum for this lawsuit.⁸⁸

Although the application of the ACPA in rem jurisdictional clause might be justified in the *Technodome.com* case on the grounds that Heathmount possessed a U.S. trademark, subsequent decisions have extended the statute further by allowing claims based on foreign trademarks and foreign domain name registrations. In *Barcelona.com v. Excelentísimo Ayuntamiento de Barcelona*, a dispute between the City of Barcelona and the long-time owner of the Barcelona.com domain name, the court ruled that the statute could be applied to the City's Spanish trademark, concluding that Congress makes no distinction between U.S. and foreign marks within the statute's text.⁸⁹ The court

v. Fagen, [2001] 197 D.L.R. (4th) 760; Sprint Communications Co. LP v. Merlin Int'l Communications Inc., [2000] 197 F.C. 44; Bell Actimedia Inc. v. Puzo, [1999] 166 F.C. 202.

⁸⁵ Brief of Appellants at 6, 22, *Heathmount*, No. 01-1153, 2002 U.S. App. LEXIS 475 (4th Cir. Jan. 10, 2002), available at http://www.eff.org/Cases/Heathmount_v_Technodome.com/20010329_appellant_brief.pdf.

⁸⁶ *Id.* at 11.

⁸⁷ *Heathmount*, 106 F. Supp. 2d. at 863.

⁸⁸ *Heathmount*, 2002 U.S. App. LEXIS 475, at 20-22.

⁸⁹ 189 F. Supp. 2d. 367, 376 (E.D. Va. 2002).

did concede that "trademark law has historically been governed and regulated on a national level."⁹⁰

In *Cable News Network v. CNnews.com*, another Virginia court removed virtually all limitations on ACPA in rem actions.⁹¹ It held that because Verisign, a company resident in Virginia, is the exclusive registry for all top-level ".com" domain names, all ".com" domains are essentially American and therefore subject to the ACPA, without regard for where the domains were registered or the location of the litigants.⁹²

Most recently, a federal court in Virginia ruled that an in rem ACPA judgment ordering the cancellation of a domain took precedence over a foreign court order blocking the cancellation.⁹³ The case involved a dispute over the *globalsantafe.com* domain name.⁹⁴ After a U.S. court invoked the ACPA to order the domain name cancelled, the registrant responded by obtaining an order from a Korean court blocking the local registrar from effecting the cancellation.⁹⁵ The legal drama then shifted back to the United States, where the court adopted a "first in time" rule to claim that it was the first to assert jurisdiction over the domain name.⁹⁶ Based on that analysis, the court then ordered Verisign, which maintains the root server, to override the local registrar by deleting the domain in question from the root server.⁹⁷

Given the broad interpretation accorded to the ACPA's in rem jurisdiction provision by U.S. courts, it is increasingly apparent that the United States has created a domain name dispute resolution policy with global application. This creates a significant limitation on the ability of countries to develop their own domain name policies, because the ACPA has an effect akin to global law and will remain an option to potential litigants independent of their national law and policy.

⁹⁰ *Id.*

⁹¹ 162 F. Supp. 2d. 484, 492 (E.D. Va. 2001).

⁹² *See id.*

⁹³ *Globalsantafe Corp. v. Globalsantafe.com*, No. Civ.A.01-1541-A, 2003 WL 261772, at*11-12 (E.D. Va. Feb. 5, 2003).

⁹⁴ *Id.* at *1-2.

⁹⁵ *Id.* at *1.

⁹⁶ *Id.* at *10-11.

⁹⁷ *Id.* at *1, *12.

4. Borderless Laws—Privacy

Several countries have adopted privacy legislation that is borderless in approach. In the United States, the Children's Online Privacy Protection Act (COPPA) applies to commercial Web sites and online services directed to, or that knowingly collect information from, children under the age of thirteen, and contains no limitation on jurisdictional applicability.⁹⁸ The statute simply renders it unlawful to collect personal information from a child without parental consent.⁹⁹

The Federal Trade Commission (FTC) is vested with responsibility for enforcing COPPA, and although it has yet to pursue any action against a foreign-based site, its rule-making guidance leaves no doubt that such sites are expected to comply with the statute in their privacy practices toward children.¹⁰⁰ FTC regulations expressly apply to any Web site operator, which is defined as

any person who operates a website located on the Internet or an online service and who collects or maintains personal information from or about the users or visitors to such website or online service, or on whose behalf such information is collected or maintained, where such website or online service is operated for commercial purposes, including any person offering products or services for sale through that website or online service, involving commerce:

- (a) Among the several States or with one or more foreign nations;
- (b) In any territory of the United States or in the District of Columbia, or between any such territory and . . . (2) Any State or foreign nation.¹⁰¹

The United States is not alone in extending its privacy-law framework beyond its borders. In May 2002, the European Union's Article 29 Data Protection Working Party released a document that assessed the international application of the E.U. data protection law to personal data processed on the Internet by non-E.U. based Web sites.¹⁰² The Working Party concluded that E.U. law was designed to

⁹⁸ 15 U.S.C. §§ 6501–6506 (2000).

⁹⁹ *Id.* § 6502.

¹⁰⁰ See Children's Online Privacy Protection Rule, 16 C.F.R. § 312.5 (2003); *see also* 64 Fed. Reg. 59,888, 59,891–92 (Nov. 3, 1999).

¹⁰¹ See 16 C.F.R. § 312.2 (defining "operator").

¹⁰² Article 29 Data Protection Working Party, Working Document on Determining the International Application of E.U. Data Protection Law to Personal Data Processing on the

apply in an extra-territorial manner.¹⁰³ Interestingly, the Working Party was comforted by the fact that the U.S. had adopted a similar approach with COPPA.¹⁰⁴

Having determined that the E.U. law applied to foreign-based sites, the Working Party examined the ramifications of applying the law to several commonplace Internet activities.¹⁰⁵ For example, it concluded that the placement of a cookie file on computer users' hard drives was covered by the legislation.¹⁰⁶ Accordingly, Web site owners were required to provide users with adequate notice, specifying in clear terms the information intended to be stored in the cookie, along with the purpose and the life of the cookie.¹⁰⁷

Australia has also incorporated extra-territorial provisions into its amended 1998 Privacy Act.¹⁰⁸ The law, as amended through December 2001, places privacy obligations on both Australian companies as well as foreign companies that conduct business in Australia and collect personal information about Australians.¹⁰⁹ Conscious of its extra-territorial approach, the law contemplates the possibility that foreign companies might face conflicts in meeting compliance requirements of competing privacy statutes.¹¹⁰ In such circumstances, the Australian law cedes jurisdiction to the foreign company's own jurisdiction.¹¹¹

5. Borderless Law—Computer Crime

In the wake of the terrorist attacks of September 11, 2001, and the growing concern over the use of computer networks for criminal purposes, it comes as little surprise to find that computer crime legislation is commonly borderless, with national authorities empowered to apply national criminal legislation against out-of-country activities.

The U.S.A. PATRIOT Act, a mammoth 342-page statute enacted in the fall of 2001, includes provisions that are expressly extra-

Internet by Non-E.U. Based Websites 2 (May 30, 2002) [hereinafter Article 29 Working Party], at http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp56_en.pdf.

¹⁰³ *Id.* at 15.

¹⁰⁴ *Id.* at 4.

¹⁰⁵ *Id.* at 10–13.

¹⁰⁶ *Id.* at 11.

¹⁰⁷ Article 29 Working Party, *supra* note 102, at 11.

¹⁰⁸ Privacy Act, 1988, § 5B (Austl.), available at <http://www.privacy.gov.au/publications/privacy88.pdf> (last visited Jan. 28, 2003).

¹⁰⁹ *Id.* § 5B(1)–(3).

¹¹⁰ *Id.* § 5B(1) (Note).

¹¹¹ *Id.*

territorial.¹¹² The most important such computer crime provision is section 814, which amends the Computer Fraud and Abuse Act.¹¹³ The amendments enhance the U.S. government's ability to prosecute hacking and denial of service attacks by expanding the definition of "protected computer" covered by the legislation.¹¹⁴ The new definition includes "a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States."¹¹⁵ The effect of the provision is to grant U.S. authorities the statutory right to prosecute foreign-based computer fraud and abuse under U.S. law, even if the activity in question may be lawful within its country of origin.

The United States is not alone in this approach. Singapore's Computer Misuse Act also contains a provision that expands its applicability outside the country's borders.¹¹⁶ The Act protects computers from unauthorized access, modification, interception, and interference.¹¹⁷ It intentionally features broad applicability, and section 11 states that "the provisions of this Act shall have effect, in relation to any person, whatever his nationality or citizenship, outside as well as within Singapore . . . [if] . . . the accused . . . the computer, program or data was in Singapore at the material time."¹¹⁸ This section clearly extends the statute's reach to out-of-country persons who hack into Singaporean computer servers or alter Web pages hosted within the country.

Similarly, Malaysia's Computer Crimes Act, which took effect in 2000, includes extra-territorial provisions.¹¹⁹ The Act is designed to address three types of computer crimes: (i) unauthorized access to computer material,¹²⁰ (ii) unauthorized modification of computer

¹¹² Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("USA PATRIOT Act"), Pub. L. No. 107-56, 115 Stat. 272.

¹¹³ *Id.* § 814 (amending 18 U.S.C. § 1030 (2000 & West. Supp. 2002)).

¹¹⁴ *Id.* § 814(a) (amending 18 U.S.C. § 1030(e)(2)).

¹¹⁵ *Id.* § 814(d)(1) (amending 18 U.S.C. § 1030(e)(2)(B)).

¹¹⁶ Computer Misuse Act, 1998, Cap 50A, § 11 (Singapore), available at <http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan002107.pdf>.

¹¹⁷ *Id.* §§ 3-8.

¹¹⁸ *Id.* § 11.

¹¹⁹ Computer Crimes Act, 1997, § 9 (Malaysia), available at <http://www.mycert.mimos.my>; Government of Malaysia, Multimedia Super Corridor (MSC), Malaysian Cyberlaws, at <http://www.msc.com.my/mdc/infrastructure/cyberlaws.asp> (last visited Mar. 24, 2003).

