Who Controls the Internet?

Illusions of a Borderless World

JACK GOLDSMITH AND TIM WU

OXFORD
UNIVERSITY PRESS

OXFORD
UNIVERSITY PRESS

Oxford University Press, Inc., publishes works that
further Oxford University's objective of excellence
in research, scholarship, and education.

Oxford New York
Auckland Cape Town Dar es Salaam Hong Kong Karachi
Kuala Lumpur Madrid Melbourne Mexico City Nairobi
New Delhi Shanghai Taipei Toronto

With offices in
Argentina Austria Brazil Chile Czech Republic France Greece
Guatemala Hungary Italy Japan Poland Portugal Singapore
South Korea Switzerland Thailand Turkey Ukraine Vietnam

Published by Oxford University Press, Inc.
198 Madison Avenue, New York, NY 10016
www.oup.com

Library of Congress Cataloging-in-Publication Data
Goldsmith, Jack L.
Who controls the internet? : illusions of a borderless world /
Jack Goldsmith and Tim Wu.
p. cm.
ISBN-13: 978-0-19-515266-1
ISBN-10: 0-19-515266-2
1. Internet—Social aspects.
2. Internet—Government policy.
3. Internet—Law and legislation.
I. Wu, Tim.
II. Title.
HM851.G65 2006 303.48'33—dc22 2005027404

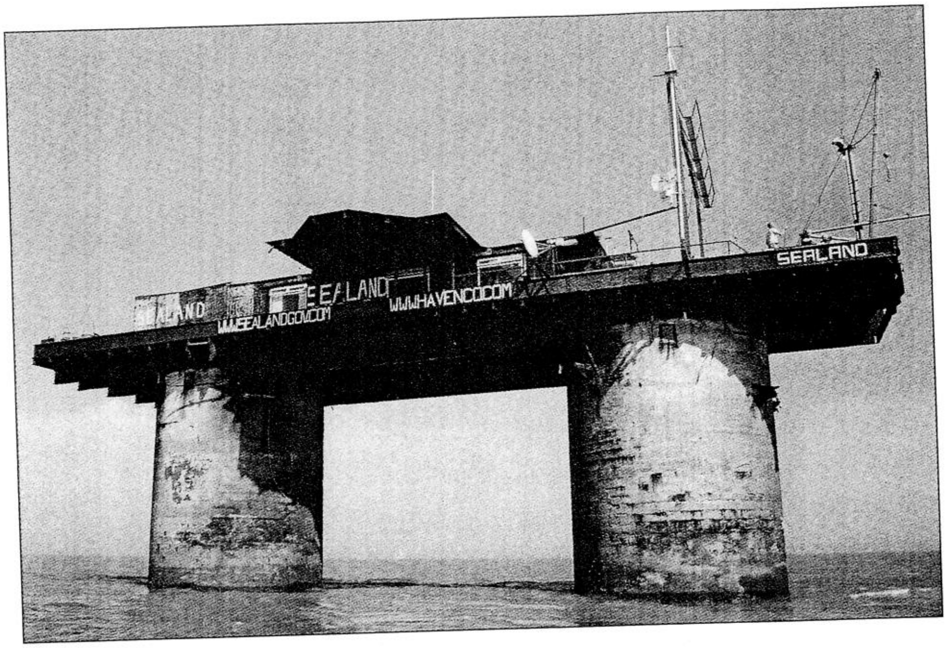
9 8 7 6 5 4 3 2 1
Printed in the United States of America
on acid-free paper

five 5

How Governments Rule the Net

In 1966 a retired British Major named Paddy Roy Bates took a liking to a small, abandoned concrete platform in the North Sea nicknamed "Rough's Tower." Rough's Tower was a World War II gun tower used by the British to fire at German bombers on their way to London. By 1966, nobody wanted the rusting contraption, so Bates renamed it the "Principality of Sealand" and declared independence from the United Kingdom, six miles away. He awarded himself the title of Prince Roy, and proceeded to issue Sealand passports and Sealand stamps with pictures of his wife, Joan, an ex-beauty queen.[1]

Sealand has had a colorful history, but before 1999, nothing suggested that a chunk of concrete and steel off the English coast might have anything to do with the history of the Internet. That year, Bates agreed to let a young man named Ryan Lackey move to Sealand and begin transforming it into a "data haven." Lackey's company, "HavenCo," equipped Sealand with banks of servers, and Internet links via microwave and satellite connections.[2] Borrowing an idea from cyberpunk fiction, HavenCo aimed to rent computer space on Sealand to anyone who wanted to escape the clutches of government. It promised potential clients—porn purveyors, tax evaders, Web gambling services, independence movements, and just about any other government-shy Internet user—that data on Sealand servers would be "physically secure against any legal action."[3] HavenCo, the company boasted, would be "the first place on earth where people are free to conduct business without someone looking over their shoulder."[4]



Sealand, off of the English Coast (Kim Gilmour)

HavenCo was the apotheosis of the late 1990s belief in the futility of territorial government in the Internet era. Lackey's company was premised on the commonplace assumption that governments cannot control what happens beyond their borders, and thus cannot control Internet communications from abroad. "If the king's writ reaches only as far as the king's sword, then much of the content of the Internet might be presumed to be free from the regulation of any particular sovereign,"[5] wrote Duke law professor James Boyle, generalizing the point.

In the end, though, HavenCo didn't realize Lackey's dreams. National governments have been able to assert control over the local effects of offshore Internet communications. They have done so not by going after computer sources abroad, but rather through coercion of entities within their borders. This chapter shows how this method of control works, and assesses some of its limitations. By witnessing the struggle to control extraterritorial harms, we can learn something not only about the history of the Internet, but also about the complex relationship among law, territory, and government power.

Beyond Borders

Many stores in New York's Chinatown sell counterfeit Gucci bags and Rolex watches at a fraction of the usual cost. While some are junk, some of the more expensive counterfeits are good enough to compete with the originals. They come from manufacturers overseas, in China, Thailand, or the Ukraine, that are far beyond the territorial control of the United States, and might as well be in Sealand. Since only a tiny fraction of these fakes can effectively be stopped at the border, HavenCo's logic would suggest that the United States and other nations are powerless to stop the trade in counterfeits.

But the counterfeits' story shows the opposite. It shows how governments control the illegal local effects of extraterritorial conduct, even when they lack the power to punish overseas producers, the resources to stop the illegal goods at the border, or the will to punish domestic consumers.

The most important targets of the laws against counterfeits—trademark laws—are local retailers.[6] If the fake Rolexes come from Thailand, it doesn't matter much that the United States can't go after the Thai manufacturers, because Wal-Mart won't sell you one. Wal-Mart doesn't sell counterfeits because doing so would be an obvious breach of a law from which it cannot hide. Wal-Mart's physical assets, its corporate headquarters, and its founding family all are in the United States, making it hard for the firm to evade U.S. government action. This is why trademark law cares little about end users. It isn't even illegal to own a counterfeit watch; it is only illegal for Wal-Mart to sell you one.[7]

It is true, of course, that even by controlling Wal-Mart, Macy's, and Sears, the United States doesn't *eliminate* counterfeit goods. Gucci and Rolex lose potential income each year to counterfeit purchases. But it doesn't follow that the trademark laws are useless. The law need not be *completely* effective to be *adequately* effective.[8] All the law aims to do is to raise the costs of the activity in order to limit that activity to acceptable levels. We do not conclude from the persistence of occasional bank robberies that laws against theft are ineffective, or even suboptimal. Often, the law accepts small evasions because achieving perfect legal control, though possible, is just too expensive.

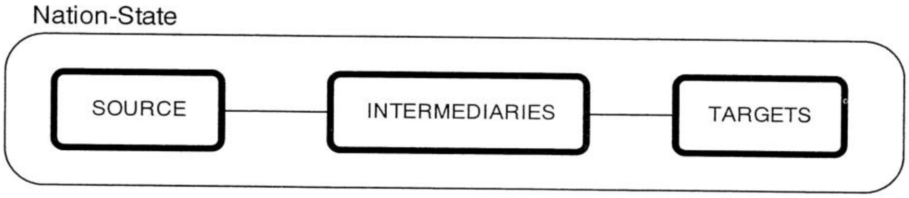
Similarly, the fact that there are sellers—like the stores in Chinatown—who are willing to assume the legal risk of selling counterfeits does not mean that the trademark laws are ineffective. To be effective, trademark law need only throw enough sand into the workings of the counterfeit market so that Gucci and Rolex continue to make smart profits. Certainly, government could do more to dry up the counterfeit market. It could hire more enforcement officers, invest more in border control, criminalize the purchase of fake goods, or increase the punishments dramatically. But the system can be adequate to its task even though the government could do more, and even though compliance is not perfect. Government regulation works by cost and bother, not by hermetic seal.

The fake Rolex example teaches a crucial lesson about how law actually works. We tend to think of law as like the Ten Commandments—a series of direct, individualized directives (thou shall not kill, steal, or bear false witness). And while some laws do work this way, many do not. It is easy to overlook how often governments control behavior not individually, but collectively, through *intermediaries.*[9] Pharmacists and doctors are made into "gatekeepers" charged with preventing certain forms of drug abuse. Bartenders are responsible for preventing their customers from driving drunk, and gun manufacturers have in recent years been held liable for the injuries of shooting victims.[10]

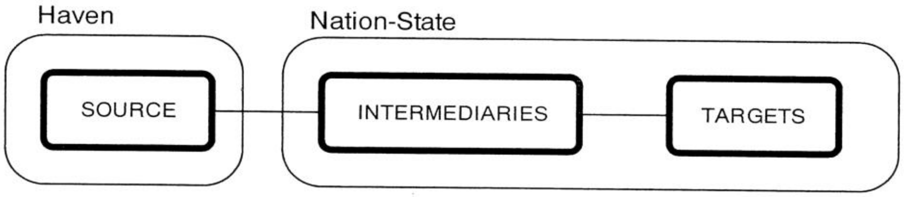
Similarly, to control offshore Internet communications from places like Sealand, governments threaten local Internet intermediaries: the people, equipment, and services within national borders that enable local Internet users to consume the offending Internet communication. Government action against such local intermediaries makes it harder for local users to obtain content from, or transact with, the law-evading content providers abroad. In this way, government affects Internet flows within their borders even though they originate abroad and cannot easily be stopped at the border.

