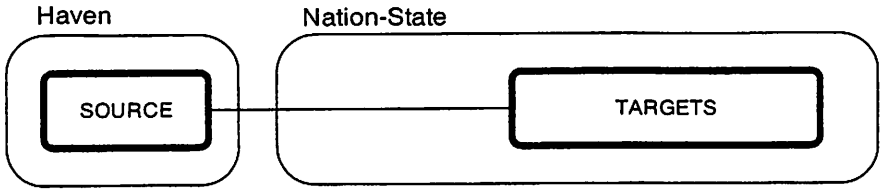
five

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]

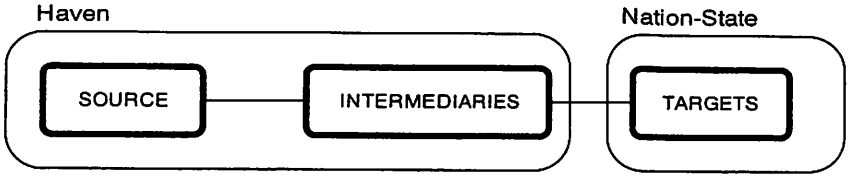


In principle, this is a powerful strategy. It leaves the government with the sole option of trying to hunt down the "target" end users, who might be numerous and expensive to find (more on this later). So, if the Internet, as advertised, is eliminating intermediaries, doesn't this mean that traditional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

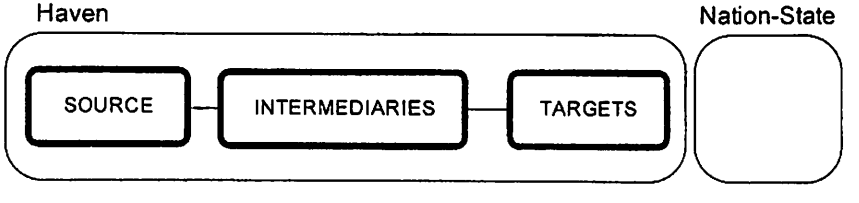
But if governments control the Net through intermediaries, why can't content providers evade this control by just circumventing intermediaries? The answer is that it is hard to get rid of intermediaries because the elimination of intermediaries is in many cases the same thing as the elimination of the 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.

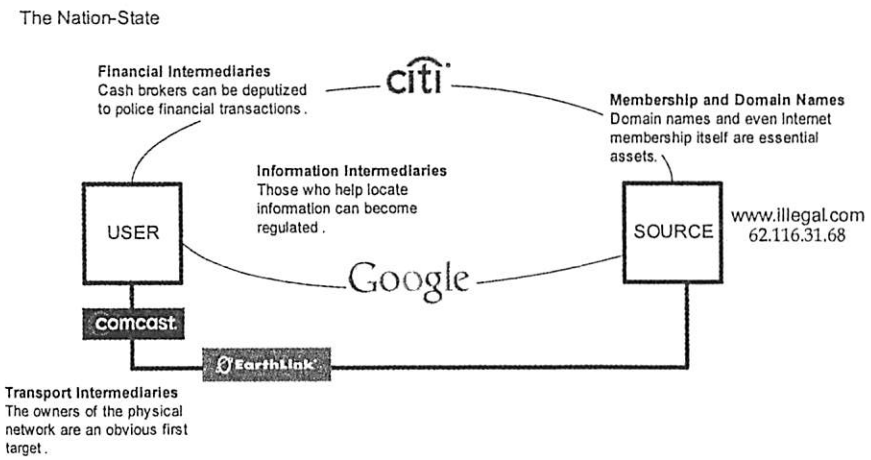


The creation of an exile community is indeed a kind of final escape from undesirable laws. Moses and the Israelis fled Egypt in search of (among other things) a better legal system. And today, more prosaically, lovers of high-stakes gambling can move to Las Vegas, and serious marijuana users can make 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



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

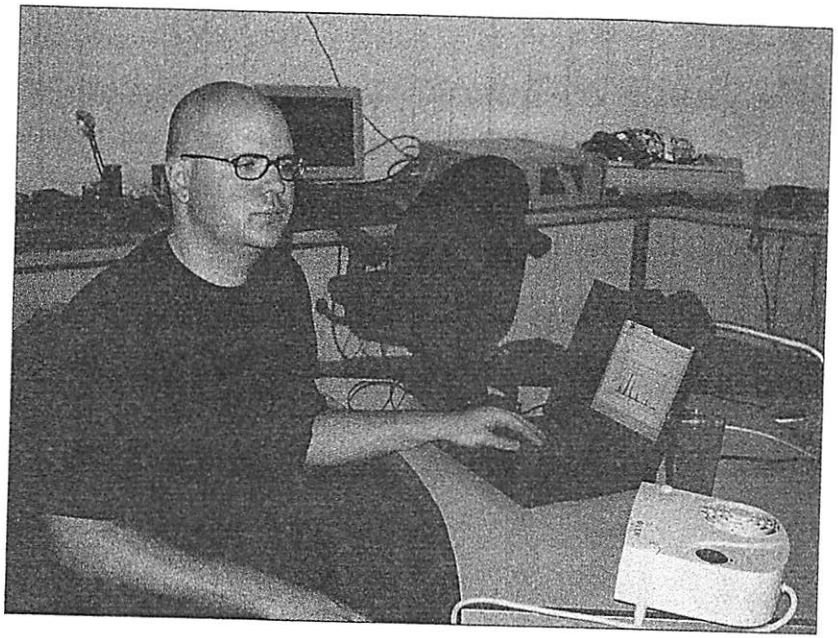
leave an activity, like pornography, basically unregulated. It doesn't mean the United States cannot control pornography, for the United States could in theory adopt techniques used in countries like Saudi Arabia that worry less about the incidental effects on protected speech. What it means is that 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 commercial 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.



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

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.

6 six

China

"Long live prostitutes" was the title of Wang's posting. Fifteen years old, living in China, and full of teenage bluster, Wang had collected fifty-four reasons to think Chinese politicians worse than prostitutes. The list included:

- There is no indicator that prostitutes will disappear, but there are many indicators that the government will collapse.
- Prostitutes allow others to oppose them, unlike the government which arrests opposition and "re-educates" them through labor.
- Prostitutes have no power, unlike those who use their power to suppress others.
- Prostitutes do not need you to love them, unlike that group which forces you to love it.
- Prostitutes win customers with credibility, unlike those who maintain power with lies.
- Prostitutes sell flesh, unlike those who sell soul.[1]

Liu Di was a psychology student at Beijing Normal University who called herself the "Stainless Steel Mouse" and ran an "artist's club" through her personal website. In 2002, in one of her many stunts, the twenty-two-year-old urged her followers to distribute Marxist literature:

> Let's conduct an experiment of behavioral art: disseminating communism on the street! We can print copies of "The Communist Manifesto." However, we should take "Communist" out of the title. Then, like sociologists, we ask people on the street to sign their names onto the Manifesto.

Liu Di wrote an essay titled "How a national security apparatus can hurt national security." Echoing typical criticism of governments everywhere, she called China's security apparatus "limitless," or possessed of "a tendency to expand, without limits, its size and functions."[2]

Wang's message and the writings of Liu Di appeared on obscure Internet sites. Nonetheless, they came to the attention of the Chinese authorities and provoked swift action. Soon after Wang posted his message, it was deleted. He was arrested in Henan and subjected to an unspecified punishment. Wang's story was printed in the *People's Daily* as a warning, with the headline "15-Year-Old Youth Punished For Making Reactionary Argument That the Government is Prostitute"[3]

The State Security Protection Bureau arrested Liu Di on her university campus on November 7, 2002. Her site was shut down, and she was jailed and forced to share a cell with a convicted murderer. When human rights groups and other Chinese Internet users protested, the government responded by arresting five Net users who had signed a petition calling for Di's release. The State Security Bureau told Liu Di's parents that their daughter was charged with "being detrimental to state security."[4] Liu Di was held for a full year, then released subject to permanent surveillance and banned from speaking to foreign journalists or traveling outside of Beijing.[5]

Liu Di, Internet writer who was arrested for her essays (AFP/AFP/Getty Images)

These examples of political control are one side of the Chinese Internet. But if you visit China, you'll be struck by a different and seemingly paradoxical reality—information technology

and mass media are flourishing as never before. By 2005, China's aggressive broadband rollouts had created nearly as many Chinese broadband users as in the United States.[6] One hundred million people in China had Internet accounts, there were 4 million Chinese blogs, countless chatrooms, and scores of commercial sites like eBay China and Ctrip.com, a travel reservation site.[7]

Facts like these led many, including the *New York Times*'s Nicholas Kristof, to believe that China's Communist Party must be losing power. As Kristof wrote in a 2005 column, *Death by a Thousand Blogs*, "the Chinese leadership . . . is digging the Communist Party's grave, by giving the Chinese people broadband."[8] Like many others, Kristof believed that the Internet, once it reaches a country, is an unstoppable liberating force. Kristof's colleague Thomas Friedman put it this way: "the Internet and globalization are acting like nutcrackers to open societies."[9]

This chapter explains why this conventional wisdom is wrong. Some people, when they see pornography and web gambling and hate speech flourishing on the Internet, wonder whether the techniques of intermediary control and individual deterrence can do the job. But as the China example shows, a government's failure to crack down on certain types of Internet communication ultimately reflects a failure of interest or will, not a failure of power. The developing Chinese Internet shows what a government that really wants to control Internet communications can accomplish.

The Chinese government does not try to control everything on the Internet. William Farris of the Congressional-Executive Commission on China states that the Chinese government is "drawing an increasingly clear line. You can talk about what you want, but no direct threats to Government."[10] It is trying to create an Internet that is free enough to support and maintain the world's fastest growing economy, and yet closed enough to tamp down political threats to its monopoly on power. The government is doing this by grafting Chinese nationalist ideology onto the network itself, in the process literally changing the nature of the Internet in China. Because of linguistic and cultural differences with the West, and because of the government's extraordinary system of monitoring and filtering, the Chinese Internet is becoming less and less like its Western counterparts—it is pulling away from the rest of the world.

China is not only an extreme example of control; it is also an extreme example of how and why the Internet is becoming bordered by geography. Only time will tell whether the China strategy will work, or whether the sheer volume of information will erode the government's influence and render the Internet in China open and free. But so far, China is showing the opposite: that the Internet enjoyed in the West is a choice—not fate, not destiny, and not natural law.

President Clinton and the China Democracy Party

When President Bill Clinton visited China in 1998, he pledged to spend time talking about freedom of information and human rights. While in Shanghai, Clinton stopped at an Internet café to mingle with young Internet users. He said afterward, "I had an incredible experience in one of these Internet cafés in Shanghai." Access, he declared, was now open to all. "Even if they didn't have computers at home, they could come to the café, buy a cup of coffee, rent a little time and access the Internet."[11] Clinton later joked about China's prospects for controlling the Net. "There's no question China has been trying to crack down on the Internet—good luck. (laughter). That's sort of like trying to nail Jell-O to the wall. (laughter)."[12]

While Clinton was visiting China, Wang Youcai, a political activist, decided to test Clinton's theory. On the morning of June 28, 1998, Wang went with two friends to the Civil Affairs Bureau in Hangzhou, China. The bureau is located near the famous and picturesque West Lake, former summer residence of the emperor, about eighty miles south of Shanghai. As part of a careful plan devised via e-mail, Wang decided to register, openly, an opposition political party, with a name similar to President Clinton's party: the "China Democracy Party."[13]

Wang was aware of the risks but felt the time was ripe. Clinton was in China; the regime had begun to signal some degree of political relaxation—yet another "Beijing Spring" in the history of Chinese politics; and the China Democracy Party had the liberating power of Internet technology on its side. Even if the registration failed, Wang had set up overseas websites, and used a U.S.-based e-mail newsletter ("VIP Reference") to communicate his ideas to thousands of mainland Chinese. The China Democracy Party would, they thought, follow a long history of overseas Chinese opposition movements and conduct its resistance in cyberspace. Wang was putting the Internet's capacity for political liberation to the test.

Wang's application was, unsurprisingly, rejected. The next day, June 29, police officers came to his home in Hangzhou. While his wife and children watched, they took Wang away. As his wife, Hu Jiangxia, later said, "Plain-clothes police came to our house around one o'clock and talked to my husband about his activities and about the China Democracy Party. They took him away just before four o'clock."[14] The detention came just as Clinton arrived in Shanghai, 80 miles from Wang's home.

Wang and others were formally charged, several weeks later, with "fomenting opposition against the government."[15] His wife wrote an impassioned letter to President Ziang Zeming. Does he "deserve to be treated like this just because of the pursuit of democracy and freedom[?]" she asked.[16] Her letter, available only outside of China, went unanswered.

On December 18, Wang was tried in a Hangzhou court without a lawyer. Facing a possible penalty of life imprisonment, he pled not guilty and conducted his own, unsuccessful, defense. His trial lasted only a few hours.[17] He was sentenced on December 21, 1998, to eleven years imprisonment and three years deprivation of political rights for subversion.[18] Around the same time, most of the other founding members of the China Democracy Party were tried and imprisoned. Wang and his colleagues had become Clinton's Jell-O, nailed to the wall.