¹²⁰ Computer Crimes Act, 1997, § 3, 4 (Malaysia).

material,¹²¹ and (iii) wrongful communication.¹²² Section 9(1) focuses on the territorial scope of the Act, providing,

The provisions of this Act shall, in relation to any person, whatever his nationality or citizenship, have effect outside as well as within Malaysia, and where an offence under this Act is committed by any person in any place outside Malaysia, he may be dealt with in respect of such offence as if it was committed at any place within Malaysia.¹²³

In light of notorious cases such as the global dissemination of the "Love Bug" virus—which wreaked havoc with computer systems worldwide but went largely unpunished due in part to inadequate computer crime legislation in the Philippines¹²⁴—the desire for computer crime legislation that targets perpetrators regardless of location is understandable. Achieving commonly agreed cybercrime standards, however, is more challenging than is often acknowledged. For example, the recently enacted Council of Europe Cybercrime Convention¹²⁵ adopts a very broad definition of cybercrime that includes offences related to copyright, thus leading to the possibility of criminal action in one jurisdiction against activity that is legal in another.¹²⁶ Although certain jurisdictions may be comfortable equating copyright infringement with cybercrime, it is likely that others will shy away from that approach, resulting in jurisdictional conflicts over the issue.

6. Borderless Law—Online Gambling

Countries are also increasingly willing to extend their regulatory authority over online gambling. For example, Australia recently enacted the Interactive Gambling Act of 2001, creating a detailed legislative scheme that regulates Internet gambling sites located outside of Australia.¹²⁷ Given the growing popularity of online gambling in Australia, federal legislators believed it was necessary to establish a statute

¹²¹ *Id.* § 5.

¹²² *Id.* § 6.

¹²³ *Id.* § 9.

¹²⁴ Jane Wakefield, *Man Accused of Love Bug Hack Goes Free*, ZDNET UK NEWS, Aug. 21, 2000, at <http://news.zdnet.co.uk/story/0,,t269-s2080935,00.html>.

¹²⁵ *Convention on Cybercrime*, 109th Sess., ETS No. 185 (Nov. 23, 2002), at <http://conventions.coe.int/Treaty/en/Treaties/Htm/185.htm>.

¹²⁶ *Id.* art. 11.

¹²⁷ Interactive Gambling Act, 2001, §§ 3, 14 (Austl.), available at <http://scaleplus.law.gov.au/cgi-bin/download.pl?/scale/data/pasteact/3/3465>.

that criminalized not only Australians who used online gambling services, but also Web sites providing gambling services to Australians, without regard for location.

Part II of the Act states that it is an offence intentionally to provide an interactive gambling service with an Australian-customer link.¹²⁸ The statute treats a gambling service as having an Australian link if any of its customers are physically present in Australia.¹²⁹ Contravention of the provision is cumulative so that a person who provides an interactive gambling service to an Australian is guilty of a separate offence with each day the service is available.¹³⁰ The Act establishes an exception for those instances in which the gambling service was not aware, and could not have ascertained with reasonable diligence (such as asking for personal data or assessing geolocational traffic data), that the service was being provided to someone with an Australian link.¹³¹

Although some question Australia's ability to enforce its anti-online gambling statute against offshore providers, there is little doubt that Australia has enacted a legislative scheme that counters the ability of users to interact with foreign Web sites under laws that do the same. Moreover, in case there was any doubt regarding the statute's intention, section 14 plainly states that "[u]nless the contrary intention appears, this Act extends to acts, omissions, matters and things outside Australia."¹³² Given that many countries have legalized online gaming,¹³³ it is likely that some offshore gambling sites will find themselves subject to competing and contrary legal systems—operating lawfully within their home jurisdiction, yet acting unlawfully under Australian law.

B. *The Regulation of Code*

Although Lawrence Lessig rightly recognized the regulatory power of code, he may have underestimated the enthusiasm with which government would begin to regulate it.¹³⁴ Lessig called on government to harness the Internet by pushing the architecture of the

¹²⁸ *Id.* § 15(1).

¹²⁹ *Id.* § 8.

¹³⁰ *Id.* § 15(2).

¹³¹ *Id.* § 15(3), (4).

¹³² Interactive Gambling Act, 2001, § 14 (Austl.).

¹³³ See Courtney Macavinta & Jeff Pelline, *Virtual Casinos Bet Big*, CNET NEWS.COM, July 11, 1997, at <http://news.com.com/2009-1023-201333.html>.

¹³⁴ See LESSIG, *supra* note 18, at 3–8.

Internet to facilitate its regulation,¹³⁵ and today it has become apparent that government is responding. If version 1.0 of cyberlaw was characterized by the power of technology to regulate, a defining feature of cyberlaw 2.0 is the government regulation of technology. Interestingly, the regulation of code has not focused on the architecture of the Internet as Lessig anticipated. Rather, government regulation has centered on network end points, where devices access digital content, as well as the design and accessibility of Web sites.

In the United States, the proposed Consumer Broadband and Digital Television Promotion Act, better known as the Hollings Bill, is the archetypal example of the regulation of code.¹³⁶ The Hollings Bill, which never made it out of committee in the Senate, required the Federal Communications Commission and the Registrar of Copyrights to oversee negotiations between representatives of digital media device manufacturers, consumer groups, and copyright owners to reach agreement on security system standards for use in digital media devices.¹³⁷ The resulting security standards would be used to ensure the secure protection of digital content.¹³⁸ Once established, digital device manufacturers would be prohibited from selling devices that do not incorporate the standards.¹³⁹ Moreover, removing or altering the security standards from a work would be prohibited without the prior authorization of the copyright owner.¹⁴⁰

As Lessig argues in *The Future of Ideas*, his follow-up to *Code and Other Laws of Cyberspace*, the danger associated with excessive copyright control rests not just with the implementation of code that controls copying but also with the support provided to these controls through law.¹⁴¹ Lessig is specifically referring to the DMCA, which provides an additional layer of legal protection to copyrights above both the traditional copyright protection and the technical measures protections.¹⁴²

¹³⁵ See *id.* at 6–7.

¹³⁶ See Consumer Broadband and Digital Television Promotion Act, S. 2048, 107th Cong. (Mar. 22, 2002); Declan McCullach, *What Hollings' Bill Would Do*, WIRED NEWS, Mar. 22, 2002, at <http://www.wired.com/news/politics/0,1283,51275,00.html>; see also Declan McCullach, *Tech Firms Fight Copy-Protection Laws*, CNET NEWS, Jan. 23, 2003, at <http://news.com.com/2100-1023-981882.html>.

¹³⁷ Consumer Broadband and Digital Television Promotion Act, S. 2048, 107th Cong. § 3(a) (Mar. 22, 2002).

¹³⁸ See *id.* § 3(d).

¹³⁹ *Id.* § 5.

¹⁴⁰ *Id.* § 6.

¹⁴¹ LAWRENCE LESSIG, *THE FUTURE OF IDEAS: THE FATE OF THE COMMONS IN A CONNECTED WORLD* 179–80 (2001).

¹⁴² See 17 U.S.C. §§ 1201–1204 (2000).

Thus, it would be unlawful to copy a motion picture, unlawful to bypass a DVD's encryption, and unlawful to break that encryption's code.¹⁴³

Similar to the DMCA, the Hollings Bill enhances the protection of copyrights by using the law to mandate control.¹⁴⁴ If successful, the Hollings Bill will illustrate how the law can be used to regulate code, and that success is likely to embolden other policymakers to launch forays into embedding code with regulation.

Other examples of the regulation of code have garnered less attention. The Workforce Investment Act of 1998, which included the Rehabilitation Act Amendments, provided that members of the public with disabilities seeking information or services from federal agencies have access to that information in a manner that is comparable with individuals without disabilities.¹⁴⁵ Moreover, it also required that federal employees with disabilities enjoy equivalent access to information as those without disabilities, forcing all private firms that engage in government procurement to ensure equal access.¹⁴⁶

The implementation of these requirements necessitated the development of new standards for accessing content on the Internet and required any agency seeking to procure federal government contracts to comply with the standard.¹⁴⁷ As a result, the U.S. government specified the design and structure of thousands of Web sites by regulating their code.¹⁴⁸

¹⁴³ See *id.*

¹⁴⁴ See *id.*; Consumer Broadband and Digital Television Promotion Act, S. 2048, 107th Cong. §§ 5, 6 (2002).

¹⁴⁵ See 29 U.S.C. § 794d(a)(1)(A) (2000).

¹⁴⁶ See *id.*

¹⁴⁷ Electronic and Information Technology Accessibility Standards, 36 C.F.R. pt. 1194 (2002); see 29 U.S.C. § 794d.

¹⁴⁸ See 36 C.F.R. § 1994. 22 (2003). The regulation includes the following technical specifications:

- (a) A text equivalent for every non-text element shall be provided (e.g., via "alt", "longdesc", or in element content).
- (b) Equivalent alternatives for any multimedia presentation shall be synchronized with the presentation.
- (c) Web pages shall be designed so that all information conveyed with color is also available without color; for example from context or markup.
- (d) Documents shall be organized so they are readable without requiring an associated style sheet.
- (e) Redundant text links shall be provided for each active region of a server-side image map.

The European Union Data Protection Working Party engaged in a similar exercise in developing regulations for the online automated processing of personal data.¹⁴⁹ Its recommendations specified privacy-friendly browser default settings, limitations on the configuration of cookies, and the elimination of auto-generated forms during software install processes.¹⁵⁰ Although the recommendations also include suggestions for information disclosure, those related to software and hardware configurations also move government into the realm of regulating code.

Although policymakers increasingly appreciate that code regulates, they are also awakening to the corollary—that code can be regulated. Although the regulation of code raises new complications by blending the policy-making attributes of code with more traditional

(f) Client-side image maps shall be provided instead of server-side image maps except where the regions cannot be defined with an available geometric shape.

(g) Row and column headers shall be identified for data tables.

(h) Markup shall be used to associate data cells and header cells for data tables that have two or more logical levels of row or column headers.

(i) Frames shall be titled with text that facilitates frame identification and navigation.

(j) Pages shall be designed to avoid causing the screen to flicker with a frequency greater than 2 Hz and lower than 55 Hz.

(k) A text-only page, with equivalent information or functionality, shall be provided to make a web site comply with the provisions of this part, when compliance cannot be accomplished in any other way. The content of the text-only page shall be updated whenever the primary page changes.

(l) When pages utilize scripting languages to display content, or to create interface elements, the information provided by the script shall be identified with functional text that can be read by assistive technology.

(m) When a web page requires that an applet, plug-in or other application be present on the client system to interpret page content, the page must provide a link to a plug-in or applet that complies with §1194.21(a) through (l).

(n) When electronic forms are designed to be completed on-line, the form shall allow people using assistive technology to access the information, field elements, and functionality required for completion and submission of the form, including all directions and cues.