Extraterritorial Control Through Local Intermediaries

How precisely does control of local intermediaries relate to the government's ability to influence offshore content providers? Most illegal acts can be understood as transactions involving three relevant parties: the "source" (the manufacturer), an intermediary (the Chinatown shops), and a "target" (the purchasers):

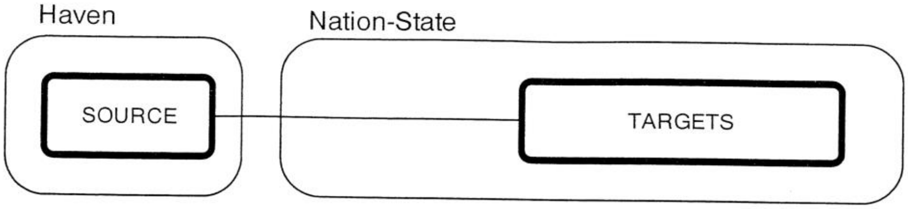


Havens move the illegal source outside the limits of the government's physical control. A simple haven strategy can be pictured as follows:



The counterfeit Gucci bags from Thailand follow this example. The source of the illegal conduct—the manufacturer of the counterfeit goods—has moved overseas. Yet, as we see in that example, both the intermediaries and the targets remain within the physical control of the government. This leads to an important insight: effective control over *any* of the three elements of the transaction permits the government to control conduct within its borders. In the counterfeit goods example, control over the intermediary sellers or (if the government had the resources) the actual purchasers could effectively control the illegal transaction.

One might think that the source can diminish the problem of government control by eliminating the intermediaries. Such *disintermediation* is what many think the Internet is supposed to be all about.[11] On the Net, after all, you don't need a stock broker to lose money, and you don't need to visit a bookstore to buy books. That evasion technique, disintermediation, is pictured here:

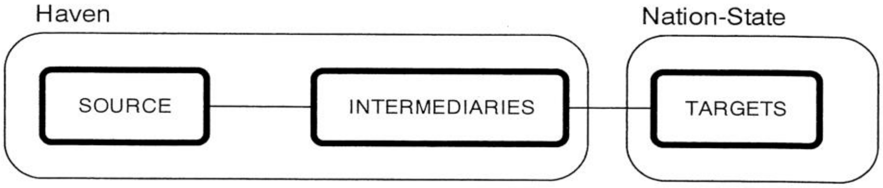


In principle, this is a powerful strategy. It leaves the government with the sole option of trying to hunt down the "target" end users, who might be numerous and expensive to find (more on this later). So, if the Internet, as advertised, is eliminating intermediaries, doesn't this mean that traditional governmental power is doomed?

The problem with this theory, which pervaded Internet thinking in the late 1990s, was its central premise. The rise of networking did not eliminate intermediaries, but rather changed who they are. It created a whole host of new intermediaries, the most important of which (for our purposes) are ISPs (Internet Service Providers), search engines, browsers, the physical network, and financial intermediaries. In short, the Internet has made the network itself the intermediary for much conduct that we might have thought had no intermediary at all prior to the Internet.

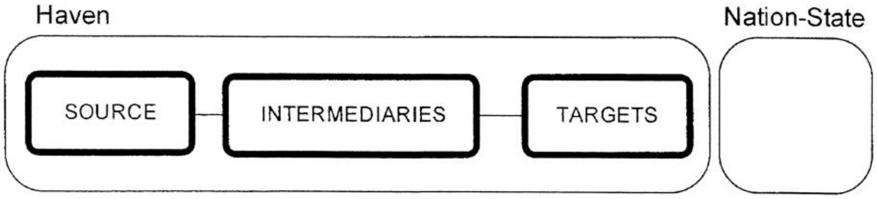
But if governments control the Net through intermediaries, why can't content providers evade this control by just circumventing intermediaries? The answer is that it is hard to get rid of intermediaries because the elimination of intermediaries is in many cases the same thing as the elimination of the underlying conduct. Specialized intermediaries exist, after all, because they allow people to do things that would be difficult, or even impossible, for them to do themselves. It doesn't make sense to speak of making telephone calls without some entity to connect calls. Car manufacturers exist because, though it might be possible for people to make cars on their own, the cost would be enormous. To truly act without any intermediaries means acting by oneself. There are few things that one can do without the direct or indirect assistance of someone else. And so in the Net context, scores of intermediaries are needed to make the Net experience work. Most of the time, they are invisible, but they are there. And they can be controlled.

What about moving the intermediaries themselves offshore, beyond the range of government control? Here is what such a move would look like schematically:



This model is no more realistic than the one that eliminates intermediaries altogether. In the Internet context, there are *always* local intermediaries. The most basic, of course, is the actual computer through which individuals access the Net, and which nations can regulate. Behind that are many more that we have already discussed: the physical communications lines, the network nodes, search engines, ISPs, and the like. If you try to access an unregulated offshore ISP through a long-distance telephone call, the phone system becomes an important intermediary. If you unplug your line and connect by Wi-Fi, the computer remains an intermediary, as does a physical network standing behind a Wi-Fi connection. And so on. Local intermediaries are a defining, and therefore ineliminable, aspect of the Internet.

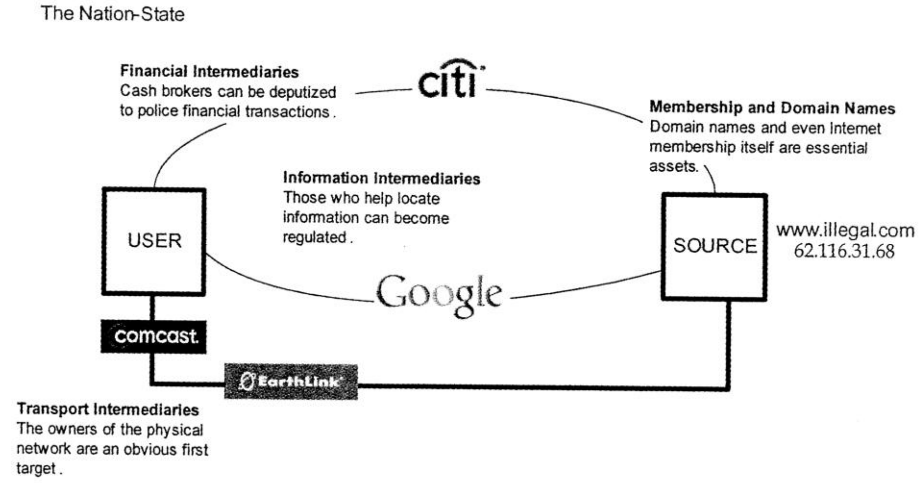
We have discussed the enforcement options that remain when the source of illegal materials moves overseas. But what if, in response to enforcement, end-users or "targets" also leave the country? This is the possibility of "total exit" pictured here.