Three days before Wang's sentencing, President Jiang Zemin gave a landmark speech commemorating the twentieth anniversary of economic reforms that began in 1978. President Clinton, during his visit earlier that year, described "a genuine movement toward openness and freedom."[19] But here Jiang spoke on a different topic: the necessity of absolute information control. "From beginning to end, we must be vigilant against infiltration, subversive activities, and separatist activities of international and domestic hostile forces," said Jiang to thunderous applause.[20] Standing before a giant golden hammer and sickle mounted between large red curtains, he announced his vision. "Only by sticking to and perfecting China's socialist political system can we

achieve the country's unification, national unity, social stability, and economic developments." He concluded that "The Western mode of political systems must never be copied."[21]

Wang Youcai's imprisonment is an example of a Chinese government strategy best expressed by the Chinese proverb "killing chicken to scare monkey." In other words, China practices Gary Becker's selective deterrence with a vengeance. Arrest and detention of those who criticize the government is the simplest method of killing the chicken to scare the monkey. But China uses the Internet to employ an array of more subtle methods to deter political activists. And it is doing much more on the Internet than practicing deterrence: It is changing the nature of the Internet itself.

Information Borders

What do the following websites have in common?

- Sex.com
- The U.S. Bankruptcy Court for the District of Massachusetts
- GALA: Gay and Lesbian Acceptance
- Depression Reality: Information and Support
- The University of Michigan Health System

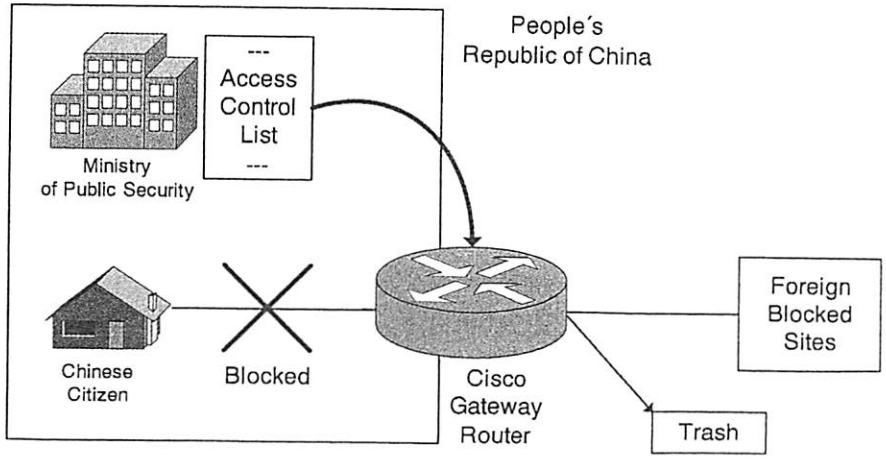
Each of these sites, external to China, was blocked or is blocked by the Chinese government as a threat to the Chinese State.[22] We know this because in 2002, Jonathan Zittrain and Ben Edelman manually dialed a Chinese Internet provider long distance, and in the guise of a Chinese end user, went looking for blocked websites. The results were the first-ever openly available list of sites that the Chinese government is blocking, or was blocking at the time.[23]

How does the Chinese government block sites outside its borders? China has surrounded itself with the world's most sophisticated information barrier, a semipermeable membrane that lets in what the government wants and blocks what it doesn't. In technical terms, it is a "firewall," rather similar to the security firewalls placed around corporations. Only this one is placed around the entire country.

China's information barrier was built primarily by Cisco, the Silicon Valley network vendor. In the early 1990s, Cisco and other companies developed products to let American corporations filter employee access to the Internet. Companies wanted the Internet, but they didn't want their employees on ESPN or playboy.com all day. Cisco demonstrated to Chinese officials long ago that the same products could be used to effectively block unwanted materials from entering China. It showed that it could be done flexibly, in a subtle fashion, and without loss of performance. Hence, the modern "Great Wall of China" is, in effect, built with American bricks.[24]

China's information barrier works because Internet data enters or leaves China at a limited number of points. At each of these "gateways," Chinese officials have ordered Chinese Internet carriers like China Telecom to deploy Cisco's equipment as a checkpoint. The key product is the "router," a sophisticated network computer that "routes" Internet traffic to the correct destination. Since a router knows how to *get* information to the right location, it can easily be reprogrammed to *lose* information instead. That's all that a basic filter is: an instruction to drop information from or for certain addresses.

In practice, the government provides a list (the "access control list") of all of the banned sites, identified by their IP address (e.g., 127.37.28.1) and their URLs (e.g., wutangclan.com). These sites, presumably, are obtained by the labor-intensive search conducted by the Internet Police or other agencies. Companies like China Telecom feed



their gateway routers the list of blocked addresses provided by the government. Subsequently, any message, or packet, carrying a forbidden address is simply dropped and never reaches its target. John Gilmore's idea from chapter 1 that the Internet "interprets censorship as damage and routes around it" is thus reversed: the router itself has become the censor.

But doesn't this filtering, which happens at high speed (what an engineer would call "wire-speed," or the speed of light), come at a performance cost? Not really. It can be more efficient to drop packets of information than to route them to their proper destination. Imagine how much easier and faster the mailman's job would be if he were allowed to dump half his mailbag into the garbage. The same goes for routers: the Cisco and other routers can block Internet traffic without a significant negative impact on performance. As a result, China gets an Internet just as fast as any other country's but limited to what China wants its citizens to see.