(o) A method shall be provided that permits users to skip repetitive navigation links.

(p) When a timed response is required, the user shall be alerted and given sufficient time to indicate more time is required.

Id.

¹⁴⁹ Data Protection Working Party, Recommendation 1/99 on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware (Feb. 23, 1999), at http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp17en.htm.

¹⁵⁰ See *id.*

government policy of regulating code, these complications are not necessarily a bad thing. For example, the regulation of code need not stop at mandating the inclusion of anti-copying technologies within all digital devices: it could be extended to require the retention of fair use rights within the implementation of such technologies, thereby using regulation of code to maintain the copyright balance.¹⁵¹

C. *The End of Self-Regulation*

Government may have been willing to yield policy-making leadership to the private sector in the mid-1990s, but as the volume of regulatory activity highlighted above suggests, cyberlaw regulation has become commonplace. Government typically consults with industry and consumer groups on their preferred approach, but it is unwilling to remain silent on matters of cyberlaw policy.

Nowhere is the shift away from self-regulation more evident than in the world of Internet governance. As the Internet blossomed from a small community of users to a global phenomenon in the mid-1990s, the governance of the domain name system underwent a similarly dramatic change. Once administered by Jon Postel, a computer scientist at the University of Southern California, in 1998, the U.S. government handed over management of domain names to ICANN, a California nonprofit company.¹⁵² ICANN's initial creation drew interest from a diverse group of stakeholders including Internet users, domain name registrars, technical groups, and intellectual property law associations.¹⁵³ Although each group offered differing perspectives on issues such as domain name dispute resolution and the creation of new domain name suffixes, there was widespread agreement on one key principle: ICANN was to be based on a self-regulatory model in which the stakeholders governed themselves, free from government interference.¹⁵⁴

¹⁵¹ See *supra* notes 18–37, 134–143 and accompanying text.

¹⁵² Milton Mueller, *ICANN and Internet Governance: Sorting through the Debris of 'Self-Regulation'*, 1 INFO 497, 498, 500 (Dec. 1999), available at <http://www.icannwatch.org/archive/muell.pdf>.

¹⁵³ *Id.* at 499.

¹⁵⁴ *Id.* at 508–09; see M. Stuart Lynn, President's Report: ICANN—The Case for Reform (Feb. 24, 2002), at <http://www.icann.org/general/lynn-reform-proposal-24feb02.htm> (last modified Feb. 27, 2002) ("ICANN's assigned mission . . . [is] to create an effective private sector policy development process capable of administrative and policy management of the Internet's naming and address allocation systems.").

Self-regulation was premised on a consensus-based approach in which policy discussion was open to all, supported by a governance structure that ensured representation at the board level for all stakeholders.¹⁵⁵ This latter goal was to be achieved by allocating half the board positions among several stakeholder groups, and by completing the other board seats with online elections, thus enabling Internet users to elect board representatives on a regional basis.¹⁵⁶

With ICANN currently engaged in major reforms, supporters and critics alike have begun to look to governments to become more engaged.¹⁵⁷ ICANN supporters want to bring government (and its financial resources) into the fold by elevating the role government plays on the ICANN board through the Government Advisory Committee,¹⁵⁸ the body that currently enables government to play a consultative role within ICANN.¹⁵⁹

ICANN critics, meanwhile, have turned to the U.S. government to call for a reevaluation of the ICANN mandate.¹⁶⁰ Although the Department of Commerce renewed its Memorandum of Understanding with ICANN in September 2002, many critics view the U.S. government as their best ally in pursuing genuine ICANN reform.¹⁶¹

Just as ICANN and its critics turn to government, governments have begun to question openly the ICANN approach, suggesting that more governmental oversight may be needed. For example, U.S. Senator Conrad Burns announced his intention to introduce new legislation that would give the U.S. government greater influence over ICANN.¹⁶² Burns argues that greater influence is needed because

¹⁵⁵ See Mueller, *supra* note 152, at 508–09.

¹⁵⁶ See Internet Corporation for Assigned Names and Numbers, March 2000 ICANN Meeting in Cairo: At Large Membership and Elections, at <http://www.icann.org/cairo/2000/atlarge-topic.htm> (last modified Oct. 6, 2002).

¹⁵⁷ See Lynn, *supra* note 154.

¹⁵⁸ See Internet Corporation for Assigned Names and Numbers, The Internet Domain Name System and the Governmental Advisory Committee (GAC) of ICANN (Oct. 2001), at <http://www.icann.org/committees/gac/outreach-en-01oct01.htm> (last modified Mar. 24, 2002).

¹⁵⁹ See Lynn, *supra* note 154.

¹⁶⁰ See Declan McCullagh, *Congress to Enter ICANN Fray*, WIRED NEWS, Mar. 14, 2002, at <http://www.wired.com/news/politics/0,1283,51041,00.html>.

¹⁶¹ See Anick Jesdanun, *ICANN Gets Another Year*, AUSTRALIAN IT, Sept. 23, 2002, at <http://australianit.news.com.au/articles/0,7204,5148890%5e16123%5e%5enbv%5e,00.html>.

¹⁶² Reuters, *Senate to Scrutinize ICANN More Closely*, STANDARD, Feb. 14, 2001, at <http://www.thestandard.com/article/display/0,1151,22210,00.html>.