The creation of an exile community is indeed a kind of final escape from undesirable laws. Moses and the Israelis fled Egypt in search of (among other things) a better legal system. And today, more prosaically, lovers of high-stakes gambling can move to Las Vegas, and serious marijuana users can make their home in Amsterdam and enjoy a different kind of life. But at some point this becomes less of a challenge to government power than an acceptance of it. If you move from the United States to Germany to escape highway speed limits, that is less what we think of as evasion, and more like what we think of as emigration.

Finding the Internet's Intermediaries

In the 1990s, Lawrence Lessig revolutionized cyberlaw thinking with his sustained analysis of the premise that "code is law."[12] What Lessig meant was that the architecture of the Internet—its hardware and software—was a different and potentially very powerful way of controlling Internet behavior. One of Lessig's aims was to throw cold water on the hyperlibertarianism of the early Internet days by showing that sometimes government does a better job than private firms (especially monopolies) of designing Internet code in ways that serve user interests. Another aim was to show that the government could control the Internet by controlling its hardware and software.[13] What we learn in the remainder of this chapter sheds a different light on Lessig's thesis. When government practices control through code, it is practicing a commonplace form of intermediary control. Sometimes the government-controlled intermediary is Wal-Mart preventing consumer access to counterfeit products, sometimes it is the bartender enforcing drinking age laws, and sometimes it is an ISP blocking access to illegal information. In what follows we work through what have


The Nation-State
Financial Intermediaries
Cash brokers can be deputized to police financial transactions.
citi
Membership and Domain Names
Domain names and even Internet membership itself are essential assets.
Information Intermediaries
Those who help locate information can become regulated.
USER
SOURCE
www.illegal.com
62.116.31.68
Google
comcast
EarthLink
Transport Intermediaries
The owners of the physical network are an obvious first target.

emerged as the primary intermediaries of government control over the Internet.

Transport

As far back as 1995, the Germans raided the Bavarian offices of Compuserve, and later indicted and tried the German manager of Compuserve Deutschland. The offense: failing to prevent child pornography, much of which came from outside Germany, from reaching German citizens.[14] The prosecution made Compuserve think twice before allowing illicit content through its German portal. In 2001, the British government threatened British ISPs with criminal prosecution for distributing illegal adoption sites, including sites located abroad. The result: British ISPs blocked the sites to keep people in Great Britain from accessing them.[15] Today, German, French, and British laws require local ISPs to screen out illegal content once they are notified of its existence.[16] A European Union Commerce Directive imposes the same basic rule—a rule that, in practice, causes ISPs to err on the side of caution in removing content.[17]

Internet Service Providers are the obvious first target for a strategy of intermediary control. It can be great fun to talk about the Internet as a formless cyberspace. But, as we saw in chapter 4, underneath it all is an ugly physical transport infrastructure: copper wires, fiber-optic cables, and the specialized routers and switches that direct information from place to place. The physical network is by necessity a local asset, owned by phone companies, cable companies, and other service providers who are already some of the most regulated companies on earth. This makes ISPs the most important and most obvious gatekeepers to the Internet.[18] Governments can achieve a large degree of control by focusing on the most important ISPs that service the vast majority of Internet users. "Pressure applied strategically to the concentric ISPs serving smaller ISPs—one or two "dolls" up in a Matryoshka sequence of destination ISPs—can cover large swaths of subscribers," explains Jonathan Zittrain.[19]

As the examples above suggest, the command-and-control Europeans are, in the Western world, pioneers in using ISPs to control unwanted Internet content. Regulation-sensitive Americans have been relatively hands-off, and in fact the United States expressly immunizes ISP from liability in many contexts for the illegal acts of third-party users.[20] At the other end of the spectrum, the true champions of information-transport control can be found in the East. As the next chapter shows in detail, China has from the beginning maintained extremely close control of every element in the Internet transport pipeline. Saudi Arabia has a less aggressive, but still extensive, nationwide filtering system. According to a 2004 report by the OpenNet Initiative, the Saudi government puts proxy servers between the government-owned Internet backbone and servers outside of the Kingdom. If a Saudi ISP user requests illicit content on a foreign server, the request travels through the intermediate proxy server, where it can be filtered and blocked.[21] All the user sees is a "block page" stating that "[a]ccess to the requested URL is not allowed!"[22] Saudi Arabia is most aggressive about blocking pornography, websites that promote drug use, Web gambling sites, information about tools to circumvent the government's filtering, and sites that promote religious dialogue between Muslims and Christians.[23]

Information Intermediaries

Norwegian Andreas Heldal-Lund describes himself as "a skeptical atheistic freethinking pacifistic positive engaged and tolerant heathen who bases his life on modern secular humanism."[24] He lives in Norway and is a member of both the "Norwegian Society of Heathens" and "Human-Etisk Forbund," a national secular humanist organization. He is also perhaps the Church of Scientology's greatest living irritant. Heldal-Lund has since 1996 devoted much time to a website, "Operation Clambake," that exposes the deepest secrets of the Church and attempts to debunk its teachings.

