REVIEW

Enforcing Law Online

Orin S. Kerr†

Who Controls the Internet?: Illusions of a Borderless World, Jack Goldsmith and Tim Wu. Oxford, 2006. Pp xii, 226.

Who Controls the Internet? is an entertaining and engaging book. Professors Goldsmith and Wu have written a short and accessible work that makes a straightforward and persuasive argument about the enforceability of law over the Internet. The book's brevity and its anecdotal approach mean that it overlooks a lot of detail; the dynamics of Internet regulation are more complicated than this short volume suggests. Whether this is a blessing or a curse depends on the reader's taste. It makes the book a fun read, but it also keeps the authors from grappling fully with the dynamics of the topics they cover. Either way, *Who Controls the Internet?* is an important addition to the literature that deserves to be widely read.

This Review begins with a summary of the book, and next discusses the cyberutopian vision of the Internet that the book targets. It then considers what seems to be the broader question underlying the book: when can law successfully regulate the Internet? It suggests that the effectiveness of a legal regime designed to regulate Internet transactions will depend in large part on four factors: who the law regulates, the cost and political viability of enforcement strategies, how much compliance is needed for the law to achieve its goals, and which side is winning the technological arms race at any given time.

I. OVERVIEW OF THE BOOK

Who Controls the Internet? is a manifesto, or perhaps more accurately, a countermanifesto. It targets the "visions of a post-territorial order" popularized during the Internet boom of the mid-1990s (p 13). Internet enthusiasts such as Julian Dibbell and John Perry Barlow

† Associate Professor, George Washington University Law School. Thanks to Lior Strahilevitz, James Grimmelmann, and Jack Goldsmith for comments on an earlier draft. Thanks to Melissa Colangelo for her excellent research assistance.

created a powerful vision of the Internet in the 1990s as "a new frontier, where people lived in peace, under their own rules, liberated from the constraints of an oppressive society and free from government meddling" (p 13). Dibbell's influential 1993 story about enforcing rules in online games[1] suggested that online communities could police themselves without traditional governments (pp 14–17). John Perry Barlow's 1996 *A Declaration of the Independence of Cyberspace* promised a new world of cyberspace that was distinct from the physical world, in which traditional governments "are not welcome" and "have no sovereignty."[2] On a less radical front, many of the Internet's founders believed that the Internet could be governed informally through consensus and engineering excellence rather than through governmental rules (pp 24–25). When the Internet was new, many decisions about Internet standards were made by consensus among engineers who volunteered their time. This arrangement was thought to be a new form of government superior to messy traditional territorial governments (pp 22–25). The vision shared by these Internet pioneers suggested that "the Internet might transcend territorial law and render the nation-state obsolete" (p 10).

Who Controls the Internet? shows that this vision was never realized and suggests a few reasons why. Goldsmith and Wu make their case using nine examples of how traditional territorial sovereignties regulate the Internet. Most readers will be familiar with some of the examples, and some will be familiar with all of them. Goldsmith and Wu tell the stories in sequence, interspersing their commentary, weaving a single narrative that shows the continuing and even "inescapable" vitality of territorial governments. Along the way, they make the case that the Internet is not borderless; rather, government regulation has made the Internet increasingly "bordered" much like the physical world (p ix).

Here are the nine examples in the order they appear:

A. The Yahoo Case

French law prohibits offering Nazi goods for sale in France. In 2000, the American Internet giant Yahoo made such goods available

---

1 Julian Dibbell, *A Rape in Cyberspace: How an Evil Clown, a Haitian Trickster Spirit, Two Wizards, and a Cast of Dozens Turned a Database into a Society*, 38 Village Voice 36 (Dec 21, 1993) (describing how a virtual Internet community reacted to an unruly participant by creating a self-governance scheme).