ICANN has exceeded its authority, does not operate in an open fashion, and is unaccountable to Internet users.¹⁶³

Similarly, the European Union has argued that governments must have greater involvement in public policy issues, recommending that ICANN always consult governments on policy matters, and that it should be able to ignore or reverse governmental advice only by a two-thirds vote of its board.¹⁶⁴ In 2002, a representative from the Legal Counsel of the United Nations noted how unusual it was to entrust domain name governance to a private body rather than to an international representative body.¹⁶⁵ He argued that the Internet requires international cooperation for both its operation and regulation and that global governmental organizations are uniquely suited to foster such cooperation.¹⁶⁶

Most recently, the International Telecommunications Union, an international body in the United Nations system, issued its clearest signal yet that governments want a larger voice in the Internet governance process.¹⁶⁷ Under the title "Internet Names: A Matter for Both Government and Private Sector," it approved a resolution on the management of multilingual domain names that promotes the role of the government in the internationalization of domain names.¹⁶⁸

A U.S. Congressional proposal to mandate the creation of a "dot-kids" second-level domain name illustrates how government is also engaging in Internet governance on the national, country-code level. The Dot Kids Implementation and Efficiency Act of 2002, passed by the House of Representatives in May of 2002, requires the National Telecommunications and Information Administration (NTIA) to establish a new dot-kids second-level domain within the dot-us country-

¹⁶³ *Id.*

¹⁶⁴ Presidency of the Council of European Union, Preparation of the Transport/Telecommunications Council on 17/18 June 2002—International Management of the Internet and ICANN Reform 5 (June 3, 2002), at <http://register.consilium.eu.int/pdf/en/02/st09/09526en2.pdf>.

¹⁶⁵ Hans Corell, Statement before WIPO Standing Committee on the Law of Trademarks, Industrial Designs and Geographical Indications, Second Special Session on the Report of the Second WIPO Internet Domain Name Process (May 21–24, 2002), Annex I, at 2–3, at <http://www.dnso.org/clubpublic/council/Arc10/pdf00001.pdf>.

¹⁶⁶ *Id.* at 3.

¹⁶⁷ International Telecommunications Union, Plenipotentiary Conference 2002 Highlights, Internet Names: A Matter for Both Government and Private Sector (Oct. 10, 2002) [hereinafter Conference 2000], at <http://www.itu.int/newsroom/pp02/Highlights/1010.html>. For information on the International Telecommunications Union ("ITU"), see <http://www.itu.int> (last visited Mar. 2003).

¹⁶⁸ Conference 2000, *supra* note 167.

code domain.¹⁶⁹ The Act provides that the dot-kids domain allows access only to material that is suitable to children under the age of thirteen.¹⁷⁰

Although it is not uncommon for government to play a role in the management of a country-code domain, mandating the creation of a new second-level domain is rare.¹⁷¹ The legislative proposal illustrates how governments worldwide are seeking a more prominent voice on Internet governance matters, and are no longer content to adhere to the self-regulatory bargain that envisioned private-sector led solutions.

Governments are also abandoning self-regulatory solutions in dealing with unsolicited commercial e-mail or spam. Although the U.S. Direct Marketing Association only recently altered its position that self-regulatory measures were sufficient to address concerns related to spam,¹⁷² it has been clear for some time that government is unconvinced by self-regulatory solutions. With spam now accounting for thirty-eight percent of all e-mail traffic, governments worldwide have begun to adopt aggressive anti-spam legislative initiatives.¹⁷³ The United States has yet to enact federal anti-spam legislation, but dozens of U.S. states now have anti-spam legislation on the books.¹⁷⁴ Moreover, the United States is not alone in the battle against spam, as Japan,¹⁷⁵ South Korea,¹⁷⁶ and the European Union¹⁷⁷ have all enacted anti-spam measures in recent months. Although some governments

¹⁶⁹ Dot Kids Implementation and Efficiency Act § 4, 47 U.S.C. § 941 (Lexis 2003).

¹⁷⁰ *Id.*

¹⁷¹ While some countries, such as Germany and the United Kingdom, have allowed the private sector to manage the national domain name infrastructure without interference, other countries, such as China, India, and Finland have used the government as the direct manager with minimal, if any, public participation.

¹⁷² See Declan McCullach, *Direct Marketers Want Anti-Spam Laws*, CNET NEWS.COM, Oct. 21, 2001, at <http://news.com.com/2100-1023-962821.html>.

¹⁷³ David Lazarus, *Spam Indigestion Worsens*, S.F. CHRONICLE, Oct. 9, 2002, at B1, available at <http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2002/10/09/BU243115.DTL>.

¹⁷⁴ See *id.*; see also Spam Laws: United States: State Laws: Summary, SpamLaws.com, at <http://www.spamlaws.com/state/summary.html> (last visited Jan. 31, 2003).

¹⁷⁵ Christopher Saunders, *Japan Takes Anti-Spam Steps*, INTERNETNEWS.COM, July 11, 2002, at <http://www.internetnews.com/IAR/article.php/1402331>.

¹⁷⁶ Yang Sung-jin, *Powerful Web Site Blocking Spam*, KOREA HERALD, Aug. 22, 2002, available at http://www.koreaherald.com/SITE/data/html_dir/2002/08/22/200208220054.asp.

¹⁷⁷ Reuters, *EU Sticking to Tough Spam Law*, WIRED NEWS, Dec. 6, 2001, at <http://www.wired.com/news/politics/0,1283,48894,00.html>.

profess to remain committed to industry-led anti-spam solutions,¹⁷⁸ the tide is clearly shifting as legislative solutions move to the forefront.

Nowhere is the shift in attitude away from self-regulation more evident than in the area of e-commerce regulation, where visions of private-sector-led policy now represent a bygone era. This is particularly true in relation to consumer e-commerce transactions. Governments have abandoned policies that left these transactions to the private bargains of sellers and purchasers, imposing instead new e-commerce consumer protection measures. For example, the Canadian Province of Manitoba has enacted e-commerce consumer protection legislation that creates new disclosure requirements for sellers and provides purchasers with assurances of recourse in the event that the transaction is not completed as planned.¹⁷⁹

The disclosure requirements include basic information such as the seller's name, business address, and phone number, as well as detailed descriptions of the goods being purchased, applicable warranties, shipping charges, delivery dates, and refund policies.¹⁸⁰ The information can be provided to the buyer via e-mail or posted on the seller's Web site, so long as the buyer can access it prior to purchase.¹⁸¹ The purchaser also has the right to cancel the transaction if the seller fails to comply with the disclosure requirements or fails to deliver the goods within thirty days of the specified delivery date.¹⁸²

The new rules also bring credit card issuers into the equation. If the seller fails to issue a refund after a buyer makes a credit card purchase online and then uses his legal rights to cancel the same transaction, the credit card issuer is required by law to cancel or reverse the

¹⁷⁸ Industry Canada, Electronic Commerce Policy, Consumer Protection, Internet and Bulk Unsolicited Electronic Mail (SPAM), Conclusion, at <http://e-com.ic.gc.ca/english/links/spam.html> (last modified Jan. 22, 2003).

¹⁷⁹ Consumer Protection Act, C.C.S.M., ch. C200, §§ 121–35 (2003) (Manitoba, Can.), available at <http://web2.gov.mb.ca/laws/statutes/ccsm/c200e.php> (unofficial version). The Consumer Protection Act was substantially amended to address Internet agreements by the Electronic Commerce and Information Act, Consumer Protection Amendment and Manitoba Evidence Amendment Act, S.M., ch. 32, §§ 32–36 (2000) (Manitoba, Can.), available at <http://web2.gov.mb.ca/laws/statutes/2000/c03200e.php#36> (unofficial version).

For an overview of Manitoba's consumer protection on the Internet, see Bradley J. Freedman, *Electronic Contracts Under Canadian Law—A Practical Guide*, 28 MANITOBA L.J. 48–51, available at http://www.umanitoba.ca/faculties/law/Journal/back_issues/articles/28_1_freedman.pdf.

¹⁸⁰ Consumer Protection Act, C.C.S.M., ch. C200, § 129(1), 129(2).

¹⁸¹ *Id.* § 129(1) ("Buyer may cancel if not provided information"), (2) ("Electronic methods of providing information").

¹⁸² *Id.* § 130(1) ("Buyer may cancel for failure to deliver"), (2) ("Attempted Delivery").

credit card charge, including any associated interest charges.¹⁸³ If the seller fails to disclose the requisite information to the consumer or does not meet the delivery deadline, the consumer can seek recourse through the credit card issuer, who is required to provide a refund.¹⁸⁴ Moreover, sellers simply cannot ignore these issues because the law itself provides that the rules cannot be avoided or limited by contract—and failure to comply may result in fines or imprisonment.¹⁸⁵

Manitoba is by no means alone in promulgating legislation of this kind. In Canada, it has been followed by Ontario, which recently introduced similar protections in a consumer protection bill.¹⁸⁶ The European Union, which also has protections in place, has aggressively introduced e-commerce consumer protection legislation as part of its E-Commerce Directive¹⁸⁷ and Distance Selling Directive.¹⁸⁸ Moreover, Asian countries have proposed limitations on various other aspects of e-commerce transactions, including restrictions related to online auctions¹⁸⁹ and online dating services.¹⁹⁰

In addition to dictating the terms of e-commerce transactions, government has also intervened by regulating what can be sold online. Several states have enacted restrictions on the online sale of wine,¹⁹¹ automobiles,¹⁹² and cigarettes.¹⁹³ In fact, some states have cre-

¹⁸³ *Id.* § 134(1) ("Buyer's recourse re credit card charges"), (2) ("Credit card issuer must reverse or cancel charges").

¹⁸⁴ *Id.* § 134(1), (2).

¹⁸⁵ Consumer Protection Act, C.C.S.M. ch. C200, § 134(3) ("Application: This section applies despite any agreement to the contrary entered into before or after this Part comes into force.").

¹⁸⁶ News Release, Ontario Ministry of Consumer and Business Services, Ernie Eves Government Introduces Bill to Improve Consumer Protection (Sept. 26, 2002), at <http://www.cbs.gov.on.ca/mcbs/english/5ECQ4C.htm>.

¹⁸⁷ See Council Directive 2000/31 of 8 June 2000 on Electronic Commerce, 2000 O.J. (L 178), available at http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/L_178/L_17820000717en00010016.pdf.

¹⁸⁸ See Council Directive 97/7 of 20 May 1997 on the Protection of Consumers in Respect of Distance Contracts, 1997 O.J. (L 144), available at http://europa.eu.int/comm/consumers/policy/developments/dist_sell/dist01_en.pdf.