For the Church of Scientology, Heldal-Lund's activities presented a serious problem of information control. A major benefit of rising through the ranks of the Church's strict internal hierarchy is access to carefully guarded teachings and writings. But in 2002 Operation Clambake's website began to host many of the important teachings of the Church.[25] Suddenly, writings that were meant to take years of preparation to read (and cost tens of thousands of dollars in training) were available to everyone on the World Wide Web.

Unable to shut down Clambake's Norwegian service provider, the Church turned to a different technique. It sent letters to Google, the Web's most popular search engine, demanding that Google take down Clambake's sites under an American law, the Digital Millennium Copyright Act.[26] According to the Church, Clambake's materials were an infringement of copyright that Google was legally obliged to block.[27] Google complied, and for a while a search for "the secret library of Scientology" failed to deliver anything related to Operation Clambake. Eventually, for reasons that remain mysterious, Google restored many of the Operation Clambake sites. The Clambake story nonetheless sheds light on an under-recognized fact: search engines like Google routinely block links because of possible governmental action.

Google receives a constant stream of letters in the United States—about thirty per month—insisting that it remove specified pages from its search results, usually because of alleged copyright or trademark infringement.[28] Google complies with most of these requests. Many of these pages are located on servers outside the United States, beyond the direct control of U.S. law.[29] But the government, or those invoking its laws, can block the offshore content provider by going after the local search engine instead.

As with information transport, Europeans are more aggressive about using search engines as Web content-blockers. In 2002, Jonathan Zittrain and Ben Edelman found that Google in France and Germany (google.fr and google.de, respectively) blocked more than one hundred sites that were available on google.com. "While google.fr and google.de use google.com's database concordance of 2,469,940,685 web pages (Google's count as of October 20, 2002), the French and German sites seem to screen search results corresponding to sites with content that might be sensitive or illegal in the respective countries," explained Zittrain and Edelman.[30] Most of the sites blocked in France and Germany unsurprisingly concerned Nazism, hate speech, white supremacy, and related sites that are banned in those countries but lawful in the United States.

The general technique of controlling information intermediaries has extraordinary potential. Consider how often you rely not just on search engines to find information but also on blogs, online newspapers, and other intermediaries that point you in the direction of useful information. It is one thing for government to crack down openly on forbidden information. But it can be harder to notice that information has become more difficult to find. It is hard, in other words, to know what you don't know.

Financial Intermediaries

In the early 2000s, online cigarette vending looked like a promising business, especially on Indian reservations that typically place no taxes on cigarettes sales. A 2001 survey found that of eighty-eight online cigarette vendors, forty-nine were on reservations and most of the rest were in low-tax states.[31] The basic advantage of buying online in bulk is convenience and tax avoidance. In New York State, for example, state taxes amount to about $15 per carton. It is thus unsurprising that, by 2004, online cigarettes were a $1 billion industry, or 3.1 percent of industry volume.[32]

All that changed in 2005. The Federal Bureau of Alcohol, Tobacco, and Firearms, joined by several states, decided to crack down on online sales. They didn't bother actually charging the vendors with anything. Instead, they went after crucial financial intermediaries—the major credit card companies. The bureau simply ordered Visa, MasterCard, and AmEx to stop taking online cigarette orders or face the consequences. Government officials argued that the online sites weren't doing enough to comply with age verification laws, and weren't making sure that states receive their sales tax.

Was the government right? Online cigarette companies are hardly the only ones who do not charge state sales tax on online sales, and as for underage buying, the tobacco vendors insisted that they do maintain controls. Experts agreed online purchases by minors were not a serious problem, or no more serious than any other way that minors get access to cigarettes. But the vendors will never have a chance to test their theory in court. The credit card companies accepted the government's position, and that was that.

"Not since the dot-com bust have so many sites gone south so quickly," reported the *New York Times* in the spring of 2005. Scores of online vendors went under in a two-week period. They "lost the means to do business profitably, and are either limping along or have shut down their operations altogether."[33] Without access to credit card payment, the cigarette websites might have tried other financial intermediaries, like PayPal. But PayPal capitulated too, just as it did in a similar situation when New York officials threatened it with fines for financing illegal offshore Web gambling.[34] Checks or direct deposits from local banks would in the end fare no better, since local officials could go after these new intermediaries with the same tools it used against the others. There might be other ways for the determined purchaser to buy online cigarettes, but at some point buying cigarettes online becomes enough of a legally dangerous pain in the rear to kill the business model.

As the cigarette example shows, governmental targeting of financial intermediaries can cripple an online industry, particularly one that is premised on convenience of payment. Could the online pharmaceutical industry prosper if the seller didn't take credit cards? Could Amazon or eBay stay in business without convenient lines of credit? Probably not. And that is how, without ever laying a finger on online sellers, the government can impose its power, often without even needing to go to court.