Chinese censorship is not only efficient but also subtle. No screen appears saying "Blocked by the Chinese State." Instead, the blocking takes on the appearance of technical error. A user who tries to reach, say, freechina.net, will get a "site not found" screen, a network timeout screen, or any one of a number of HTTP error codes.[25] And it can be difficult for an end user (and researchers) to know whether the problem is in fact censorship or technical difficulties. The mandated list of blocked sites changes as political events develop. For example, sometimes the *New York Times* website is available on computers in China, and sometimes it isn't.[26] This uncertainty, coupled with the general unreliability of the Internet, helps mask efforts at censorship.

So what does the Chinese government block? In 2005, Zittrain and a new team of Harvard researchers repeated Zittrain's original study and concluded that "China operates the most extensive, technologically sophisticated, and broad-reaching system of Internet filtering in the world."[27] They found that Chinese filtering had grown to focus even more carefully on the principal perceived threats to the Communist Party: Tibetan independence groups and human rights sites like Human Rights Watch or Amnesty International; religious or spiritual sites, such as Christian, Muslim, Jewish, Hindu, and even new-age churches; and, of course, any and all information related to the banned Falun Gong religious movement. And finally, the Party justifies the border blocking as a kind of defense against Western "dumping" of information on China. As the Party says, "Western countries, headed by the United States . . . dump on China massive amounts of information of all kinds, including their political models, value systems, and lifestyles, in order to oppose and edge out socialist values."[28]

China's border barriers are important. But ultimately they are not its most important form of Internet control. Some may imagine that Chinese citizens are dying to read an uncensored version of the *New York Post*, but that isn't so. Domestic interest in foreign sites within China is low to begin with, because the sites don't focus on China and usually aren't written in Chinese. As a result, the real centerpiece of China's system of information control is its internal controls.

Internal Controls

In the spring of 2005, China watchers and Microsoft haters found common ground when Microsoft admitted that its "MSN Spaces" service, allowing users to set up blogs in China, would block all titles like "freedom" and "democracy." A blog site titled "democracy" generated an error message as follows: "This message includes forbidden language. Please delete the prohibited expression."[29]

Microsoft is not the only American company helping the Chinese government to censor within its borders. Say you're using a Yahoo China online discussion forum and you type "It's time for an independent Taiwan and multiparty elections in China." In all probability, no one will react. The reason? Yahoo China, with the help of a time delay and a human or software filter, will block your message before it hits the chatroom.[30] As we saw in chapter 1, Yahoo, the former champion of free-speech rights in the United States, plays an entirely different role in China. It employs a host of censorship systems that continually monitor and filter what people see.

Just as Cisco's routers patrol the boundaries of China, American commercial service providers like Microsoft and Yahoo run an even more sophisticated program of internal information control within China. Through these and other methods of internal control, China has created a system—originally called the "golden shield" by the Ministry of Public Security—that complements China's external barrier.

Beginning in 2000, the Chinese Information Industry Ministry issued regulations defining the different kinds of content banned from discussion forums. In addition, as we saw in chapter 1, major commercial operators like Yahoo agreed in 2002 to a binding "self-discipline pact." The pact obliges signatories "not to produce or disseminate harmful texts or news likely to jeopardize national security and social stability, violate laws and regulations, or spread false news, superstitions and obscenities."[31]

In 2003, a group named Reporters Without Borders decided to test the effectiveness of the internal Chinese filters.[32] It wanted to see what would actually happen if political postings were made. Was it all just a lot of talk—or would posts actually be taken down? The results give us rare insight into the operation of an active censorship regime. They show a censorship system that is far from perfect, yet nonetheless prevents effective debate of topics the government does not want discussed.

The reporters, working from overseas, logged on to websites and began typing forbidden words. The first thing they learned was that all messages containing a set of forbidden words were automatically screened by software and never reached anyone. In their testing, any message or posting on a discussion forum stating words like "human rights," "Taiwan independence," "pornography," "oral sex," "BBC," or "Falun Gong" was filtered by machine and lost forever.

What about more subtle messages? The reporters found a subjective sliding scale at work, betraying a human intelligence. More sensitive or controversial messages would be blocked or quickly deleted. Less sensitive messages would last a little longer, but then also eventually be deleted. Direct criticism of government officials—such as demands for new political leadership—were in the former category, either never reaching the forum or facing near-immediate deletion. Conversely, less controversial subjects, like discussion of the Chinese role in the war in Iraq, lasted longer. But the important thing was that the messages did not last: most of those that even made it to the discussion group were eventually taken down within the hour.