¹⁸⁹ E.g., John Markoff, *Auction Sites in Japan Fear Move to Limit Online Sales*, NYTIMES.COM, Feb. 6, 2002, at <http://www.nytimes.com/2002/02/06/technology/06AUCT.html>.

¹⁹⁰ E.g., *Police Consider Legal Action on Internet Dating Sites*, JAPAN TODAY, Oct. 3, 2002, at <http://www.japantoday.com/e/?content=news&cat=2&id=232828>.

¹⁹¹ E.g., Paul Kanoho, *Restrictions on Alcohol Sales on the Internet: Issues of Safety and Freedom*, INTERNET L. JOURNAL.COM, Apr. 16, 2001, at <http://www.tilj.com/content/econheadline04140102.htm>.

¹⁹² E.g., Linda Rosencrance, *Automakers Sue Arizona Over Online Car Sales*, COMPUTER-WORLD, July 13, 2000, at <http://www.computerworld.com/managementtopics/ebusiness/story/0,10801,47090,00.html>.

ated limitations on payment processes by questioning the legality of third-party payment systems such as PayPal¹⁹⁴ and by reaching agreements with credit card issuers to deny approval for online gambling transactions.¹⁹⁵

Government may have once believed that it should not regulate the Internet and Internet-based activity, but this is clearly no longer the case. From macro issues, such as global Internet governance, to micro concerns, such as the physical address of online sellers, government regulation has clearly replaced self-regulation as the cyber-law regulatory method of choice.

CONCLUSION

Although the three principles of Cyberlaw 1.0 may appear distinct, they are in fact tied together by one larger principle—that government would not, could not, and should not apply its traditional regulatory mechanisms to the Internet. The existence of a borderless Internet and bordered laws implies that governments lacked the moral authority to apply their rules to people who had not elected them sovereign. Many of those who focused on the regulatory power of code did so with the belief that traditional lawmaking—East Coast Code in Lessig's parlance—would be unable to regulate activity online as offline.¹⁹⁶ Government may well have believed both of these premises for it enthusiastically adopted industry's mantra that the Internet was different and that it was ill-equipped to flex its regulatory muscle.

No sooner had these principles been accepted than we find them being rapidly undermined. In this emerging cyberlaw framework, government plays the central regulatory role, much as it does for most offline activities. It is being assisted in this regard by technology, which is reshaping the Internet to match more closely its real-space equivalent, complete with borders that mirror those found in a *Rand McNally Atlas*.

¹⁹³ E.g., Todd R. Weiss, *Judge Overturns NY Law Banning Online Cigarette Sales*, COMPUTERWORLD, June 8, 2001, at <http://www.computerworld.com/managementtopics/ebusiness/story/0,10801,61255,00.html>.

¹⁹⁴ Michael Liedtke, *PayPal Warns its Service is About to Shut Down in Louisiana, Casting Cloud over IPO*, NAPLES DAILY NEWS, Feb. 12, 2002, available at <http://www.naplesnews.com/02/02/business/d745055a.htm>.

¹⁹⁵ Press Release, Office of New York State Attorney General Eliot Spitzer, *Financial Giant Joins Fight Against Online Gambling* (June 14, 2002) (outlining agreement in which leading credit card issuer Citibank agreed to block key Internet transactions), at http://www.oag.state.ny.us/press/2002/jun/jun14a_02.html.

¹⁹⁶ See *supra* text accompanying notes 36–37.

In many respects, the changing cyberlaw environment creates greater challenges than its predecessor. Private-sector-led policy envisioned the likelihood of policy disputes, but was content to grant private parties the room to sort through those disputes through contractual mechanisms free from government interference. The popularity of borderless laws escalates these disputes to the international level. Private parties will still face policy disputes, but they will now be joined by countries who, burdened by the extra-territorial application of foreign laws, struggle to assert national sovereignty over policy choices.

The regulation of code, meanwhile, creates many of the same concerns as regulation by code. At one level, it transfers the policy choices embedded in code from industry to government. This is a more democratic approach that assuages concerns that industry will act in a self-interested manner at the expense of the general public interest. Although government may be just as likely to make poor policy choices, there is some comfort in knowing that the choices are made by policymakers who are accountable under our system of democracy in ways that corporate officials are not.

At another level, however, government intervention into code poses troubling implications for the innovation process. Government may be well-suited to represent the concerns of consumers and small businesses, but many would doubt whether it is equipped to prescribe Web site specifications, much less mandate the inclusion of new technologies into consumer products.

The replacement of self-regulatory solutions with more traditional forms of government lawmaking also creates new concerns. Although the ICANN experiment illustrates how self-regulation risks rapid devolution into a series of self-interested choices that exclude the public interest, it is by no means certain that government can or will make better choices. In fact, government processes may be so slow as to cause more harm than good. Moreover, the emergence of conflicting regulatory rules on all aspects of e-commerce are likely to cause many companies to forego the benefits of e-commerce, unwilling to bear the burden of a costly regulatory framework.

Although this new version of cyberlaw may indeed present some difficult policy choices, it is important that these issues be addressed through the prism of the real, rather than the construct of the perceived. Cyberlaw 2.0 has arrived, bringing with it a shift from a borderless network to borderless law, from code that regulates to code that is regulated, and from self-regulation to government regulation.