The Domain Name System and Internet Membership

In the fall of 2000, Al Gore and George W. Bush were fighting for the American presidency, aided by hundreds of millions in campaign contributions. That gave James Baumgartner, a student at the Rensselaer Polytechnic Institute, a clever idea. As a commentary on the role of money in the election, he opened the website voteauction.com as a place for otherwise uninterested voters to sell their votes to the highest bidder.[35] Its slogan was "Bringing Capitalism and Democracy Closer Together." With so much money being spent trying to influence elections, why not just pay the money directly to the voter? Baumgartner billed Voteauction as "the only election platform channeling 'soft money' directly to the democratic consumer."[36]

The site actually worked. As the *Chicago Tribune* reported in early October of 2000, 521 unidentified people in Illinois had agreed to sell their presidential votes. The top anonymous bid for the 521 votes was $8,500, or $16.31 per head.[37] While Baumgartner intended the site as satire, the Chicago Board of Election Commissioners decided there was nothing funny about offering to buy and sell votes, and it moved to shut down Voteauction as quickly as possible. And it chose a novel means. Instead of targeting Baumgartner, or trying to hunt down the vote-sellers themselves, it went after an essential asset—the name "voteauction.com."[38]

In short order, an Illinois judge imposed an injunction not on Voteauction but on its U.S. domain name registry, Domain Bank, which had a standard domain name registration agreement prohibiting domain name use for "illegal purposes."[39] Domain Bank banished voteauction.com's domain name as if it were the itinerant Mr. Bungle, "shutting down voteauction.com all over the world."[40] One week later, voteauction.com opened up under a new domain name, "vote-auction.com," registered in Switzerland with the International Council of Registrars (CORE).[41] But CORE too had a prohibition against illegal uses in its standard domain name registration agreement, and after extensive telephone and e-mail discussions, vote-auction.com was shut down.[42] Voteauction later began trying to publicize its numerical IP address, http://62.116.31.68, but that address is obviously much harder to find, and by then the voting was over.[43]

In 2003, John Ashcroft's Justice Department began a controversial crackdown on Web vendors of drug paraphernalia—purveyors of bongs, vaporizers, and other favorites. Its method: the seizure of the website domain names themselves. The Justice Department explained that seizing property used in the commission of a crime is a routine matter. And rather than shutting down the sites, the Justice Department, in effect, hijacked them. Visitors looking for a new pipe would instead read:

> BY APPLICATION OF THE UNITED STATES DRUG ENFORCEMENT ADMINISTRATION, THE WEBSITE YOU ARE ATTEMPTING TO VISIT HAS BEEN RESTRAINED BY THE UNITED STATES DISTRICT COURT.[44]

Since its experiment with drug sites, the Justice Department has also begun seizing the domain names of sites that facilitate copyright infringement, replacing them with warnings against piracy. "I believe this is one area—intellectual property rights—where there is a deterrent effect from aggressive and effective criminal prosecution," said Ross Nadel of the San Francisco U.S. Attorney's Office. Nadel predicted that the government would redirect users to a privacy warning page following future domain name seizures.[45]

Tight control over domain names is another looming and particularly effective way for nations to control Internet behavior. As discussed in Chapter 3, we take it for granted that the Internet's "membership policy" is neutral and open. But that's contingent, already under attack from several quarters, and a fact that could gradually change. Countries know that as a general matter, membership rules have always been a powerful means of control, whether it's at a country club or the World Trade Organization. There may come a time, and that time might be soon, when accurately disclosing who you are is a condition of Internet membership. There may soon come a time when abusing your privileges as a member of the Internet could lead to expulsion from the club.

As these and other examples show, government has many types of intermediaries it can use for indirect control. None of these examples should obscure the most basic means of control: the direct physical coercion of individuals.

Targeting Individuals

Tore Tvedt ran a Norwegian organization called Vigrid, devoted to the worship of Odin, other ancient Norse gods, and the ideology of the Nazi party. Fearing Norwegian hate-speech laws, Tvedt had a clever idea. He placed his anti-Semitic propaganda on a server in the United States, beyond the reach of Norwegian authorities. Unfortunately for Tvedt, he didn't do anything to put *himself* out of the reach of Norwegian authorities. One day in 2002, the Norwegian police simply arrived at the home of Tvedt and placed him under arrest.[46]

Tvedt illustrates the simplest and most direct strategy that governments use in response to illegal Internet content from abroad—physical arrest of individuals inside their borders. Sometimes, as with Tvedt, they do so to dry up the *supply* side of unwanted Internet communications. What happened to Tvedt also happened to Duane Pede and Jeff D'Ambrosia, two Americans who lived in the United States and were convicted of running an Internet gambling site from an island off the coast of Venezuela.[47] Other times, governments crack down on individuals in order to dry up the *demand* side. When the FBI closed down Landslide Productions, a Texas-based website that gave paid subscribers access to hundreds of Russian and Indonesian child porn sites, they discovered a database full of subscribers worldwide.[48] Authorities in the United States, Canada, and Great Britain used this information to arrest thousands of Landslide customers within their borders.[49]

Some may be skeptical of the effectiveness of arresting a few law violators when so many are violating the law. But this skepticism overlooks the deterrence effects of individual enforcement. In the late 1960s, economist and Nobel laureate Gary Becker argued that lawbreakers were rational, and that their decisions to break laws reflected a calculation of costs (including the chances of getting caught and the possibility of fines or jail time) and benefits (the financial and other rewards of crime).[50] The government, Becker argued, doesn't need to catch every lawbreaker to control lawbreaking. It just needs to increase the likelihood and severity of punishments to the point where for most people the costs of committing crime are less than the benefits. The economics of deterrence led Becker to argue that government shouldn't waste too much money looking for criminals but instead should just raise the sanctions for breaking the law. You might think more than twice about parking illegally if a parking ticket meant a month in prison.

Matters are not, of course, as simple as Becker suggested. Fear of punishment is not the only reason people obey the law. Reflecting this intuition, academic work since Becker's article has pointed out the limits on the amount of deterrence that can be achieved just by increasing punishments. Some people, for example, are poor enough that they don't fear fines, or are so pessimistic about their future prospects that going to jail may not seem so bad. And of course there's an upper limit on what most governments can threaten. For various social and moral reasons, parking violations do not usually result in one-month prison sentences. If governments punished relatively minor wrongs (like Internet gambling) as severely as serious crimes (like bank robbery), the law would lose its ability to send a message about what citizens should not do, and what they *really* should not do.[51]

So there are limits to deterrence through individual enforcement. But Becker's basic point—that even criminals respond to incentives—is sound. Enforcement against individuals is rarely an isolated strategy but usually part of a unified strategy that involves various means of intermediate control as well. The interesting and difficult question is how much individual enforcement adds, especially in situations like those of mass disobedience that often prevail on the Internet, such as music filesharing. The point for now is simply that enforcement against individuals has at least some effect and is part of an integrated governmental strategy to crack down on law evasion.

Challenges

Our discussion of the techniques of government control over the Internet is not meant to suggest that the techniques always work perfectly. They do not. Nor do we mean to suggest that government control over Internet activities will always be as successful as when these activities take place outside the Internet. They will not, as consumers of pornography, web gambling, and free digital music know. At one level, these points are unsurprising. Every great technological innovation has the potential to lower the cost of violating law. The telephone, at least before wiretapping, made it easier for criminals to plan their activities. The record player and the radio increased the incidence of infringement of copyright-protected music. Transportation advances (the automobile, the airplane) made it easier for criminals to plan and commit crimes from abroad, or to commit crimes in one place and flee to another.

The same is true of the Internet, as porn and web gambling show. But as we have emphasized throughout this book, law has never been perfect. It succeeds by lowering the incidence of prohibited activities to an acceptable degree. The Internet will not, as Barlow and other romantics suggested, make it so easy to violate so many laws that the nation-state itself will cease to function. But in certain areas, techniques of law avoidance will prove more effective than in others. The interesting and difficult questions are how such new techniques of control will fare against new techniques of avoidance—and what the ultimate results of such arms races will be. We consider three main issues: small nations, intermediary minimization, and mixing.

The techniques of intermediary control are generally less effective in small nations, where opportunities for Internet intermediary control are diminished. The United States and France can control offshore Internet communications through intermediaries more readily than Fiji and Ghana because the larger countries have a larger array of intermediaries to go after. We learned in chapter 1 that France was able to influence the local effects of Yahoo's U.S. servers because Yahoo had many assets, including a subsidiary, in France. But Yahoo doesn't have a presence or assets in Fiji or Ghana. Nor do information intermediaries like Google or Blogger. That doesn't leave a country like Fiji without options. It can choose to block the Internet altogether, and it can still order its necessarily local intermediaries—for example, ISPs—to filter forbidden materials. But some of the techniques available to large-market countries are just unavailable to those with smaller markets.

Even in powerful countries, intermediaries, while impossible to eliminate, can in some contexts be relatively hard to control. The story of Web gambling in the United States provides a good example. In response to the rise of web gambling services in Caribbean countries like Antigua, U.S. enforcement officials focused their attention on local financial intermediaries—the credit card companies and Internet payment systems (like PayPal) that made it possible for Americans to ante up online. In 2002, New York's redoubtable attorney general, Eliot Spitzer, used threats of prosecution to convince every major American credit card provider and online payment system to stop honoring web gambling transactions. "With this agreement, we will cut off an enormous line of credit that was a jackpot off illegal offshore casinos," Spitzer proclaimed.[52] This technique seemed to work pretty well, driving half of Antiguan web gambling firms out of business, and (in the words of the Antiguan prime minister) leaving a "significant, negative impact upon the [Antiguan] economy."[53]

But Spitzer's efforts did not end matters. As we'll see in chapter 10, Antigua brought an action against the United States in the World Trade Organization. The web gambling firms fought back as well. Instead of relying on credit cards, they began to ask customers to wire money from local banks to offshore banks to use for chips.[54] Because there are thousands of local banks in the United States, this strategy dramatically multiplied the number of intermediaries in the United States that enforcement officials must crack down on. And this, in turn, means that financial control of offshore web gambling is more complicated and expensive for local officials, for now they must go after thousands of intermediaries rather than just a dozen or so.

This arms race increased the costs to government of controlling gambling. But at the same time, of course, it increased the costs to gamblers themselves, who must now arrange to transfer money from banks rather than type in a credit card number, and who face heightened chances of legal jeopardy. It is difficult to generalize about when and under what conditions these swings of regulation and evasion will reach equilibrium. The government's resources dwarf those of private entities, and can, with sufficient focus and will, be expected to prevail in most contests. But the government does not always have the focus and will to prevail, often because at some cost the activity in question is simply not worth cracking down on further.

This latter point relates to the third technique of avoidance: mixing. Why is it so easy to get Internet porn in the United States? You might think it's because Internet porn is inherently difficult to control, but there's more to it than that. As we saw in chapter 2, the American Congress reacted quickly to the initial flood of Internet porn, passing the Communications Decency Act in 1996—a law that would have done much to drive pornography behind ID-protected walls. But the problem for government's efforts to control pornography is that it's hard to distinguish it from stuff the U.S. government doesn't want blocked, like artistic expression, sexual education, and news. As a result, the government's interest in stopping porn collided with its constitutional commitment to free speech. The Supreme Court, as we saw in chapter 2, concluded that the law's effort to crackdown on Internet porn swept up too much protected speech along the way. When a new technology that makes it much cheaper and easier to make and distribute pornography combines with the fact that pornography is hard to distinguish from deeply valued protected speech, the result is an increase in the incidence of available pornography.