In time, the user-accounts used to post messages were blocked and kicked off the discussion list. Had the reporters actually been in China, there is some possibility they would have been arrested and

prosecuted for subversive acts. Why would the ISPs erase messages and delete users? The reason is simple: threats directed at ISPs themselves. As the Congressional-Executive Commission (CEC) set up by Congress in early 2000 to monitor China's conduct has observed, systems "known for allowing cutting-edge postings on politically sensitive topics routinely disappear from the Internet altogether."[33]

The scale of human involvement in China's internal censorship system may be changing. The CEC reported that the Chinese government funded research in software designed to identify the political viewpoint of information. It described a "Falun Gong Content Examination System" that designates pro–Falun Gong information as "black," anti–Falun Gong information as "red," and articles dealing with Buddhism and health care as "neutral." "The system can be installed on personal computers, servers, and at national gateways, so that as soon as a user tries to visit a web page that is pro-Falun Gong, the system can filter the page and immediately notify authorities."[34] While the effectiveness of the Falun Gong content examination software is hard to verify, it is clear that China will continue to invest in ever-more automated internal control and filtering systems.

Increasingly sophisticated filtering systems are not, of course, the only methods of internal control. The Chinese government also deters unwanted political communication (and in the process enhances its monitoring capabilities). For example, it requires bloggers to register with the central government, and it closely polices Internet cafés.[35] In the early 2000s, authorities conducted major crackdowns that closed thousands of "illegal" cafés across the country.[36] Today, regulations in cities like Shanghai, where Clinton went, require users to register with their national ID card before logging on. Regulated cafés also feature cameras pointed at computer screens and, occasionally, roving police officers who simply watch what users are doing. Far from being a liberating force, the Internet café in China has become a major site of government surveillance.

Promoting Nationalism

Ma Zhichun lives in central China and meets the exacting qualifications necessary for his job. He is less than forty years old, a university

graduate with a background in journalism, and has extensive experience using the Internet. Ma's job is "Internet Commentator" for the Siquan City External Propaganda Office. He is paid to secretly influence public opinion, as found on chatrooms and elsewhere, in directions that favor the government. As Ma explains his job, "the key is to seize the initiative."[37]

It is wrong to say that the Internet has failed to promote a new political consciousness in China; it just hasn't been the kind the West had hoped for. Sometimes, to be sure, dissidents have used the Internet to the government's disadvantage, and sometimes political sentiment on the Net has exposed the political corruption of individual officials. But what has emerged, usually with the tacit support of the government, is Internet support for a different ideology: Chinese nationalism, often laced with virulent anti-American or anti-Japanese sentiment. The government is using the Internet, in other words, to direct anger away from the Communist government and toward China's foreign "enemies."

In May of 1999, an American B-2 bomber, using an outdated map, dropped four 2,000-pound bombs on the Chinese embassy in Belgrade, destroying the building and killing three Chinese citizens.[38] Government-operated media immediately suggested, on the Internet and elsewhere, that the bombing was no mistake. As anti-American riots erupted, the *People's Daily*, China's largest newspaper, helpfully created a chat-forum called the "Anti-Bombing Forum" (later changed to the "Strong country forum.") According to Shanthi Kalathil of the Carnegie Endowment, the forums played a "small but significant role in legitimizing among an elite, wired section of the population the Chinese government's position that the bombing was deliberate."[39] They also provided the first outlet for anti-American rage on the Internet, setting a pattern that has been followed and encouraged.

In 2001, an American EP-3 surveillance plane was confronted by two F-8 Chinese military jets off the southeastern Chinese coast. The American plane collided with one of the F-8s, killing the Chinese pilot and forcing the American plane to conduct an emergency landing.[40] The Americans were held by the Chinese government for a time, and the Internet chatrooms erupted as never before. "If little Bush goes on squawking, we should rope together his 24 white pigs and parade them through the streets," read one reported posting.[41] The official online and paper media fed the fire. "On this planet only the stuck-up United States is this rude and unreasonable."[42]

Japan has not been left out. In 2003, Internet chatrooms buzzed with anger after reports of police breaking up a giant orgy held in a Chinese hotel by Japanese businessmen. In the spring of 2005, the Japanese government approved the use of a controversial textbook which among other things refers to Japanese occupation troops as "liberators." Anger on Chinese chatrooms spilled into the street and raged for weeks. Protestors stormed Japanese department stores and chanted anti-Japanese slogans, fueled by chatroom rage.[43] According to reports, the protests were well within the control of the government and sometimes even orchestrated by it. One protest organizer explained, "We provided the police with the names of the people participating and the slogans we would use."[44]