2 John Perry Barlow, *A Declaration of the Independence of Cyberspace* (Feb 8, 1996), online at http://homes.eff.org/~barlow/Declaration-Final.html (visited Apr 17, 2007).

around the world through its online auction site (p 1). When sued in France for violating French law, Yahoo argued that the company could not comply with French law because it could not make the prohibited goods unavailable in France without taking them offline altogether (p 5). A French judge nonetheless ordered Yahoo to "take all necessary measures" to block visits by Internet users in France to Nazi auction sites available on Yahoo.com (p 5). Faced with the difficulty of blocking access by French users only and the prospect of the seizure of Yahoo-owned assets in France if it failed to comply, Yahoo changed its policy and pulled the auctions to comply with the French court's order (p 8).

B. Jon Postel and Root Authority

The Internet relies on a master naming and numbering authority that provides the key to translating human-readable Internet addresses such as those ending in ".com" or ".edu" into computer-readable Internet addresses like 128.143.28.135. A computer scientist named Jon Postel managed the system starting in 1977 pursuant to a Defense Department contract (p 33). In the 1990s, however, there was a power struggle between established computer scientists such as Postel and United States government officials who had ultimate control over the master naming and number authority. In an ambiguous episode in 1998, Postel may have tried to take command of the authority on his own (pp 43–46).[3] The matter was quickly resolved, however, when White House official Ira Magaziner threatened to sue Postel and his employer unless he immediately returned the authority to the United States government (pp 45–46). Since that time, the United States government has retained unquestioned control over the naming and numbering authority.

C. Geo-ID

In the last five years, a number of commercial services have become available that attempt to identify the geographical location of websurfers (pp 58–62). These so-called Geo-ID services send electronic tracing packets to the computers of Internet users and report back about the major computers that were used to deliver the communications to them. By sending lots of different tracing packets and cross-checking the results with databases of other computers, these

---

[3] Postel asked operators of eight of the twelve regional root servers to recognize his own server as the authoritative root. All eight operators, perhaps out of respect for Postel, immediately complied with his request.

services often can get a rough sense of the physical location of individual websurfers. This tool allows advertisers to feature advertisements of local merchants, helps credit card companies identify fraudulent online purchases, and lets Major League Baseball stream video online without breaching blackout commitments to local television stations (p 61). Geo-ID isn't perfect. For example, it can't locate AOL subscribers given AOL's network configuration, and it can be defeated relatively easily by determined users. But it often works relatively well, and at its best can determine the country of individual Internet users with 99 percent accuracy (p 61).

D. Intermediaries

The experience of Internet users relies on the cooperation of intermediary computers operated by large companies, such as Internet service providers, search engines, and credit card companies. Governments can regulate intermediaries within their jurisdiction, and those efforts often work reasonably well as methods of regulating the experience of Internet users (pp 68–72). For example, governmental pressures on search engines and credit card companies to block certain transactions can help enforce governmental prohibitions on those transactions. Users can work around these limits, but most won't. Because the Internet tends to require cooperation among many entities, it is difficult for computer services to take advantage of safe havens (pp 72–80). This explains the failure of "Sealand," an abandoned concrete tower in the North Sea six miles from the United Kingdom. In 1999, Sealand tried to establish itself as a data haven for companies seeking to escape governmental regulation, but failed in part because no one would cooperate with companies that based services there (pp 65–66).

E. China

The number of Internet users in China passed 100 million in 2005, but the Internet they experience is heavily censored (pp 87–90). The Chinese government has imposed a firewall on all international Internet traffic, and it blocks all traffic between China and certain prohibited IP addresses and domain names outside of China. The Chinese government also administers a massive internal censorship regime. Internet users in China cannot post messages containing forbidden words or criticize the government; the messages will be screened and deleted without being posted, and in some cases may lead to the poster's arrest (pp 95–97). Even less-critical comments are often scrubbed later

by government censors. It is too early to tell whether the Chinese government's efforts will succeed, but they raise the prospect of a very different Internet in China than the one experienced in the rest of the world. Further, the software that makes this censorship possible was designed and is administered by the same U.S. companies that were part of the Internet boom, such as Cisco and Yahoo (pp 93–95).

F. Peer-to-Peer Filesharing

In the late 1990s, millions of Internet users embraced peer-to-peer filesharing services that facilitated the distribution of copyrighted files such as music. However, lawsuits brought by the Recording Industry Association of America (RIAA) put a serious dent in the use of such services. First, the RIAA successfully sued Napster, an early service that used a central directory to facilitate filesharing (pp 106–08). Next, the RIAA successfully sued Grokster, winning an important ruling from the Supreme Court that companies could not legally base a business model on inducing copyright infringement (p 121).[4] Third, the RIAA brought thousands of lawsuits against individual users (pp 114–15). This troubling legal environment paved the way for the success of iTunes, which is supported by the copyright owners and is now as successful as peer-to-peer networks (pp 114–25). In short, traditional territorial copyright law has remained very important.

G. eBay

The enormously popular auction site eBay started on a small scale in 1995, and when it was small it relied on trust and informal dispute resolution (pp 130–32). As it grew, however, eBay came to rely on more traditional forms of government enforcement to ensure that customers could rely on eBay-hosted auctions. Currently, eBay auctions result in traditional binding contracts and its full-time security staff of eight hundred works very closely with law enforcement to fight fraud and help the police investigate eBay-related crimes (p 135). Further, eBay's recent international expansion has concentrated on countries that combine large economies with well-functioning legal systems (pp 143–45). For example, eBay has not expanded to Russia because the Russian legal system is chaotic; contracts are not respected,

---

[4] *Metro-Goldwyn-Mayer Studios, Inc v Grokster, Ltd*, 545 US 913, 919 (2005) ("We hold that one who distributes a device with the object of promoting its use to infringe copyright . . . is liable for the resulting acts on infringement by third parties.").

and the Russian criminal justice system is a failure (pp 144–145).[5] eBay's very successful business strategy reveals that even Internet-based businesses remain profoundly reliant on traditional territorial governments.

H. The Gutnick Case

The Wall Street Journal posted a story on its website in October 2000 suggesting that Australian billionaire Joseph Gutnick had engaged in shady dealings with a convicted money launderer.[6] Gutnick read the story online from Australia, and he brought a libel suit in an Australian court against the Journal's parent corporation, Dow Jones & Company (Dow Jones). Australian libel law is much broader than U.S. libel law. Dow Jones argued to the Australian High Court that it was not bound by the Australian standard because its servers were in the United States; the Australian court disagreed, ruling that the tort of defamation occurs where the person who downloads the material is located (pp 151–54). Dow Jones ended up paying Gutnick AU$180,000 in damages and AU$400,000 to settle the case (p 148).

I. International Agreements and Organizations

The jurisdictional complications of the Internet have led to a number of international disputes and efforts at resolution among traditional territorial governments. For example, government representatives within the Council of Europe created a cybercrime convention, although relatively few countries have joined it. Continuing disagreement over the root authority now focuses on perspectives of representatives of different countries. The World Trade Organization has jumped into the fray over the legality of Internet gambling by adjudicating a complaint by Antigua and Barbados against the United States. Finally, the European Union data protection directive has a global impact on privacy practices in the United States (pp 165–78). In all of these cases, traditional governments are taking the primary role in representing the interests of their citizens in how the Internet is regulated.

* * *

5 See generally, for example, *Blood Money; Corruption in Russia*, Economist 53 (Oct 22, 2005) (providing examples of corruption's constant presence in Russian economic life).

6 The story, Bill Alpert, *Unholy Gains*, Barron's 24 (Oct 30, 2000), was reproduced on the Wall Street Journal's website where it was discovered by Gutnick.

What is the lesson of these nine stories? According to Goldsmith and Wu, the stories teach that traditional territorial governments continue to play a critical role in the development and management of the Internet:

> [P]hysical coercion by government—the hallmark of a traditional legal system—remains far more important than anyone expected. This may sound crude and ugly and even depressing. Yet at a fundamental level, it's the most important thing missing from most predictions of where globalization will lead, and the most significant gap in predictions about the future shape of the Internet (p 180).