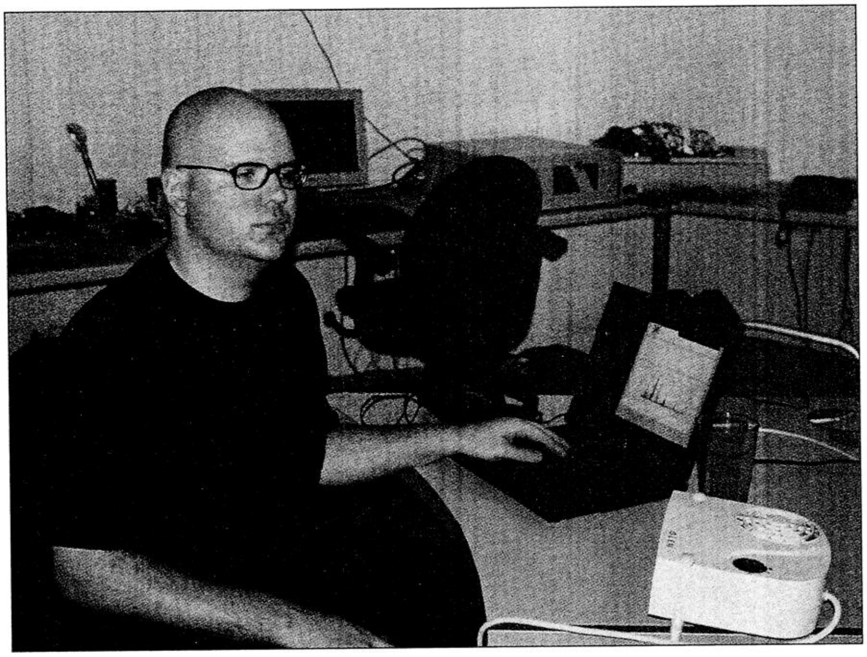
This is the technique of "mixing" legal and illegal conduct. For law avoiders, it means structuring conduct so that a given business—for example, pornography—can only be stopped at the expense of giving up things that government and society value highly—like artistic expression and an open environment for speech. Mixing gives the government no choice but to lose what it likes when it bans what it doesn't like. It means taking advantage of deeply held national values, like commitments to open commerce, free speech, or respect for citizen privacy. That can be enough for a country like the United States to leave an activity, like pornography, basically unregulated. It doesn't mean the United States cannot control pornography, for the United States could in theory adopt techniques used in countries like Saudi Arabia that worry less about the incidental effects on protected speech. What it means is that the United States would be forced to compromise in ways it is unwilling to do.

Nation size, intermediary minimization, and mixing can all affect the success of national Internet control. We address additional challenges to Internet control in chapter 10. But while these challenges should not be overlooked, they should not be overstated either. Along other dimensions, the Internet, like all previous communications technologies, increases government power. For example, it enhances the government's ability to monitor the everyday activities of its citizens, to know about, and thus potentially to control, what is going on in every recess of the nation, and to convey government information and propaganda. These Internet-related powers are often held in check in countries like the United States that value privacy and free speech. But as we will see in chapter 6, in the hands of a government like China that does not share these values, the Internet enables frighteningly unprecedented control by the government over individuals.

Epilogue

On August 3, 2003, HavenCo founder Ryan Lackey went to Las Vegas to give an astonishing speech at DefCon, the annual convention for computer hackers. His talk was titled "HavenCo: What Really Happened."[55] HavenCo, he revealed to the world, had never been the success it was portrayed to be. The story of the giant server farm, hidden deep in the recesses of Sealand, was a lie: HavenCo's equipment consisted of "five relay racks standing mostly empty."[56] The "dozens" of customers HavenCo claimed were, at the best of times, roughly ten, almost all online casinos.[57] And now, Lackey reported to the crowd, HavenCo was dead.

HavenCo died for two related reasons. The first was the absence of cooperative intermediaries, especially financial intermediaries. "Sovereignty alone," said Lackey, "has little value without commer-



Ryan Lackey, founder of HavenCo, spent long periods living on Sealand (Kim Gilmour).

cial support from banks, etc."[58] Banks wouldn't cooperate with HavenCo, one suspects, for the same reasons that U.S. financial institutions are not cooperating with online cigarette sales. Local pressure on these crucial intermediaries influences how they interact with providers of information content.

Sealand itself also turned out to be susceptible to the pressures of powerful governments. More than anything else, Prince Michael, the ruler of Sealand, wanted recognition as an actual country. HavenCo's unseemly activities, he began to believe, were an impediment to that dream. The Prince began to insist that HavenCo adhere to "norms of international practice and custom" and demanded that nothing "offensive" be available from his sovereign nation.[59] But of course, the hosting of "offensive" content was HavenCo's raison d'être. Without it, HavenCo was nothing. The company sank into a slow decline, shedding customers and losing money, until finally came what Lackey called the "nationalization" of HavenCo in November 2002, when Sealand kicked HavenCo off the island. Sealand today nominally owns what remains of HavenCo—a jumbled pile of network equipment, rotting and obsolete.