For anyone acquainted with twentieth-century Chinese history, there is something very familiar about government-sanctioned anger against "enemies." During the Cultural Revolution it was "old ways" and whoever had been chosen as the reactionary of the week. China is today a very different place than it was in the 1960s or the 1990s. The

Anti-Japanese protests stirred by Internet chatrooms (Frederic J. Brown/AFP/Getty Images)

government, however, is not above defining enemies and not above using public rage as a political tool. Even after the September 11, 2001, attacks on the United States, there were mixed reactions from Chinese Internet users. Though China itself has been the victim of terrorist attacks, Americans who live in China were shocked by the responses. Some Chinese did express their horror at what had happened, but just as common was a sense that America was getting what it "deserved." A censorious government says much by what it doesn't choose to block. Left untouched was one well-reported post: "Airplanes? Why not an atomic bomb?"[45]

Changing the Network

In the middle of all this control we must keep sight of a crucial fact. Unlike Burma or Cuba, China is not stopping technological progress in exchange for totalitarian control. Quite the opposite: China wants to have the fastest and most sophisticated information network in the world. It is spending tens of billions to achieve this goal.[46] It is following the South Korean model—mass investment in Internet infrastructure. China wants to become one of the most advanced networking countries on earth while continuing to maintain control of information.

Consider the story of video-on-demand. In the 1990s and early 2000s there was much talk in the United States of the promises of "video-on-demand," the delivery of movies and video to consumers' homes. Despite industry blather, there were few examples of actual deployments, and no examples of such systems making money. Enron did report more than $100 million in revenue from its video-on-demand business and projected the value of the unit at $20 billion. But the service had, in fact, never launched.[47] Video-on-demand was notable in the United States largely as a means of defrauding investors.

Yet visit the campus at Beijing University, better known as BeiDa, and you're in for a surprise. The dorm rooms at BeiDa are crowded, holding six students in a room an American would find crowded for one. Yet the computers in the crowded dormitories of BeiDa are equipped with advanced video-on-demand capabilities. Indeed, a broad range of films are available, including popular commercial releases from Hong Kong and Hollywood. The students, of course, take it for granted. But it is in small ways like these that urban China, while still behind, is becoming more wired, and more Internet driven, than its Western counterparts.

Conventional wisdom has suggested this will never work—a country cannot open itself up to the Internet *and* maintain fierce political control over its citizens. As Tom Friedman wrote of China in 2000: "What makes the Internet so dangerous for police states is that they can't afford not to have it, because they will fall behind economically if they do. But if they have it, it means they simply can't control information the way they once did."[48] A country could either reject the network and remain a technological backwater, or let the Internet in and lose all control.

But none of that is true if the center of gravity shifts, if China has the power to create its own sphere of influence over network norms. In raw numbers, China is becoming its own network center of gravity. According to a recent survey, the number of Chinese Internet users had risen to 103 million by July 2005, making China second only to the United States in number of Internet users.[49] The size of the Chinese domestic Internet now exceeds the world Internet of 1997. That size means more power to control the most basic building blocks of network design: network standards.

In the United States, Wi-Fi, or wireless Internet technology, is widely hailed as the harbinger of easy, open, and anonymous Internet access. Oftentimes, in any large city, you just turn your computer on and find that you're connected. Cafés and campuses across the United States and Europe are just two of the locations that have gone wireless. Wi-Fi is fast, usually anonymous, and often free.

While China likes the promise of wireless technology, it doesn't like the anonymity and anarchy of the American standard. In the early 2000s, China therefore took up the fight for its own, closed, Wi-Fi standard. In December 2003, citing "national security" concerns, it mandated that a technology known as the WAPI, the "WLAN Authentication and Privacy Infrastructure" be incorporated into every Wi-Fi device used within its borders by June 1, 2004.[50] What WAPI does is simple: it makes a wireless network closed rather than open, by forcing every user of a wireless network to register with a centralized authentication point.[51]

China's WAPI initiative, however, ran into trouble with world trade rules. "This is the most ludicrous trade barrier I have ever come across," said Frank Vargo at the time, a representative of the U.S. National Association of Manufacturers.[52] Certainly part of China's motive was to give business to local companies, since it refused to give foreign companies access to its encryption standard. But there is something deeper going on here. As the founding engineers knew, control over the Internet's standards is how network norms are created. As China seizes control over certain standards, it can put its mark on what kind of products reach its markets and ultimately have a say in what the network is like. The WAPI effort, noted Dave Eberhart, was "a long-term move to make the Chinese WAPI the world standard, dissing long-standing [standards bodies]."[53]