In other words, governments matter, even in the Internet age. The utopians of the 1990s were "in the grips of a strange technological determinism that views the Internet as an unstoppable juggernaut that will overrun the old and outdated determinants of human organization" (p 183). But the utopians were wrong, as they failed to see that ultimately it is governments that control the Internet, not the Internet that controls governments. The Internet is not borderless; rather, it is becoming increasingly bordered, and the experience of Internet users increasingly hinges on their physical location. The future of the Internet thus hinges on which governmental visions of the Internet win out: "[S]truggles between nations and their national network ideologies . . . will do much to determine how life on the bordered Internet is lived" (p 184).

II. THE CYBERUTOPIANS

Much of *Who Controls the Internet?* dismantles the "cyberutopian" view of Internet regulation, which predicted a "post-territorial world" in which traditional governments "have no sovereignty." The cyberutopian view amounts to a claim that traditional laws are wholly unenforceable online, and Goldsmith and Wu's anecdotal approach is perfectly suited to demolish this argument (p 81). Goldsmith and Wu mostly let the facts speak for themselves, and their examples of how traditional laws have proven to be enforced online make it hard to take the cyberutopian vision seriously. To be fair, it's not clear how many people today embrace the cyberutopian vision. I would guess its popularity has diminished considerably in the last few years. To the extent that the writings of Barlow and Dibbell continue to be influential, however, *Who Controls the Internet?* offers a powerful response.

It's interesting to consider Goldsmith and Wu's argument alongside work on the origins of Internet culture, such as Fred Turner's new

book, *From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism.*[7] Turner details how the early Internet pioneers were steeped in the 1960s counterculture, and how that influence helped shape early perceptions of the Internet. In particular, Turner traces how the beginning of Stewart Brand's influential "Whole Earth Catalog" in 1968 popularized the combination of countercultural values, rejection of hierarchy, technology, and virtual community that later spread to computers.[8] The Whole Earth Catalog targeted the needs of hippies who had moved to communes in the middle 1960s and who needed to know of the latest social and technological developments for use in their do-it-yourself communities.[9] Brand's catalog offered a virtual networking forum for the sharing of ideas and tools among the back-to-the-landers who had separated themselves from traditional institutions and living arrangements in favor of a new way of nonhierarchical living.[10]

As odd as it seems today, the Whole Earth Catalog had tremendous public appeal in the late 1960s and early 1970s. It sold about 2.5 million copies[11] and won the National Book Award in 1971.[12] Then, in 1985, the Whole Earth Catalog went online with the creation of The WELL, the Whole Earth 'Lectronic Link. The WELL was (and still is)[13] a computer service that that arose in part as an effort to put the Catalog online with the assistance of Stewart Brand.[14] The WELL offered a virtual community for users that self-consciously mirrored the ideology of the Whole Earth Catalog and became wildly successful among early Internet pioneers. Turner suggests that the experience of The WELL exerted a strong influence on early perceptions of the Internet, including those of WELL member John Perry Barlow.[15]

Reading *Who Controls the Internet?* and Turner's new book together helps explain why it is so easy for Goldsmith and Wu to poke

---

7 Fred Turner, *From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism* (Chicago 2006). For another work in this same vein, see John Markoff, *What the Dormouse Said: How the Sixties Counterculture Shaped the Personal Computer* (Viking 2005).

8 See Turner, *From Counterculture to Cyberculture* at 73–81.

9 See id at 73–78.

10 See id at 79.

11 Id at 81.

12 Id at 118.

13 See The WELL, online at http://www.well.com (visited Apr 17, 2007). The webpage welcomes viewers "to a gathering place that's like no other—remarkably uninhibited, intelligent, and iconoclastic." Id.

