The Internet and Hieronymus Bosch: Fear, Protection, and Liberty in Cyberspace

Harry R. Lewis

It is trite but true: We are in the middle of an information revolution. News, gossip, entertainment, lies, and propaganda move over huge distances in the blink of an eye. All of it, from the newspapers of record to juvenile cell phone photos, to what you bought at the supermarket last Thursday, is archived for parties unknown to retrieve, who knows when in the future. Electronic communication already reaches the majority of the world's population, and no technological obstacle prevents virtually everyone from having constant access to everything. In parts of the world where connectivity is lagging because cables are few and electricity is scarce, mobile communication is growing exponentially (see, for example, the statistics of the International Telecommunications Union at http://www.itu.int/ITU-D/ict/statistics/ict/). If the world is not fully connected in twenty-five years, it will not be for want of technology or money, but because of politics.

The question before this human generation is how the power of information ubiquity will be used and how it will be controlled. The societies of the world are struggling with the social dilemmas posed by the rapidly evolving technologies. Conveniences that teenagers take for granted—for example, taking photographs anywhere and sending them instantaneously to anyone on earth—neither science fiction writers nor engineers quite foresaw. Nor are such innovations socially inevitable, even when widely disseminated, as Iranians discovered in the summer of 2009 when they tried to send images of postelection uprisings out of the country. Such citizen journalism was simply banned, with heavy penalties imposed on transgressors. With every communications invention comes questions of both exploitation and control.

The Cycle of Invention and Control

The revolution is enlightening, empowering, and alarming. Technologically, it is easier to speak and it is easier to listen than ever before; easier to share knowledge and to gain knowledge; and easier to find and communicate with others who share the same interests. But potentiality is not the same as reality. And the same technologies are as easily used to spread misinformation, defamation, and terror.

Societies respond to what they consider threats. They may try to prevent production of information, to throttle its source, to block its receipt, or to filter it out of the communications network in transit. Any response may regulate much more than the original threat. Overreactions have unintended consequences and are sometimes scaled back; malefactors bypass the regulations, creating incentives to expand them further. By the time a measure of social stability has evolved, other new technologies give birth to unanticipated problems.

This schema of invention and control plays out in widely disparate domains. It frames the story of political censorship in totalitarian countries, the story of uncensored blogging in the United States, the story of age restrictions on Myspace, and the story of music downloading in college dormitory rooms. It is even the story of U.S. government censorship of broadcast television, an old American story given new life by changes in broadcast technology. In fact, as we shall see, it is as old as the most ancient myths of human origin.

The cycle of invention, opportunity, threat, alarm, response, and reaction plays out differently in different societies, but the societies interact with each other, creating more uncertainty and confusion. And so we have anonymous Internet routing that enables Iranian dissidents to view the Internet as it looks in free societies, and so we have self-censorship by U.S. publishers whose Web sites are visible in countries with less forgiving defamation laws.

Politics, Person, and Property

However information is produced and communicated, societies take an interest in exploiting and controlling it in three domains: politics, personhood, and property. For example, the political domain includes democratic participation using mobile phones and the Internet on the one hand, and cyberterrorism and the arrest of dissident bloggers on the other. The personal domain includes the vast opportunities of social networking on the one hand, and the threats to the safety of networked children on the other. Property exploitation and control involve, most famously, the complex relation between the music industry and music fans, whose intercourse as producers, consumers, and "pirates" of recorded music is now entirely digital.

These three domains share digital tools and techniques. The power to detect and censor political dissidents can as easily be exploited to detect and prosecute those improperly distributing copyrighted movies. Once a form of technological control has been invented and deployed, it can be redirected, exported, or adapted.

Claims to the effect that the Internet is making us dumber, or is causing unheard-of levels of sex crimes, should be greeted skeptically. Digital technologies are tools, intrinsically no more dangerous than a book with blank pages. And yet something is different and consequential about the social impact of digital technologies. They are at once the most effective methods of disseminating information ever invented and the best technologies for restricting and monitoring its flow. The digital world is all about control.

The social dilemma at the core of the information revolution is whether it will prove to be liberating or limiting. As we experience it in midstream today, it is to some degree both, for most of us. We can look up baseball statistics at the ballpark and connect to old friends in ways never before possible. We can read Supreme Court decisions day and night without going to the library, and millions of

people can hear today an amazing vocal performance that was recorded only yesterday. Yet we fear that casual disclosure of a few digits of information about ourselves will result in our life savings disappearing to Eastern Europe, or that bad people loitering on the information superhighway will take advantage of our elderly or juvenile relatives. We fear that corporations and governments alike will mindlessly aggregate data about the most important and the most trivial activities of our lives—and will then misuse that information or let it slip into hands we wish did not have it.

Information and Power

Humankind has long experience coping with information flows. For as long as people have been telling things to one another, other people have been trying to control who hears what. Some twenty-five centuries ago, Socrates argued that young people are particularly impressionable and should be shielded from corrupting influences. "The first thing," says Socrates in Plato's *Republic* (1888), "will be to establish a censorship of the writers of fiction, and let the censors receive any tale of fiction which is good, and reject the bad." Suppressing fiction was not enough, he opined—sometimes you have to suppress the truth too. "The doings of Cronus, and the sufferings which in turn his son inflicted upon him, even if they were true, ought certainly not to be lightly told to young and thoughtless persons; if possible, they had better be buried in silence." (The Golden-Age god Cronus ate his infant children, knowing one was destined to overthrow him—but the youngest child, Zeus, was hidden away by his mother and survived to gain dominion over his father. Not a family dynamic, apparently, for Greek boys to use as a model.)

Today's revolution is also about the spreading of stories—and not just stories but anything expressible. The revolution is astonishing when we notice it, but often we do not see it happening, because it manifests

in mundane things like shopping and gossiping, not headline events such as wars, flu epidemics, and space flights. (And infanticides.)

Commercial interests tend to highlight our convenience and downplay our vulnerability. Cell phone companies do not advertise that they keep copies of our address books and our family photos, which can be subpoenaed when we are hauled into court. We do not think about that even when we lose our phone and are thrilled to find all our data magically restored on the replacement unit.

What drives the revolution is not politics or ideas. The information revolution has its gurus, but no inspirational spokesman could have led this revolution. Inventions caused the explosion: the cell phone, the Internet, the digital camera, the personal computer—and behind them all, semiconductors and integrated circuits and fiber optic cables. It is a disruptive and even destructive technological revolution in the commerce of ideas, knowledge, and thought. Nothing could be more defining of this age of human civilization than how we utilize our new power over those insubstantial products of the human mind—words and images, fantasies and facts. Our descendants will judge us on what decisions we made, and what we allowed others to make for us, about how these technologies would be put to use.

Like many other technological histories, this one is a tale of power shifts: technology empowers those who control it and weakens others. Military technologies, such as the saddle, the gun, and the atomic bomb, were decisive in wars waged before these inventions escaped the exclusive control of their possessors and, for better or worse, leveled the global playing field. Technologies of building construction, locomotion, and food production have all for a time given nations economic advantages over their competitors and control over the welfare of their people. Can the new technologies of insubstantial zeroes and ones really have such dramatic impact on society?

In fact, technologies of information have always precipitated power grabs. Gutenberg started printing books using movable type shortly

after 1450—at first just the Bible and perhaps a few grammars. But within fifty years the Catholic Church was burning heretical printed works that were falling into the hands of the faithful. After a century the problem of disapproved books became so serious that the technology was put to work against itself. In 1559 the Church printed the *Index Librorum Prohibitorum,* a book listing all the prohibited books—including the works of Kepler and other scientific tracts that ultimately would dislodge man from the center of the universe and the Church itself from its authority over human minds. The lists of books that should not exist were reissued periodically until 1966, when Pope Paul VI decided that the list itself should no longer exist—a nicely recursive end to five centuries of technologically enabled suppression of technologically enabled information flows.

Liberty, Protection, and Control

So today's struggles over the spread of information are not new in kind, only in degree. As in the past, the key dialectic in the struggle for control of information is between fear and liberty, between protection and control. The spread of information is dangerous, so the technology that spreads it must be regulated. The regulations require human judgment to administer, and those judgments may be colored by incentives to control thought, not merely to protect the vulnerable.

Information regulation requires that someone decide for other people what information they should have. To the extent we believe that human beings can and should decide for themselves what to do with the information that is available to them, any regulation of information is a threat to human liberty. To the extent that information liberty is a precondition to human empowerment, any regulation of information is inimical to social progress.

Plato's censors and the Church's imprimaturs were ultimately ineffective controls over ideas. But with everything reduced to bits, the

digital controls are at once more universal and more varied. We see examples every day:

- The Chinese government fears that its citizens will get "wrong" information about Tibet and the Uighurs, so it controls what Web sites are accessible inside China, even attempting to enforce installation of "Green Dam" censoring and tracking software on every computer sold in China. Many other countries have their own Web censorship practices. Little sexual content is available in Saudi Arabia. (For detailed information on Internet censorship worldwide, see the site of the OpenNet Initiative, http://opennet.net/.) The new Iraqi democracy is planning to impose some of the censorship that was lifted after the fall of the regime of Saddam Hussein and to force Internet cafés to register and be monitored. A government minister explains, "We are living in such a dangerous time that we need to control things" (Williams 2009).
- Though politics and sex are the usual reasons for government censorship, once the technology is available it can be retargeted in an instant for other purposes. During the summer of 2009 the Chinese government, embarrassed by a scandal involving dealings of a Chinese company with the government of the African nation of Namibia, ordered that Chinese search engines return no results in response to searches for "Namibia." For those in China who rely on the Web for information about the world, Namibia simply ceased to exist (Heacock 2009).
- Parents, fearing that their children will use the Internet to talk to pedophiles, install monitoring software that enables them to monitor their children's activities and even be notified if their children wander into prohibited regions of cyberspace. The states' attorneys general have instructed the industry to come up with better child protection tools, threatening legal requirements in the absence of voluntary action (Medina 2007).

✳ The recording and movie industries fear that the Internet's capacity to make and distribute copies of digital audio and video files will hurt their profits, and have induced Congress to enact copyright statutes with strict rules and severe sanctions, of which the industries themselves are the enforcers. The policing tools are digital, of course; when teenagers persist in music sharing, the industries lobby for stronger regulations, requiring large-scale monitoring of data flows through the heart of the Internet. For example, in 2010 France passed a "three strikes" law that denies Internet access to users who repeatedly download copyrighted works. "When you violate driving laws, your car is taken away," a French official analogized (Lankarani 2009). This analogy is seductive—why shouldn't transporting bits be regulated like transporting atoms?—but disingenuous. Driving is a public activity that poses an immediate threat of physical harm. Drivers expect to be monitored, not only by the police but by other drivers, whose safety is jeopardized by reckless driving. Accessing the Internet, at least from one's own home, is a private transport of words and ideas, akin to talking on the telephone rather than driving. Monitoring Internet communications is like wiretapping. In the early days of telephony, warrantless wiretapping was legal. The U.S. Supreme Court ruled in 1928 that if someone installs a telephone, "The reasonable view is that . . . the wires beyond his house and messages while passing over them are not within the protection of the Fourth Amendment" (*Olmstead v. U.S.* 1928). By 1967, the telephone was recognized as an essential vehicle for private speech and the Court (in its decision in *Katz v. U.S.*) reversed the default—the government cannot listen in without a warrant. The practice of Internet monitoring, along the lines desired by the music and movie industries and codified by the French "three strikes" law, resembles the presumptions of early telephony. Internet service providers are allowed, and even expected, to monitor all network activity on the chance that

someone is violating some law—even a civil statute such as that prohibiting downloads of copyrighted music. It is as though Federal Express were required to check all packages it delivers for unauthorized music CDs. Monitoring the Internet is monitoring the world of thoughts and ideas and words—some may be illegal, but in an enlightened democracy, the government should show specific grounds for suspicion before monitoring any individual's communications.

- Apple, fearing that Google will gain a competitive head start in the market for consumer control of telephone calls, removed the digital imprimatur it had previously granted to the Google Voice application for the Apple iPhone. Because iPhone apps are "tethered," Apple can unilaterally remove them, without the cooperation of the iPhone owner.
- Apple also uses its control over iPhone software to censor a dictionary. Citing its policy against obscene or pornographic material, Apple refused to allow the Ninjawords dictionary app onto the iPhone until words such as "shit" and "fuck," which appear in virtually every dictionary of the English language, were removed (Gruber 2009).
- Amazon, upon discovering that it sold certain books to Kindle owners without proper authority from the copyright holder, removed the books from the Kindles, issuing refunds. Surprised owners discovered that they never really owned the books in the first place; their Kindles are tethered to Amazon (Stone 2009a). The precedent having been established, Kindle owners wonder whether Amazon might reach into their homes to remove books for other reasons—say a claim that the book is unlawfully obscene or perhaps merely unkind to Amazon founder Jeff Bezos.

Bits Reductionism

The prospect of books mysteriously disappearing from Kindles has a nightmarish resemblance to the medieval bonfires of the vanities. But the new information control mechanisms are distinguished from the old by bits reductionism, the simple idea that "it's all just bits"—anything that can be expressed, can be expressed as a series of zeroes and ones. Once content is reduced to bits, there are no more photographs and recipes, pornographic movies and Skype telephone calls, novels and accounts payable. There are just sequences of bits. Any possibility of moving or storing or making a million copies of one sequence of bits is a possibility for any other sequence of bits. And any control that can be exerted over one sequence could be exerted over any other.

The technological revolution in the commerce of ideas is merely a special case in the commerce of bits. Technologically, all distinctions between ideas and any other kind of expression have been obliterated. Bits reductionism has given birth to media convergence. The engineering of radio, telephone, and computer communications is now the same. Movies flow over the Internet, the Internet flows over the cellular telephone network, and Grandma's telephone calls flow into the home through the same digital pipes that bring Oprah Winfrey's television shows.

The dual forces of bits reductionism and media convergence make it possible to collapse all forms of regulation. To regulate the flow of ideas one must regulate the flow of bits, and while regulating the flow of bits the flow of other forms of expression can be regulated as a side effect. The antipiracy filters being deployed in France are functionally similar to antipornography filters being deployed in Australia; once deployed for one purpose, the filtering technology can readily be expanded to serve another.

So where the flow of ideas is free, the flow of every form of expression is free. Where the flow of verbal or pictorial trash is regulated, the flow of ideas can also be regulated collaterally.

These convergent and overlapping and collapsing effects of bits reductionism explain why the digital revolution defies analysis into the classical social categories. For Plato a story was a story; perhaps true and perhaps false, but it was not his medical history or grocery list or lute music. There was no way for a medieval pope to put offending private mail on the *Index Librorum Prohibitorum*. With all forms of communication now flowing through the same network, it takes only a software tweak to retarget censorship or monitoring technologies. The old dilemmas about censorship, about mind protection versus mind control, are now convoluted with issues of privacy, creativity, expressiveness, entertainment, business management, education, socialization, reputation, and the very essence of personal identity. Interference with the flow of bits to fix a problem in one area is likely to have an effect in another.

Consider the story of the infamous Lori Drew, the Missouri woman who used a Myspace account to impersonate a nonexistent teenage boy named Josh. Megan Meier, a teenage girl, was distressed by Josh's taunts and committed suicide. No Missouri statute was applicable, but a federal prosecutor successfully brought charges against Drew under a statute enacted to criminalize cyberattacks on the computers of banks and credit card companies. The judge set the verdict aside, reasoning correctly that the prosecutor's legal theory would make almost everyone a criminal; even fibbing about one's age on a Web site (as Megan Meier herself had done) would become a federal crime.

The Lori Drew tale illustrates at least three forms of convergence: an Internet invention created to enhance social connectivity becomes a tool of identity fraud, exciting a demand for regulation (a new Missouri law might have been applicable in the Drew case if had been enacted earlier); the Computer Fraud and Abuse Act (CFAA), originally enacted to fight interstate monetary fraud, is applied to a social communication between neighbors because the computer they were using was in another state; and the CFAA itself was necessary because the Internet, never designed for secure communication, rapidly became a critical tool of world finance.

Or consider the curiously important question of whether, the First Amendment notwithstanding, the U.S. government can prohibit Nicole Richie from saying "shit" on television. The Supreme Court decided yes, in a 5–4 vote along conservative-liberal lines (*FCC v. Fox Television* 2009). The matter was narrowly decided on a question of administrative process; on its face, the issue had nothing to do with the digital revolution. But Justice Thomas, who voted with the majority and is surely among the most socially conservative members of the court, wrote his own opinion. He noted that communications technology was so much more abundant than it had been in the 1930s, when the Court affirmed the FCC's authority to censor broadcasting, that the old rationale for this exception to the First Amendment—that the electromagnetic spectrum was a scarce resource that Congress had the right to nationalize—might have to be revisited. Thomas signaled that, if a similar case came back on free speech grounds, he might flip his vote.

Internet Universalism

The Internet was designed to be ubiquitous and placeless, both hard to control and highly resilient. Though the scale of the network is vastly greater than its designers conceived, their design goals have largely been achieved. Governments have a hard time keeping disapproved material away from their citizens, and natural catastrophes such as Hurricane Katrina and the December 26, 2006 earthquake in the South China Sea leave the network as a whole running fine. Even more importantly, the Internet was not designed to carry phone calls, MP3s, or email. It was just designed to carry bits and, by extension, anything that could be expressed in bits, which means anything that can be expressed. As the Information Sciences Institute (1981) states,

> The internet protocol is specifically limited in scope to provide the functions necessary to deliver a package of bits (an internet datagram) from a source to a destination over an interconnected system

-1—
0—
+1—

> of networks. There are no mechanisms to augment end-to-end data reliability, flow control, sequencing, or other services commonly found in host-to-host protocols.

That passage comes from an Internet design document. It says, essentially, that you can make this network do lots of things; we have not even bothered to think what they might be. What we are giving you is a set of basic tools and raw materials for communications between computers; go use your imagination. If reliable or smooth or secret communication is important to you, those things may be possible, but it is your job to figure out how to achieve them. All we can tell you is that anybody, anywhere in the world, using any kind of computer, who follows these rules and gets connected to another computer on the Internet will inherit all those unforeseen inventions that you build on top.

The Internet was born in a spirit of innocent—perhaps naive—fearlessness. And that is how the Internet, whose earliest uses were dull things such as sharing printers among mainframe computers and sharing software between engineering groups, came to be the engine of Wikipedia and Facebook and Skype and online banking, and also amateur pornography and international money laundering.

So the Internet facilitates the dissemination of dangerous information, because of its inherent lack of moral direction. It is, like a knife, simply a tool, which can be used for good or evil.

Dangerous and Enlightening Knowledge

How do we cope with dangerous knowledge, with knowledge that can be harmful? That is an old question, but not merely an old question. It is perhaps still the ultimate question about the human condition. It is the question we have been asking ourselves since the fateful day the serpent told Eve about the tree in the middle of the garden, and told her that God had a particular reason for warning her about that particular tree: "When you eat of it your eyes will be opened, and you will

be like God." Eve reckoned that "the tree was to be desired to make one wise," ate the fruit, and shared it with Adam—at which point God threw them both out of the garden, pausing only to clothe them and to issue a few curses.

Full knowledge is, in many religious traditions, dangerous.

Of course it is also what makes us joyful, and thoughtful, and wise, and inventive. Our capacity to build new and more advanced cultures on top of the accumulated knowledge of the past is distinctively human (notwithstanding the limited forms of cultural transmission that have been observed in animal societies).

The progressive force of knowledge has, as a long tradition in human self-understanding, an association with evil and sin. In fact, our human burden lies in our freedom to master the use of what we know. In Greek mythology, Prometheus, like Adam and Eve, endured a severe punishment for seeking divine knowledge. Prometheus stole fire from Zeus, and with it all the other useful arts of civilization. The price Prometheus paid was to be chained to a rock and to have his liver gnawed at by an eagle, but humankind got its own punishment: Zeus sent Pandora (the first woman) to tempt Prometheus's brother, and when she succumbed to her curiosity and opened her famous box, ills and ailments escaped, afflicting us to this day. (Only Hope remained behind.) Still, Prometheus is remembered not only as the original dangerous technologist but also as the progenitor of the human race; to the Greeks we are actually defined by our curiosity and noble creativity.

To an idealist about the future of humanity, progress is measured by capacity to use knowledge to improve human life. The optimistic view of the effect of universal learning was articulated and revered in the eighteenth-century Enlightenment as never before. Confidence in the power of learning, if only individuals could have access to it, nourished the antiauthoritarian political morality that justified the American Revolution. It is no accident that Benjamin Franklin was both inventor and diplomat, or that Thomas Jefferson was both a visionary polymath and an inspired political revolutionary.

Political freedom has been, from the founding of the American republic, of a piece with information freedom. Self-determination requires the freedom to speak and the freedom to learn, which are characteristic of the natural state of human existence.

Jefferson in particular was prescient on the peculiarities of ideas and information and knowledge, how hard they are to control. He wrote, in an 1813 letter to Isaac McPherson,

> If nature has made any one thing less susceptible than all others of exclusive property, it is the action of the thinking power called an idea, which an individual may exclusively possess as long as he keeps it to himself; but the moment it is divulged, it forces itself into the possession of every one, and the receiver cannot dispossess himself of it. Its peculiar character, too, is that no one possesses the less, because every other possesses the whole of it. He who receives an idea from me, receives instruction himself without lessening mine; as he who lights his taper at mine, receives light without darkening me. That ideas should freely spread from one to another over the globe, for the moral and mutual instruction of man, and improvement of his condition, seems to have been peculiarly and benevolently designed by nature, when she made them, like fire, expansible over all space, without lessening their density in any point, and like the air in which we breathe, move, and have our physical being, incapable of confinement or exclusive appropriation.

If Jefferson saw a downside to the explosive spread of ideas across the globe, he did not mention it here. The conflagration would contribute to the "moral and mutual instruction of man," period. The more people know, the better. Ideas spread naturally and cannot be fenced in. And nature has benevolently provided that you do not lose your ideas when others get them; enlightenment simply spreads without cost to you.

Until recently, the economics of information transfer kept Jefferson's dream in the realm of imagination. To paraphrase John Perry Barlow (1993), you could not get the wine without paying for the

bottle—to learn something you had to buy a physical object, a book or a newspaper or a magazine, and publishing cost money. The economics have been radically changed by Moore's law—the exponential growth in computing and storage capacity of silicon chips—and by corresponding improvements in rotating storage. Digital technologies have made possible previously unimaginable decreases in the cost of information storage and communication. The Internet is the realization of Jefferson's dream: the marginal cost of reproduction and transmission are plummeting toward nil.

Yet universal enlightenment hardly seems to be at hand. What stands in the way? Broadband access is far from universal, but that is not the problem—the rule of reason seems not to have triumphed even in zip codes with good Internet service. What has gone wrong?

A technology of liberation has evolved into a technology of control for two related reasons.

The first reason is commercial. Because information (for example, in the form of digital songs and movies) is valuable, the network and the laws that govern it are structured so that information can be monetized. Advertising pays for Internet services we too readily consider free, such as search engines and news services, so the network and the laws that govern it are designed to make advertising effective. With the emergence of commercial information monopolies, or near-monopolies, comes the possibility that the new information universe will become more limited rather than more open.

Amazon's withdrawal of Orwell's *1984* from customers' Kindles (see Fowler 2009) was a creepy event but not a dangerous one, given the continued existence of print copies. But suppose that readers become dependent on Google's vast digital book library and Google, under some future corporate leadership, were to selectively prune its collection for reasons of politics or religion or taste. Or suppose, after the merger of an information carrier such as Comcast with a content provider such as NBC Universal (see Kahn 2010), that competing media no longer flow readily to the carrier's customers. There is no more

reason to expect information corporations to act as public servants than there would be to expect an unregulated supplier of oil or electricity always to act in the public interest.

There is a remarkable historical precedent for concern over "network neutrality," as the principle of separation of content and carrier has come to be known. Here is an excerpt from an article titled "The Telegraph Monopoly" from the February 9, 1884, edition of the *New York Times,* reporting testimony before the U.S. Congress in 1884, describing what happened because of the Western Union monopoly on telegraphy:

> A few years ago a man started a news bureau in Cincinnati. A correspondent in New-York [*sic*] filed the market reports each morning and the Cincinnati gentleman sold the information to customers. The Western Union asked him to sell out to them and he refused; thereupon his messages were taken away from the "through" wire and sent by a "way" wire. The difference in time was an hour, and the man was ruined. . . . The Western Union . . . controlled the market prices, all the political and general news sent over its wires—every single important personal communication sent in the country.

The second justification for control of information technologies is the protection of personal security—of individuals and of nations. From the desire to catch the bad guys before they do anything comes the inclination to control any technology used to do ill, and information technologies in particular. Examples include the UAE's demand that BlackBerry communications be open for government inspection since antigovernment forces might conspire using encrypted communications (Meier and Worth 2010) and India's proposal to ban Google Earth because the Mumbai terrorists had used it to plan their attack (Blakely 2008). In both these cases, as in many others, fear of the novel clouds the issue. Bad guys use not only BlackBerry phones and Google Earth, but cars and boats, which no one would consider banning. The cost of banning or heavily controlling the new technologies is not as

apparent, but every premature restriction on technology leaves many inventive uses stillborn.

The information technologies for protecting commerce and protecting people have a lot in common. In both cases the crucial tools are automatic monitors that watch for patterns of bits in information flows. The result is an unholy alliance between governments and content companies (owners and distributors of copyrighted works). After all, if Internet service providers (ISPs) were required to watch for pirated movies to protect the nation's intellectual property industry, how could any reasonable person argue against using the same monitoring tools to prevent another 9/11?

Internet Fear

The possibility of artificial scarcity for commercial advantage should not blind us to a deeper and more primitive risk to information freedom. Fears, some old and some new, have arisen along with the hopes for the new information technologies; and the reactions to the fears are smothering the liberating forces. Let's look at a few of these fears.

- Jefferson's image of ideas expanding like fire over all space sounds very much like the recording industry's nightmare of a single digital copy of a song going to the laptops of a million teenagers by means of an Internet file-sharing service. The passing into consumer hands of the means of digital reproduction has sparked a remarkable escalation in negative imagery: "theft," "piracy," and so on. And not just imagery but legislation, and even regulation of the manufacture of equipment—attempts to make copying of copyrighted material not just illegal but impossible, no matter what the collateral damage.
- Ancient fears that the morals of youth will be corrupted by what they hear or read have come back to life with new vigor in the Internet era. The U.S. Congress tried to outlaw the display of

"indecent" (though not legally obscene) material to children over the Internet. The law was overturned on constitutional grounds, but similar censorship occurs routinely in other countries, even enlightened democracies acting to protect the morals of adults. Australia is currently testing a national blacklist of sites to be blocked to protect the public morality ("Australia to Implement" 2008).

- Fear that children will associate online with bad people has led to tracking and monitoring requirements and to a market in "nanny software" to make parents aware of their children's wanderings through cyberspace. Of course, the same technologies that can control personal computer use by American children can be directed at monitoring the activities of citizens of totalitarian regimes—or even in the United States, where the Defense Department's Total Information Awareness program was killed only when Congress became aware of its potential as a program of civilian surveillance.
- Even as Google, Amazon, and Facebook accumulate vast amounts of personal information about their users, badly aimed privacy protection legislation threatens to undercut the Web's usefulness. Requirements that children be at least thirteen years old to get accounts on social networking sites have done little to protect children's privacy but have done much, often with parental support, to teach them to lie about their age (boyd et al. 2010).

The Internet was conceived in the defense world, designed by academic and industrial research engineers, and transported into the commercial world only after its core design had been widely deployed. Engineers are naturally libertarian. Whether they are designing cars or computer networks, their ideals are utility, speed, and flexibility. Software engineers are spared the ethical issues that confront the designers of munitions; engineering in the world of zeroes and ones

inherits the nonnormative, amoral quality of mathematics. