Chapter 11

The Empires Strike Back

The promise was freedom. And, for a time, freedom was the reality.

The Internet, some of us believed early on, would be a largely unregulated sphere where boundaries would not matter—where, for good and bad, individual freedom would be the paramount condition. After all, the Internet was a robust communications system; it could, in theory, withstand a nuclear attack. So early Netizens can be forgiven for assuming that different rules applied because, for a time, they did.

Cyber-liberty, we saw, would extend to culture and information in powerful, even unprecedented, ways. The Internet—the first many-to-many medium—was going to liberate us from the tyranny of centralized media and the rancid consumerism that says we are merely receptacles for what Big Business, including Big Media, wants us to buy. We were going to turn the world of "take it or leave it" into an informed global conversation. Consumers would become true customers. The governed would become "we, the people" participants in the political process.

But the clampdown has begun. Everywhere we look, the forces of centralization and authority are finding ways to slow—and perhaps halt altogether—the advances we've made.

They include the usual suspects, namely government, big telecommunications companies, and what I call the copyright cartel of entertainment companies. But, sadly, they also include some of the technology pioneers who once promised so much in the way of digital liberty.

Could these increasing restrictions impinge on grassroots journalism? They could indeed, and we will have to fight to keep our freedoms. The alternative could be a news regime that is dictated almost entirely by governments and mega-corporations—a situation worse than what we have today when Big Media already controls so much.

What follows is a description of the most serious threats, and what we might do, individually and collectively, to counter them.

GOVERNMENTS GET NERVOUS; BIG BUSINESS GETS NOSY

So far, state intervention has tended to be more blunt than subtle when applied to grassroots journalism. For example, several times during 2003, the government of China flipped a switch, figuratively speaking, and indiscriminately turned off access to thousands of weblogs. The Great Firewall, already in use to block specific news and information sites the government didn't want its people to see (including my own newspaper's), was now preventing all manner of sites created on Blogspot.com (a leading blog-hosting site) from being read by web users inside the country.[286]

China is far from alone in censoring political content. Saudi Arabia has pervasive controls, according to a study by Jonathan Zittrain and Ben Edelman of the Berkman Center for Internet and Society at Harvard Law School. But government interference—such as stopping data traffic at arbitrary borders on the whim of a government or a company—is growing more common in general, not less, and it's not just in repressive regimes such as China and Saudi Arabia, but also in France and Singapore. Nor is filtering the only infringement. Law enforcement officials in the Western democracies, including the United States, are pushing for surveillance capabilities that would surely have a chilling effect on politically off-center speech.[287]

Truly free access to information—the word "free" is used here in the context of "freedom," not cost—implies an ability to send and receive information without being tracked. We're losing that ability swiftly, and the supreme irony is that American businesses, not governments, have been the prime privacy invaders when it comes to applying technology for everyday surveillance.[288]

Under the Web's original architecture there was no way for anyone to know you'd visited a web site or what you'd done there. But in the mid-1990s, Netscape developed "cookies," little files placed on users' computers that allowed the owner of a web site to track where visitors went, and when. Stanford law professor Lawrence Lessig, concerned about the privacy implication of cookies, said that rather than naming the technology something "sweet and happy like 'cookies,'" they should have named it what it was: "Network Spy."

Cookies had, and have, big privacy implications. But like all such technologies, they have their good points. They can save time for the user, storing one's preferences for a particular site. Without cookies, my personalized Yahoo! page would not exist. But fears about cookies led some Net users to set their web browsers to refuse their placement on their computers so their movements couldn't be tracked. Site developers, meanwhile, found them invaluable for marketing and ease-of-use purposes. Cookies became a staple on the Internet, and they aren't going away.

Cookies become a more serious privacy problem when you consider a real-world situation. When you go to a shopping mall, no one follows you around with a video camera, recording everything you look at. (Hidden cameras, becoming more ubiquitous, may change this equation.) But that's exactly what cookies allow: a view of everything a computer user does on the Web. As a result, people's private data has become a commodity to be bartered to the highest bidder, or to anyone wielding a subpoena.

Computers can also track the movement of information around the Internet. Lessig related the time he set up a Morpheus peer-to-peer server so people could freely download copies of his lectures. He got a frantic call from the Stanford "network police"—the university's systems administrators—saying there had been illegal activity detected on a machine in his office—and as a result, the machine had been disconnected. Fearing the wrath of the entertainment industry, the administrators had assumed illegal acts because of the presence of the technology, even though they were actually thwarting an entirely legal use of the software.[289]

Filtering of spam and other so-called objectionable content, meanwhile, has led to an ad hoc system of content blocking. Spam blacklists run by volunteer organizations have been adopted widely, causing the mail of innocent users—who happen to be using an Internet service provider that also has a spammer using the same system—to disappear into a black hole. This isn't censorship, legally, because governments aren't doing the blocking. But it's a disturbing trend when good intentions lead to the widespread blocking of content that is objectionable only to a narrow subset of those who'd receive it.

Filtering can include what technologists call "IP Mapping," in which a server checks the Internet address from which some data is being requested. The inevitable result will be Internet zoning. As noted in Chapter 10, someday soon, when people from different countries visit the same page, they'll see different information.

THE COPYRIGHT CARTEL

Article I, Section 8 of the Constitution gives Congress the power to "promote the progress of science and useful arts, by securing for limited times to authors and inventors the exclusive right to their respective writings and discoveries."

I won't go into the historical details of copyright law (Lessig's writings, in particular his book *Free Culture: How Big Media Uses Technology and the Law to Lock Down Culture and Control Creativity*,[290] are a good place to learn more.) But, it's safe to say that today's situation has perverted the Founders' intent, and it looks as though the situation could get much worse.

What's important to understand is how the very notion of copyright has changed since the Founders first enshrined it in the Constitution. Originally intended as a bargain between creators and the rest of us, it has become an instrument of harsh, absolute control. Balance has disappeared.

By law and tradition, copyright laws gave rights to users of a copyrighted work, not just to the work's creator. For example, scholars could quote from copyrighted works in order to create new works. This is the notion of "fair use"—to use a small portion of another's work as part of a new work. Fair use has expanded in recent times to include, among other things, making personal backups of software and time-shifting television programs (recording a show to watch it later). But the forces of control have moved the line. They believe fair use is something that can be granted only by the copyright holder if he or she (or it, in the case of a corporate holder) is willing to grant fair use—and the law, when new technology comes into use, increasingly supports their position.

But the whole point of fair use is to define a zone of use that copyright holders don't specifically authorize, and may even oppose, but which is legal anyway. Siva Vaidhyanathan, director of the undergraduate program in communication studies in New York University's Department of Culture and Communication, tells the story of the author who wrote a scholarly book about country music but didn't quote any lyrics. The author's skittish publisher, fearing lawsuits from copyright holders even though use of such quotes would plainly have fallen under fair-use guidelines, decided it wasn't worth the trouble to get permission; hence, the book was published without all the lyrics she wanted to use.[291] To turn fair use into

the exclusive realm of authorized uses is to remove fair use almost entirely. We'll come back to this crucial point later in this chapter.

One of the keystones of "intellectual property" is that a work goes into the public domain after what the Founders defined as "limited times," which allowed a copyrighted work to pass into the public domain so others might freely build upon it. "Limited times" were first defined as 14 years but have been progressively extended by Congress at the behest of copyright holders such as Disney. What were once 14-year terms have now been extended to the life of the author plus 75 years, or 95 years when a copyright is held by a corporation. By amazing coincidence, copyright terms seem to get extended every time Mickey Mouse comes close to entering the public domain, which means that nothing is going into the public domain anymore. This is a double-barreled heist by the copyright holders. They're stealing from our common heritage in order to protect a few valuable works. And they're thwarting innovation.

If the rules and enforcement regimes that apply today had been applied in the 1930s, Walt Disney might never have been able to create Mickey Mouse, which was a derivative work based on other people's creations. And Victor Hugo is surely spinning in his grave at the way the Disney empire of today took *The Hunchback of Notre Dame* and turned that story into a children's cartoon. But his work had entered the public domain, and new art was the result.

What does this mean for modern grassroots journalism, which relies on people's freedom to use all manner of digital content in all manner of ways? Nothing good.

EYE OF THE BEHOLDER

There are many ironies in the current copyright debate. None is more notable than the fact that the industries now pushing for

such absolute control got their start doing what they'd call "piracy" today. But it's also a shame to see an industry that has fought so honorably to maintain First Amendment protections, without which it could not itself survive, now leading a charge that threatens other people's speech.

Technological advances always threaten established business models. And the people whose businesses are threatened always try to stop progress. Cory Doctorow is an online civil libertarian and science fiction author who published two novels and also made them freely downloadable online the day they were in bookstores. "The Vaudeville performers who sued Marconi for inventing the radio had to go from a regime where they had *one hundred percent* control over who could get into the theater and hear them perform to a regime where they had *zero* percent control over who could build or acquire a radio and tune into a recording of them performing," he told me. The performers, in other words, wanted to prevent new technology from disrupting a successful old business model.

It wasn't the only time. In one of the most important recent examples, Hollywood tried to kill off the home video recorder. Only by the narrowest margin in the Supreme Court, in a crucial 1984 decision, did Americans preserve the right to tape a TV show and play it back later.[292]

The advent of digital technology terrified the entertainment industry, and for apparently good reasons. After all, a digital copy of something doesn't degrade the way analog copies, such as a copy of a videotape, do in just a couple of generations. And cyberspace threatened to be the world's biggest enabler of infringement because of how easy it is to copy and distribute materials over it.