14 See Turner, *From Counterculture to Cyberculture* at 142 (cited in note 7).

15 See id at 162.

holes in the cyberutopian vision of the Internet. The cyberutopian worldview mirrored the values and experience of The WELL, and The WELL in turn reflected the new communalist lifestyle and countercultural worldview of the Whole Earth Catalog. When experienced WELL users wrote and spoke about their experience during the early Internet boom, they were like explorers of a new world reporting back about their incredible discoveries. But what Barlow and others pitched as the new world of cyberspace in the 1990s was less "the Internet" than the Whole Earth Catalog in cyberspace. It was one application of the Internet that reflected a particular ideology, a particular set of users, and a particular time. Like the blind men feeling the elephant, Barlow and others reported on their experience as if it captured the essence of the Internet. In a sense, *Who Controls the Internet?* shines light on some of the other parts of the elephant.

Of course, it is too simple to trace the cyberutopian vision solely from The WELL. No doubt there were many overlapping influences, of which The WELL was only one. My own pet theory is that the cyberutopian vision is essentially "Consciousness III" from *The Greening of America*, the popular 1970 counterculture manifesto by Yale Law professor Charles Reich.[16] Reich posited that America was witnessing "the revolution of the new generation,"[17] the arrival of a new consciousness free from traditional social, economic, and governmental institutions. Reich's history began with "Consciousness I," the era of free-market individualism, which Reich contended was replaced by "Consciousness II," the era of faith in established government and economic institutions and submission to the "American Corporate State."[18] Reich's book announced the arrival of Consciousness III, a new consciousness in which the bounty of new technologies enabled everyone to live "without the guideposts of the past"[19] in a paradise of individual happiness and experimentation. The revolution of Consciousness III would release people from the constraints imposed by traditional governments and corporations and would replace them with

16 Charles Reich, *The Greening of America* 217–64 (Random House 1970).

17 Id at 4 (arguing that this generation's "protest and rebellion, their culture, clothes, music, drugs, ways of thought, and liberated life-style are not a passing fad").

18 See id at 22 (describing Consciousness I as focused on "self-repression" and individualism and embracing an idealistic philosophy of humanism), 67 (arguing that "acceptance of the priority of institutions, organizations, and society" characterizes Consciousness II). See also id at 89 (describing the connections between Consciousness II and the American Corporate State).

19 Id at 219.

spontaneously formed communities[20] and self-actualization aided by psychedelic drugs such as LSD[21] and the music of the Grateful Dead.[22]

It seems to me that the cyberutopian view is essentially "Consciousness III in Cyberspace,"[23] and that it was bound to be discredited as the Internet grew. Like Consciousness III, the cyberutopian Internet was the revolution of the new generation, a new world that rejected established governments and the American Corporate State in favor of spontaneously formed communities and the pursuit of individual happiness. Just substitute the "consensual hallucination"[24] of cyberspace for the individualized hallucination of LSD and the two match up remarkably closely. Perhaps such a vision seemed plausible when a small and homogenous group of American citizens made up the overwhelming chunk of Internet users. In 1985, the roughly twenty thousand Internet users in the United States were about 90 percent of Internet users worldwide.[25] But eventually the Internet went global. In 2005, the more than 200 million Americans estimated to use the Internet make up only about 17 percent of worldwide users.[26] Today's vast international audience of Internet users is remarkably different from the small homogeneous audience twenty years ago, and today's audience has no more use for Consciousness III online than it does offline.

III. WHEN IS LAW EFFECTIVE ONLINE?

If *Who Controls the Internet?* has a significant flaw, that flaw lies less in what it says than what it doesn't. Goldsmith and Wu correctly note that law is *sometimes* enforceable online. The result is an Internet that can seem "bordered," in that the regulatory effect of traditional law creates a sort of border (p viii). But just as surely as this is *sometimes* true, it is obviously not *always* true, and Goldsmith and Wu don't offer a general framework for explaining when it is true and when it

---

20 Id at 251 (noting that Consciousness III "is beginning to experiment with small communities of different sorts").

21 Id at 258 (remarking that "[o]ne of the most important means for restoring dulled consciousness is psychedelic drugs").

22 Id at 245 (observing that "a pulsing new energy" defined the new music).

23 Fred Turner briefly notes this possible connection as well. See Turner, *From Counterculture to Cyberculture* at 37 (cited in note 7).

24 See William Gibson, *Neuromancer* 5 (Ace Science Fiction 1984) ("[The protagonist] operated on an almost permanent adrenaline high, a byproduct of youth and efficiency, jacked into a custom cyberspace deck that projected his disembodied consciousness into the consensual hallucination that was the matrix.").

25 eTForecasts, *Internet User Forecast by Country*, online at http://www.etforecasts.com/products/ES_intusersv2.htm (visited Apr 17, 2007).

26 See id (noting that in 2005 nearly 1.1 billion people used the Internet worldwide).

isn't. Goldsmith and Wu occasionally discuss why particular regulatory techniques are likely or unlikely to work. However, they don't offer a general account of when law will succeed and when it will fail. This isn't a fatal flaw, as you can always fault authors for not writing the book you wanted them to write. But I think a reader can't help but wonder about this question when reading the book.

What might such an account look like? It might start with the basic dynamic in many of the cases Goldsmith and Wu cover. Computers and the Internet often change how easy it is to violate or comply with the law, and changes that facilitate lawbreaking will tend to trigger a response by those who want greater compliance with legal rules. Computers can make the difficult easy and the easy hard, and those changes will tend to lead to increases in some kind of lawbreaking and decreases in other kinds of lawbreaking. When technology makes lawbreaking easier and compliance more difficult, compliance will decrease. Victims, governments, and businesses seeking greater compliance will either change enforcement strategies, attempt to change substantive legal standards, or look for technical solutions to restore the status quo ante. The result is a struggle over compliance levels between governments and beneficiaries of legal protection on one side and regulated users on the other side. For the sake of simplicity, we can model this as a contest between two sides: pro-enforcement interests and anti-enforcement interests.

This dynamic appears in many of the case studies covered in *Who Controls the Internet?*. For example, peer-to-peer filesharing makes it vastly easier for users to violate copyright laws; copyright owners responded with civil actions against both users and the services themselves. In the Yahoo case, Internet technology made it harder for Yahoo to avoid making its auctions available in France. French users responded with a successful enforcement action against Yahoo that forced Yahoo to take its auctions offline. The same dynamic explains eBay's business strategy. Internet auctions are more prone to fraud than physical auctions because the parties communicate remotely and often anonymously. As a result, eBay will only do business in countries where it can harness the local legal system in response to the new dynamic. Finally, Internet technologies permit Chinese citizens to engage in free speech that is illegal in China; in response, the Chinese government implemented a draconian censorship regime to deter the illegal speech. All four of these examples reflect the same contest between pro-enforcement interests and anti-enforcement interests.

This brings us to the important question: How do we know which side will win out? In other words, when is a legal regime that regulates

Internet users and Internet transactions likely to be effective and enforceable? There are no strict rules here, of course, but I think we can gain some insights by considering four factors: first, whom the law regulates; second, how much compliance is needed for the law to achieve its goals; third, which side is winning the technological arms race at any given time; and fourth, the cost and political viability of enforcement strategies. My sense is that these four factors provide a modestly helpful guide to predicting when and how legal regimes will be effective online.

Let's start with the question of whom the law regulates. Different regulatory schemes can target different types of audiences, and some audiences will prove easier to influence than others. Goldsmith and Wu recognize this point in their discussion of intermediaries (pp 68–72), but the point is worth generalizing. Some legal regimes will target businesses, and others will target users; some will try to alter the behavior of the general public, whereas others will try to change the behavior of a few dedicated wrongdoers. As a general rule, businesses will tend to be easier to regulate than individual users. They are easier to find and less likely to be judgment proof, making them more vulnerable to legal action. Similarly, members of the general public will tend to be easier to regulate than dedicated individuals who are committed (for whatever reason) to violate the law. A modest regulatory countermeasure may encourage the public to comply with legal rules, while the same measure may simply trigger a counter-countermeasure from more dedicated users.

A second principle is that measuring the success of any legal regime depends on the goals it seeks to achieve. There is no absolute measure of success. Some regimes need perfect or close-to-perfect compliance to be effective, and others can be effective if compliance is modest. Compare the enforcement of copyright law in the United States with the enforcement of China's draconian censorship system. If the copyright laws are modestly enforceable, that is likely to be enough; copyright holders merely need to sell enough products to have a significant incentive to create (pp 114–15). On the other hand, China's censorship regime requires greater levels of compliance. It won't achieve its nefarious goals if millions of Chinese can circumvent or otherwise ignore it. The lesson probably is obvious, but still remains very important: imperfect compliance may or may not be adequate depending on the goals of the law.

A third principle is that the success of any online legal regime can be measured accurately only in the near term. The outcome of a struggle between pro-enforcement and anti-enforcement interests depends

on technology, law, social practice, and enforcement strategies. But all four are fluid and dynamic, and when they change, enforceability often changes with them. This leads to what is sometimes referred to as a "technological arms race,"[27] the cat-and-mouse game between pro-enforcement and anti-enforcement interests. Consider the recent history of copyright and copy protections. An abbreviated timeline might go something like this: First, the Internet facilitated copyright infringement. In response, copyright owners tried creating code-based copy and access protections on their digital works. Users responded by creating and distributing programs that circumvented the copy and access protections. Next, copyright owners responded by pushing Congress to prohibit possession and distribution of those programs.[28] Although copy protections are only part of the broader picture of the enforcement of copyright law online, the cycles of call-and-response between the two sides are a predictable reaction to changing law, technology, and social practice.

Finally, a fourth principle is that pro-enforcement interests choose from a range of possible responses, and the effectiveness of a regulatory regime at any given time depends on which responses those interests pursue—which in turn depend on which responses are politically feasible and economically sensible. This theme underlies Goldmith and Wu's discussions of China (pp 87–104) and peer-to-peer networks (pp 112–21), but it's worth making the point explicit. Increasing the level of enforcement can be a modest response. The threat of legal action may deter some actors (such as users of peer-to-peer networks), and successful legal actions may force others to comply (such as with the Yahoo and Gutnick cases). Alternatively, pro-enforcement interests might work to change the substantive law, either by establishing new precedents or lobbying the legislature; they might distribute new technologies that encourage enforcement; or they may push for legal changes that regulate code more directly. The most draconian approach tracks the Chinese model of reconfiguring the network to achieve the government's design. This extreme approach achieves the most complete compliance, although of course at extremely high social and economic cost.

---

27 See generally Lee Kovarsky, *A Technological Theory of the Arms Race*, 81 Ind L J 917 (2006) (discussing the technological arms race in terms of the Digital Millennium Copyright Act).

28 See, for example, Orin S. Kerr, *A Lukewarm Defense of the Digital Millennium Copyright Act*, in Adam Thierer and Wayne Crews, eds, *Copy Fights: The Future of Intellectual Property in the Information Age* 163, 163–70 (Cato Institute 2002).

What do these principles tell us about the enforcement of law on the Internet and the argument of *Who Controls the Internet?*? First, they suggest that Goldsmith and Wu picked their examples carefully. Several of their examples involve the regulation of corporations, including Yahoo, Dow Jones, Grokster, and intermediaries. Others involved disputes in which the pro-enforcement forces have made only recent gains, such as recent improvements in the development of Geo-ID and the Supreme Court's *Grokster* decision. The China example analyzed the selection of a draconian enforcement scheme unlikely to be followed outside totalitarian countries. And modest enforcement is sufficient in examples such as digital copyright and the regulation of intermediaries. Viewed collectively, these examples reflect a subset of cases in which the pro-enforcement narrative is a particularly plausible one.

It's possible to tell a mirror image story, of course. Imagine another book with the same title, but with the following nine examples of how law is unenforceable online: (1) Although every computer connected to the Internet is subject to frequent attack by outsiders, the federal government only brings criminal charges for computer hacking against about one hundred defendants per year.[29] (2) In 2000, Onel de Guzman sent out the "Love Bug" virus from the Philippines; although the virus caused billions of dollars in damage worldwide, de Guzman was never charged because the Philippines did not have a computer crime law that allowed extradition.[30] (3) About two-thirds of all e-mail is unwanted "spam," unsolicited commercial e-mail.[31] (4) Computer viruses and malware make up about 1 percent of all e-mail,[32] although criminal prosecutions for sending out viruses or malware remain extremely rare. (5) Sophisticated pedophiles can use proxy servers and anonymous chatrooms to share images of child pornography with little fear of being caught by police.[33] (6) The Russian mafia executes massive-scale hacking and virus attacks with impunity from within the

---

29 The Federal Justice Statistics Resource Center's dataset indicates that in 2004, ninety-four defendants were charged under the Computer Fraud and Abuse Act, 18 USC § 1030 (2000). See Federal Justice Statistics Resource Center, online at http://fjsrc.urban.org/analysis/t_sec/stat.cfm (visited Apr 17, 2007).

30 See Rajiv Chandrasekaran, *Filipinos Struggle to Take a Byte Out of Crime*, Wash Post A01 (May 14, 2000) (noting that "[a]lthough the United States and the Philippines have an extradition treaty, Philippine law requires that both countries legally recognize a given offense before a suspect can be extradited [and] there is no Philippine law that prevents release of a virus").

31 See Enid Burns, *The Deadly Duo: Spam and Viruses, September 2006* (Oct 19, 2006), online at http://www.clickz.com/showPage.html?page=3623742 (visited Apr 17, 2007).

32 See id.

33 See Philip Jenkins, *Beyond Tolerance* 52–87 (NYU 2001).

former Soviet Union.[34] (7) Although Internet gambling is illegal in every state, millions of Americans gamble online, generating about $6 billion in revenues for the approximately two thousand Internet gambling sites.[35] (8) Use of peer-to-peer networks remains very high despite the efforts of copyright owners to shut them down. (9) It is easy to set up an anonymous blog or e-mail account and send threats or make false claims that are very difficult to trace. As these nine examples show, the enforceability of law online has a decidedly mixed record. The proper narrative depends on where you look.

More broadly, it's possible to make some rough predictions about the kinds of conditions that are most or least conducive to an effective regulatory regime online. When the four factors point in one direction, the law is very likely to be effective. When they point in the opposite direction, the converse is true. For example, the most-promising conditions for an effective regulatory regime will involve easily regulated parties (such as businesses) that can be influenced by modest and politically feasible measures to provide enough enforcement of the law to render it effective. The least-promising regimes will target parties that are difficult to regulate (such as dedicated wrongdoers), require near-perfect compliance, and demand enforcement measures that are exceedingly expensive or politically infeasible. In cases somewhere in the middle, effectiveness may cycle between greater and lesser degrees over time as the technological arms race evolves.

In sum, the real answer to "Who Controls the Internet?" may be every law professor's favorite: it depends. Governments exert control over the Internet in some contexts but not in others.

IV. CONCLUSION

A decade ago, it was popular to think of the Internet as a new world of cyberspace with different rules and limitless possibilities. Some of this perception reflected the technology of the day. Most users connected through a slow dial-up connection, and the experience of logging on really did seem like ramping on to the information superhighway and entering a virtual world. Many expected the future to be much like the present, and assumed that the virtual world of cyberspace would become only more lifelike and separate from the physical world.

---

[34] See, for example, Laura Lorek, *Russian Mafia Net Threat* (July 16, 2001), online at http://www.eweek.com/article2/0,3959,1237772,00.asp (visited Apr 17, 2007).

[35] See Adam Goldman, *Gambling Measure Isn't Sure Bet*, Deseret Morning News A02 (Oct 25, 2006).

Who Controls the Internet? offers an important reminder that our experience with the Internet today is different from the future we expected. In the last decade, the Internet has become more tied to our physical-world experience rather than less. We no longer go to cyberspace; Internet connectivity comes to us. We connect wirelessly from our laptops, cell phones, Treos, and Blackberries, and we conceive of the Internet more as a set of tools than as a separate place. *Who Controls the Internet?* reminds us that those tools are regulated by law much like any others. The question is not whether law will regulate cyberspace, but how.