Under pressure from the United States and threat of World Trade Organization intervention, China ultimately suspended its absolute requirement of selling WAPI with every Wi-Fi. But China hasn't given up on the standard, which it is still pushing. The real significance of this episode is for the future of standard-setting. Rebecca MacKinnon, a China expert, puts it this way: "What happens when the next wireless standard is invented in China and performs to government specifications? That's the aspect of this episode that should not be ignored. China is doing what it can to influence the network protocols of the future."[54] Its actions portend a future when China does battle with other nations, most likely the United States, over major Internet standards.[55]

The billions spent building the Chinese network are also having their effects. Physically, the Internet within China looks more and more like a giant office network, centralized by design.[56] In the spring of 2005, China announced its latest buildout—the "Next Carrying Network," or CN2, a massive new intra-Chinese network that will be incredibly fast, but also built by a single, government-owned company and easily filtered at every step. While such things are hard to measure, Internet maps suggest that growth in China's domestic bandwith is rapidly outpacing the speed of its international connections.[57] Network-wise, China will soon be like a country with a great internal transport system but relatively few roads leading in or out. That means information coming from abroad will be that much slower to arrive, that much more likely to get stuck in a network traffic jam.

Countermeasures

Some technologically savvy readers may be thinking that these controls will be ineffective because Chinese users can get around them. It is an article of faith among techno-optimists that China's controls are fallible and therefore destined to fail.

It is of course true that technologically savvy users can avoid many and perhaps most of the Internet controls imposed by the Chinese government. But as we have argued throughout this book, governmental controls need not be perfect to be effective. The real question is whether and how circumvention of control by a few savvy users will make any difference to China's political evolution. Any movement toward democracy and Western-style government must compete with the nationalist ideology that the Communist Party is weaving into the Internet itself. The effect of the government's control of the media, including the Internet, is not to kill all discussion of democracy, but to put any democratic movement at a major comparative disadvantage.

Consider the all-important chatrooms, where discussions of democracy are banned. Not a problem, some say—even on the most closely monitored chatrooms, people will talk about "cabbages" when they mean "democracy." As one blogger wrote, "No democratic movement in the history of mankind has ever stalled just because the word 'democracy' could not be uttered."[58] True, inventing secret languages can make it hard for the government to understand and censor ideas. But it also makes it hard for ordinary Chinese to have any idea what you're talking about. As Harvard law professor Bill Stuntz puts it, a secret code "is only effective if people know it, and if other people know it in any significant number, the government will likely also know it, and so can block it. It's a perfect catch-22. The secret code either won't work, or its users will be caught."[59]

At a broader level, if you're talking about carrots and cabbages instead of multiparty elections, the Communist Party is already ahead. The cabbage discussion must be seen in context: it is competing with open and fervent discussions of China's greatness, along with complaints about the latest Japanese or American "outrage." In the history of nations, arguments for tolerance and democratic values have not always beaten out nationalist fervor among the masses. And in China, so far, Internet-driven nationalism appears to be beating democracy

hands down—especially when the democratic movement is saddled with extensive controls.

The ultimate effect of the Internet and China's efforts to control it on China's political evolution is difficult for anyone to assess. But if this chapter suggests anything, it is that the West must abandon the facile yet still dominant assumption that these controls are meaningless or ineffective or bound to fail. We in the West are used to an Internet that is free. But the story of the People's Republic shows the contingency of the Internet's identity, a contingency that reflects its birth in the United States. China is an enormous force that is changing the Internet's identity. As law professor Peter Yu puts it, "the question is no longer how the Internet will affect China. It is how China will affect the Internet."[60]

seven

The Filesharing Movement

Some people change history by accident, and Niklas Zennstrom counts as one of them. This soft-spoken and still largely unknown Swede, described by the *Washington Post* as a "younger, hipper version of Bill Gates," started two small companies in the early 2000s that have already done much to change how people exchange information in the twenty-first century.[1] His first company created a filesharing software application called "Kazaa" that was destined to become the most downloaded program in history. Millions of people used Kazaa to exchange billions of songs in open defiance of national copyright laws.

This chapter chronicles the filesharing movement, in which Zennstrom and Kazaa played a big role. At its height this movement led many to believe that filesharing might upend the central role of national copyright law in the distribution of information. With the benefit of hindsight, we can now see that this was not to be. And so in part, this chapter is a sequel to chapters 5 and 6, showing again the importance of law and national government, even for filesharing—a technology designed to be impossible to control.

This chapter also introduces a crucial new theme: the effect of technological change on the market and the legal system. Filesharing introduced a cheaper method of distributing music that sparked massive changes in the economics of music distribution and the behavior of consumers. These changes were a jolt to the copyright law system that seemed to many to render it irrelevant. What appeared a threat to copyright law, however, turned out simply to be the law's hesitation and