But the industry has cleverly, though wrongly, framed the argument as "stealing" versus "property rights." In fact, the issue is nothing of the kind. Ideas are different than physical property, and they have been treated distinctly through our history. If I take your car, you can't use it. If I have a copy of your song, you still have the song. Infringement is wrong, and I don't

defend it. But there has always been some infringement, and copyright holders have lived with it as part of their overall bargain with society.

Hollywood, and the music companies in particular, began sounding an alarm in the early 1990s. They had the ear of Congress—largely a result of large campaign donations plus a bias toward property rights over all other rights—and in 1998, they persuaded federal lawmakers to pass the Digital Millennium Copyright Act (DMCA), a law that was said to bring copyright policy into the digital age and that respected the rights of users and producers.

The DMCA was radical and complex legislation.[293] It tipped the balance toward copyright holders far beyond anything they'd enjoyed before. One especially bad provision criminalized the use of technology that could be used to circumvent copy protections, no matter how legitimately someone might use the circumvention. It's even forbidden to tell people how they can do such things, as Jon Johansen, the Norwegian hacker of DVD encryption code, and Eric Corley, the publisher who dared post it, discovered to their dismay.

The law has been abused repeatedly. Scholars have faced legal threats for publishing research about the weak security protections the entertainment companies have used on their material.[294] A Russian programmer was indicted in 2002, and his company was put on trial (and acquitted) for selling software that could be used to make copies of electronic books.[295] A printer company has used the DMCA to sue the maker of an inexpensive replacement cartridge.[296] The cases grow in number and strangeness every year.

CHARM AND TOUGHNESS

No one could sum up the issue from the entertainment industry's perspective better than Jack Valenti, longtime head of

the Motion Picture Association of America and point man for the copyright lobby. He was his typically charming self when I visited him in his Washington office in the fall of 2002. According to Valenti, everything flows from the principle that Hollywood wants to make its customers happy, and the Internet could be one of the greatest vehicles for making people happy. But the Net's potential is counterbalanced by major threats, and unlike previous methods of delivering movies to customers, the Net gives people new ways of "taking things that don't belong to them."

It sounded so, well, reasonable. But Valenti genteelly refused to answer a key question, namely how Hollywood thought it could protect its films and TV shows from being copied and distributed on the Internet while not infringing upon citizen's fair use rights rights (such as quoting from, not just time-shifting, programming) that are so vital to journalism and intellectual innovation in general. And he was adamant that technology in the future—including personal computers—will have to be modified to prevent people from making unauthorized copies.

Valenti, who said in early 2004 he'd step down from his post later in the year, named three main areas where the entertainment industry is looking for fixes—namely, the broadcast flag, the analog hole, and peer-to-peer file sharing. In each case, negotiations with technology and consumer-electronics companies will have to produce a mutually agreeable result, he said.

Only one had been negotiated with the tech industry, and the FCC enacted it in 2003. This was the "broadcast flag"[297]—the practice of marking digitally broadcast material to prevent unauthorized copying. Theoretically, home TV viewers would still be able to time-shift digital broadcasts, but they wouldn't be able to redistribute the shows they'd copied. Of course, even the right to copy at home is merely a rule, and you can be sure the entertainment companies will try to circumscribe even this level of customer freedom. And never mind that it's impossible to effectively prevent one kind of use—copying beyond the home—while fully permitting the in-home flexibility at the same time.

The next problem Valenti identified was what the entertainment companies call the "analog hole." Humans can't read the zeroes and ones that make up digital media. Machines translate digital content into what our eyes and ears see and hear as video and audio. So even if you can lock down the zeroes and ones, all someone has to do is play the video on a TV, then use a video camera to make a copy of what's on the screen, redigitize that copy and, boom, the problem starts again. The industry is looking for technology—and laws—to make it impossible and illegal to do this.

The third area of worry was the biggest: peer-to-peer online file sharing. The movie industry watched what happened in the music business and got scared.[298] The movies now available on the Net have escaped control forever, but something needs to be done to prevent theft of movies through file-sharing networks, he said.

The entertainment companies are now demanding that technology companies restrict the capabilities of devices at the outset. They want to cripple PCs and other devices so they can't make copies the copyright holders don't explicitly allow. The Broadcast Flag is one such step in a dangerous direction. Even more brazenly, the entertainment industry also wants permission to hack into networks and machines it believes are being used to violate copyrights. In 2002, a California congressman proposed legislation that would legalize this corporate intrusion; so far, thankfully, it hasn't gone very far.[299]

Give copyright holders the ability to "fix" all of their perceived infringement problems, and you give them unprecedented control over tomorrow's information, over culture itself. Here's an example: it is currently illegal to copy a snippet of video directly from a DVD to use as part of another work. But you can do this with a piece of text, though the e-book industry is working to prevent even a small cut and paste unless authorized by the copyright holder. If we need permission or have to pay, simply to quote from other works, scholarship will be only one casualty.

There is also a serious privacy question in the copyright debate. The only possible way for entertainment companies to enforce their copyrights will be to track what individuals purchase and how they use it. Someday, sooner than you may like, big corporations and governments will know every copyrighted work you read, listen to, and watch. Anyone with a sense of history should fear such a system.[300]

This kind of future would doom much, though not all, of the participatory journalism I've been promoting in this book. For example, if every amateur journalist had to ask permission before quoting from a copyrighted work or was forced to pay for each quotation, most wouldn't bother. The ever-present threat of the copyright police who interpret fair use through Congress' latest restrictive laws, would be as chilling as anything we could imagine.

Sadly, it isn't just the movie and music companies that are taking this stance. Book publishers have increasingly looked at online distribution with fear, when they should see it as a practical step beyond antiquated printing and distribution systems, and an opportunity to win new customers. They are supporting a system that mocks the First Amendment, on which they rely for their very existence; publishing, after all, is built on a foundation of free speech. Lending libraries in particular are in jeopardy if publishers take the same hard line that the music and movie companies have taken, because in a pay-per-view copyright regime, lending becomes impossible.[301]

Then again, intellectual consistency rarely survives financial threats, perceived or real. Again, I can understand the worries. Publishers are worrying more about the effect illegal distribution might have on the bottom line than they are considering the incredible possibilities in exploiting (in the best sense of the word) the potential. I like the idea of being able to annotate an electronic book and go to other resources via, say, hyperlinks; but if the cost is an inability to make a backup copy to use on another electronic device, or even a restriction prohibiting me from giving the book away, that's too high.

Here's one more way the entertainment industry's goals could put a severe crimp on tomorrow's journalism. In Chapter 2, I explained the value of peer-to-peer technology for inexpensively distributing large audio and video files created, for example, by a blogger. Internet service providers charge based on the amount of traffic your site receives and the amount of bandwidth it takes to serve your content to the people who want to see it. In other words, the more popular your content becomes, the more it costs you—a painfully opposite situation then the one you face in the physical world where economies of scale work in your favor.

Now remember that the entertainment industry hates peer-to-peer technology because it doesn't control it. Also recall that it has launched a blizzard of lawsuits that killed innovative companies such as Napster and ReplayTV, a company that created home video systems for recording and storing programs, as well as for skipping commercials. The entertainment industry has also launched a platoon of lobbyists to persuade Congress and regulators to put the clamps on other peer-to-peer technologies, and it's going after people who use them.[302]

If it succeeds in its clampdown, it will foreclose the single most effective method of distribution for grassroots audio and video. Even if all it accomplishes is to force peer-to-peer services to individually track what is sent and where, it will send a chill over the kind of grassroots journalism that has been so vital to freedom in authoritarian nations. The future of media doesn't just belong to people who can depend on a First Amendment; it also belongs to the rest of the world, or it should.

THE TECH INDUSTRY SELLOUT

A few years ago, policy watchers talked about the war being waged between copyright protection and innovation. The lines were drawn: Silicon Valley was inventing new technology, and Hollywood wanted to control its use. The news from the front is

not good for the people who depend on technology to produce tomorrow's news.

Slowly but surely, key members of the tech elite have evolved from being fiercely independent to being a lackey for the entertainment companies on some key issues. Intel, the giant maker of computer chips, has its fingers all over the Broadcast Flag technology that the FCC has mandated. This wasn't the first time Intel betrayed its own customers. It did so during the DVD negotiations years earlier, when Hollywood demanded a Content Scrambling System that led to severely restricted uses for DVDs—a system that an Intel insider later acknowledged had caused PC users real problems.

But no technology company has done more to curry favor with the copyright cartel than Microsoft, a company that (like many technology firms) repeatedly ignored copyright law in building its own powerful business. Here's how Cory Doctorow put it:

> When Microsoft shipped its first search-engine (which makes a copy of every page it searches), it violated the letter of copyright law. When Microsoft made its first proxy server (which makes a copy of every page it caches), it broke copyright law. When Microsoft shipped its first CD-ripping technology, it broke copyright law.
>
> It broke copyright law because copyright law was broken. Copyright law changes all the time to reflect the new tools that companies like Microsoft invent. If Microsoft wants to deliver a compelling service to its customers, let it make general-purpose tools that have the side-effect of breaking Sony and Apple's DRM [Digital Rights Management], giving its customers more choice in the players they use. Microsoft has shown its willingness to go head-to-head with antitrust people to defend its bottom line: next to them, the copyright courts and lawmakers are pantywaists, Microsoft could eat those guys for lunch, exactly the way Sony kicked their asses in 1984 when they defended their right to build and sell VCRs, even though some people might do bad things with them. Just like the early MP3 player makers did when they ate Sony's lunch by shipping product when Sony wouldn't.[303]

Unfortunately, Microsoft's answer has been to build Digital Rights Management—the more appropriate term is "Digital Restrictions Management"—into just about everything it makes. Restrictions range widely. You might be allowed to view something on multiple devices, or just one. You might be permitted to copy a section, or all, or none. You might not be able to print a text document, and so on. These restrictions are notably part of the "Windows Media Center" system that connects PCs with TVs and other devices. The mantra of DRM-believers is that they are enhancing security and protecting intellectual property. The effect, however, is to deny people fair use and other noncontroversial uses of what they have bought, or even own.

Even Apple has jumped aboard the DRM train, though not with the same zeal Microsoft has shown. Apple's iTunes Music Store, which sells songs, encodes them in a format that can't easily be converted to the wide-open MP3 or OGG formats. The DRM scheme, instituted because the music industry demanded it, gives Apple users more freedom to copy songs among different devices than we saw in prior DRM schemes. But it tends to penalize some of Apple's best customers—people who repeatedly buy new Macs. An iTunes Music Store customer can listen to the songs on five computers, but managing authorizations can be a hassle. It's also important to remember that what freedoms Apple gives today can disappear tomorrow.[304]

Microsoft, Intel, and several other major technology companies are now working on a "Trusted Computing" initiative, putatively designed to prevent viruses and worms from taking hold of people's PCs and to keep documents secure from prying eyes. Sounds good, but the effect may be devastating to information freedom. The premise of these systems is not trust; it's mistrust. In effect, security expert Ross Anderson wrote in 2003, trusted computing "will transfer the ultimate control of your PC from you to whoever wrote the software it happens to be running." He went on:

> [Trusted Computing] provides a computing platform on which you can't tamper with the application software, and where these applications can communicate securely with their authors and with each other. The original motivation was digital rights management (DRM): Disney will be able to sell you DVDs that will decrypt and run on a TC platform, but which you won't be able to copy. The music industry will be able to sell you music downloads that you won't be able to swap. They will be able to sell you CDs that you'll only be able to play three times, or only on your birthday. All sorts of new marketing possibilities will open up.

But now consider the ways it could be used, beyond simple tracking by copyright holders of what they sell. Anderson wrote:

> The potential for abuse extends far beyond commercial bullying and economic warfare into political censorship. I expect that it will proceed a step at a time. First, some well-intentioned police force will get an order against a pornographic picture of a child, or a manual on how to sabotage railroad signals. All TC-compliant PCs will delete, or perhaps report, these bad documents. Then a litigant in a libel or copyright case will get a civil court order against an offending document; perhaps the Scientologists will seek to blacklist the famous Fishman Affidavit. A dictator's secret police could punish the author of a dissident leaflet by deleting everything she ever created using that system—her new book, her tax return, even her kids' birthday cards—wherever it had ended up. In the West, a court might use a confiscation doctrine to "blackhole" a machine that had been used to make a pornographic picture of a child. Once lawyers, policemen and judges realise the potential, the trickle will become a flood.[305]

The Trusted Computing moves bring to mind a conversation in early 2000 with Andy Grove, longtime chief executive at Intel and one of the real pioneers in the tech industry. He was talking about how easy it would soon be to send videos back and forth with his grandchildren. If trends continued, I suggested, he'd someday need Hollywood's permission. The man

who wrote the best seller, *Only the Paranoid Survive*,[306] then called me paranoid. Several years later, amid the copyright industry's increasing clampdown and Intel's unfortunate leadership in helping the copyright holders lock everything down, I asked him if I'd really been all that paranoid. I never got a direct reply.

THE END OF END-TO-END?

A key design goal of the original Internet was called the "end-to-end principle." Essentially, it states that we want to keep the intelligence out at the edges of the network and make the transportation of data as simple as possible in between. In other words, use the network to get the zeros and ones back and forth with as little interference as possible, and let people using PCs, servers, and other devices do everything else. In an email, David P. Reed, one of the people credited with the notion, described it this way:

> Communications systems should not implement functions that can be implemented by their users. In particular, systems designers should work very hard to find or invent system designs that avoid putting specific user-oriented functions into inflexible infrastructure, by moving the implementation of those functions to the edges of the network where they are implemented as part of the user-controlled applications.
>
> It's been the experience in the Internet design community that many functions that are thought to be "network" functions or capabilities are possible to implement in the form of protocols among users or user applications. For example, security can be implemented by end-to-end encryption and end-to-end credentials [that can't be forged], so that the network need not be secure at all.
>
> Similarly, when you are forced to think about problems such as spam in an end-to-end way, you start to realize that

> the problem with spam cannot be solved in the "network"—instead it is a problem among users of the network, and must be solved there. It's still difficult, of course, but its difficulty is inherent in the conflict between the desire to allow anyone to contact us freely and the desire to be left alone. The network cannot understand the details of our individual desires; the end-to-end principle says it should not even try.
>
> The positive value of the end-to-end argument is that it preserves the flexibility of the network to adapt to both new unanticipated uses, and new unanticipated implementation technology.

In a world where we may end up with one, two, or at most three broadband telecommunications providers in any given community, the end-to-end principle is in serious jeopardy. Should giant telecommunications companies—namely cable and local phone providers—have vertical control over everything from the data transport to the content itself? For example, as I was writing this book, Comcast, the cable monopoly in my area, was trying to buy Disney. The attempt failed. If this happened, Comcast could have decided to deliver Disney's content online more quickly than someone else's, discriminating on the basis of financial considerations. Such a regime would have been a disaster for the unimpeded flow of information. We should insist on a more horizontal system, in which the owner of the pipe is obliged to provide interconnections to competing services. Unfortunately, today's regulatory and political power brokers lean in the wrong direction.

In 2003, the cable and phone companies insisted that they needed vertical control. Otherwise, they threatened, they wouldn't provide broadband data connections to U.S. households. They persuaded the Federal Communications Commission's chairman, Michael Powell, and a majority of his colleagues, that their stand was correct. The FCC gave U.S. regional phone companies the right to control access to any new high-speed data pipes they built, even though they were told they had to keep sharing, for the time being, their copper lines.

This policy essentially mirrored earlier rules allowing the cable companies, which also created networks by getting government-granted monopolies, to refuse to share access to their lines.[307]

The cable and phone companies have shown again and again that they abuse their power. They are historical monopolies with control over vast territories given to them by governments. But they used to be regulated monopolies. Increasingly, they are freeing themselves of regulation.

The big telecom carriers, which have been too slow to actually build out their own broadband infrastructures, don't like it when others use their tactics. State and local governments can and should be building their own fiber networks, as some already have done, such as in Ashland, Oregon. Unsurprisingly, the phone and cable companies have been lobbying state legislatures to forbid this practice, and in several states it's now illegal for municipalities to be Internet service providers.

In a few years, barring major inroads by wireless competition, U.S. high-speed data access could be largely under the thumb of two of the most anticompetitive industries around: the cable and phone monopolies. I doubt they'd dare to stamp out speech they don't like. But they could turn their systems into what industry people call "walled gardens," where the content they provide receives preferential treatment and where they discriminate against material they don't control; my Comcast-Disney example hasn't occurred yet, but the concept isn't idle speculation.

Cisco Systems, the company that sells the equipment used to direct Internet traffic around the Internet, is happily offering telecommunications companies the tools to create these walled gardens. Shamefully, the earliest use of this technology has been by dictatorships, with which Cisco and a host of other big tech firms, including Nortel and Microsoft, have cooperated. According to Amnesty International, the technology is used to firewall their citizens from certain content. The companies denied the implications, saying they weren't responsible for how customers used what they sold.[308]

Even without overt discrimination, market power distorts choices. SBC Communications, one of America's biggest telecommunications companies, has a partnership with Yahoo! for customers who sign up for DSL connections. Yahoo! content receives preferred placement on subscribers' homepages. Subscribers can change the homepage, but most customers of any product stick with the default.

"It's not an on-off thing," Yale Braunstein, professor in the School of Information Management and Systems at the University of California-Berkeley, told me. "Yes, you'll be able to get to *The New York Times*, but it may be harder to get there."

News-article text will always be a relatively quick download. But when it comes to more advanced information content, video in particular, the telecom providers' opportunities for turning a system to its own advantage are far greater.

This is why Walt Disney Co. signed a little-noticed letter in late 2002 to the FCC, urging the FCC to insist on equal treatment for all Internet services on these increasingly concentrated pipelines.[309] Disney's co-signers included Microsoft and several public-interest groups that are normally not on the side of either of those companies. I've been critical of Disney's intentions in some areas, but here the company is standing for freedom.

The cable-TV industry responded to the letter by noting, accurately, that Microsoft was hypocritical to be decrying the kind of anti-competitive tactics for which it had become notorious over the years. Even hypocrites, however, can be right.

At the moment, the cable giants have an even greater incentive to rig their systems than SBC does. The cable giants own much of the TV programming that flows on their systems and they want to keep it that way. Comcast, now by far the biggest American cable operator, has many ownership interests in content.

Worrying about explicit cross-ownership misses the bigger issue, Braunstein said. If you replace ownership with exclusive contracts such as SBC's deal with Yahoo!, you've achieved the same result.

Big Media's inattention to this issue is at least somewhat understandable. The threat is still more theoretical than real, at least in the United States. People in China, where the government censors Internet content, know firsthand the danger of centralized choke points.

Of course, the mass media, buried in a conflict of interest, is also ignoring the current threat posed by growing ownership concentration. Witness the recent scandalous failure to cover the FCC's media-ownership rules until after the fact. The TV network news shows all but ignored their corporate parents' lobbying to extend media consolidation while the rules were pending. This wouldn't be such a problem if there were lots of data conduits, but there aren't. The answer is to separate content from delivery in such concentrated markets.

The Internet is an infinitely diverse medium. But if you can't find it, or if there are artificial barriers to seeing content on it, diversity means nothing.[310]

RETURN OF THE JEDI USERS

At the annual Consumer Electronics Show in January 2004, Carly Fiorina, the chief executive of Hewlett-Packard, surrounded herself on a Las Vegas stage with some popular entertainers. She, the head of a technology company, then declared an oath of fealty to the copyright industry.

In coming years, HP will be selling consumer electronics such as PC-based home media centers, music players, digital TVs, and more. Fiorina vowed that HP will use every method at its disposal to help copyright holders block unauthorized use of their content. If HP also restricts customers' "fair use" rights—the ability to make personal copies and quote from others' works—I guess that's someone else's problem.

Well, here's my oath: the HP laptop I bought a couple of months ago is the last product I'll buy from the company until it

remembers some of the other principles of its founding and success, such as customer empowerment.

What I'm getting at here is the power of the customer. The problem is that the Microsofts and Intels and HPs think first of their customers in the entertainment industry, and second of their customers in the real world.

I'm also getting at the power of the customer to become politically active. How? Here are three things anyone can and should do:

- Write and call your elected officials, not just in Washington but also in state capitals, because Hollywood and its allies are working at all levels of government to control information.
- Contribute to organizations that defend your rights. The Electronic Frontier Foundation[311] is just one of many that hire lawyers and lobbyists to counter the armies of professionals doing the copyright industry's bidding. Check this book's accompanying web site for a list of organizations and what they do.
- Use your power as a customer. Don't buy from companies that cheat artists and abuse fair use. When you attend a concert of an independent artist, buy her CD there. Again, there are more tips on the web site.

Hackers are coming to the rescue in some respects. I'm not advocating civil disobedience, though I am occasionally in technical violation of the copyright laws (such as when I "rip" a DVD I've just purchased to my computer's hard drive to watch it on a plane).

Technologists are now building "overlay networks"—systems of running encrypted (scrambled) and anonymized data over other networks and then making the data look like normal communications. If they succeed, there will be several effects beyond the obvious threats to copyright holders, a serious issue that I don't deny. But the positive impact would be real, too. Telecommunications carriers won't be able to look inside the data stream and discriminate against certain content. If all

traffic is indistinguishable, notes Doctorow, then the only answer is to pull the plug and shut everything down.

I do encourage people who are creating content to license it under a "Creative Commons" license,[312] which lets you reserve some rights while giving people more freedom to use your material in ways that honor our traditions. This book, for example, is being published under a Creative Commons license that permits people to download it freely from the Internet, but not to sell it (more on this in Chapter 12).

How can we preserve the end-to-endness of the Net in the face of the new monopolists? We could embark on a crash program, funded by taxpayers, to bring broadband to every home and business in America in the same way we built the interstate highways at taxpayer expense.[313] Maybe it should be a build-out of networks using fiber and wireless technologies. Maybe it should be subsidies that allow end users to buy what they want, spurring industry innovation along the way.

We could also build fiber-optic lines (or systems combining fiber and wireless) to everyone, filling in the "last mile"—connecting our homes to the high-speed "backbone" lines linking geographic regions—that has been so underserved. Then let the marketplace provide the content and management of the networks.

At the very least, we must have rules—and yes, that means hard-nosed regulation and enforcement—ensuring that the cable and phone companies cannot discriminate against any content.

A DEREGULATORY RESCUE?

Another wildcard has appeared, and it's the most exciting of all, because we might be able to give the monopolists what they're demanding and still have genuine competition. Why? Because

the FCC may truly be moving toward a rational policy on how to regulate—or, in this case, deregulate—the airwaves.

The FCC Spectrum Policy Task Force[314] is looking for ways to update the regulation of this vital public resource. Since the 1930s, the United States has licensed specific parts of the spectrum—the airwaves that carry radio, TV, cellular calls, police and emergency communications, and more—to government agencies and private companies, based on the principle that spectrum was scarce and we had to apportion a dwindling resource.

This principle is based on old science, according to some of the best thinkers in the field. They say, persuasively, that spectrum is essentially limitless if we use it right—that is, with modern radios and transmitting devices that make yesterday's interference problems go away.

These thinkers may well have persuaded FCC Chairman Michael Powell, who has been disturbingly willing to give the media, cable, and phone companies what they want. What he said in a speech in 2003 shows that he grasps the spectrum issue and the opportunity it may present to spur genuine competition in broadband.

"Modern technology has fundamentally changed the nature and extent of spectrum use," Powell said. "I believe the commission should continuously examine whether there are market or technological solutions that can—in the long run—replace or supplement pure regulatory solutions to interference."[315]

If Powell and his colleagues—and a Congress that tends to bow to the interests of well-financed corporations that have power and want to keep it—enact smart spectrum policy, all the sleazy machinations of the cable and phone monopolies won't matter.

There's plenty of evidence that innovation would explode if the FCC frees up more unlicensed spectrum. Look at what has happened with Wi-Fi, a brand-new technology and resultant industry that went from nothing to widespread deployment in

just a few years using unlicensed spectrum. Or maybe, as I'll discuss shortly, the spectrum is even more open for innovation than most people suspect.

Some in the tech industry understand this well. Even as they hold their noses and support the cable/phone broadband duopoly in the short term, they're also pushing for the emergence of competition from other sources including innovative new wireless technologies. A senior Intel executive told me he loathed the phone and cable companies, but hoped to bypass them entirely in the end.

If the FCC does the right thing with spectrum, while local governments deploy lots of fiber, the phone and cable companies can have their wires because then the monopolists won't have the power to abuse what they own, not when competition has arrived to provide an alternative.

In the long run, we might restore the end-to-end principle through sheer physics.

THE END OF SCARCITY?

What if the scarcity of the airwaves turns out to be an artifact of history and outmoded technology? If scarcity can be overcome, the implications are both exciting and disruptive—we will see a cornucopia of communications that foreshadows woes and opportunities for some of our biggest telecommunications companies. David P. Reed told me that the FCC's fundamental mission is flawed, maybe obsolete.

Reed is no newcomer to the tech scene. He holds a Ph.D. from the Massachusetts Institute of Technology, where he taught computer science and headed the Laboratory for Computer Science's Computer Systems Structure Group. He was chief scientist at Lotus Development and Software Arts, two pioneering software companies, and worked at the now closed Interval Research, the Paul Allen–funded think tank in Palo

Alto. He's been involved in the technical details of the Internet for several decades, and lately has been a consultant, entrepreneur, and researcher.[316]

Simply put, he said, we have to start looking at spectrum as an almost limitless commodity, not a scarce one.

The current regulatory regime that allocates spectrum "is a legal metaphor that does not correspond to physical reality," he told me. Why not? First, he said, the notion of interference has more to do with the equipment we use to send and receive signals than with the physics of radio waves. "Radio waves pass through each other," Reed said. "They do not damage each other."

In the early days of radio, the equipment could easily be confused by overlapping signals. But we can now make devices that can sort out the traffic.

The second way that reality defies the old logic is what happens when you add wireless devices to networks. I won't go into the details of Reed's argument, which you can find on his site, but he contends that you end up with more capacity—the ability to move bits of data around—than when you started.

"In principle, the capacity of a certain bandwidth in a certain physical space increases with the number of transceivers in a given space," he said. Yet the FCC regulates the airwaves as if the capacity was a fixed amount.[317]

Yes, he said, this is counter-intuitive. And, to be sure, there are experts who disagree with him.

But if he and others in his camp are right, we have a lot of work ahead to fix a hopelessly broken regulatory system. And if that happens, the sky is literally the limit for future communications. At the same time, the consequences for some of the most powerful companies in our economy may be grim because they are based on economic scarcity. The value of the big broadcasting companies, for example, has much to do with their government-granted licenses to control specific parts of the airwaves.

Reed wants the FCC to open up some spectrum for the new, more open wireless networks, giving entrepreneurs a new public space in which to innovate and create value for the rest of us. He's not sure who'll make money in this space, but surely, equipment manufacturers and other companies, especially software companies, will be in the middle of a wave of innovation.

Software is a key, perhaps the key, to the future Reed envisions. Most radio-like devices using today's spectrum—radios, televisions, mobile phones, and the like—are based on the old way of doing things, constrained by hardware to receive and transmit signals in specific ways and in specific places.

To get the full multiplier effect, he said, we need devices with fairly generic but powerful hardware components. "Software defined radios" will be vastly more adaptable and useful than their old-fashioned cousins, according to Reed and others who are promoting the concept. The military has been using these devices, called "agile radio," for some time; civilian availability is getting closer as costs come down.

Imagining this new world conjures a boost for a civil liberty we take for granted in America but which has been dampened under the current regulatory scheme. I'm talking about free speech. Regulation of the airwaves has specifically included curbs on speech, such as the FCC's commands to the nation's TV and radio broadcasters about what may or may not be said on the air. That regulation took an ugly turn in the spring of 2004 as the FCC, egged on by an election-year Congress, slammed huge fines on broadcasters in what was surely the most direct attack in years on free speech.

Such restrictions on speech have been justified, in part, under the idea that the spectrum is a public and limited resource. If that is not true, there's no reason to regulate speech in this way. Someday, perhaps, the First Amendment will mean something when people broadcast their views, not just when they put them on paper or on the Internet.

The worst direction for the FCC to move right now, Reed said, is to keep giving or auctioning spectrum to "monopoly owners" that won't use it efficiently. A new kind of open space is all about the public good, he said, and there's a fine analogy in recent history.

"We need to do for spectrum," he said, "what the Internet did for the network."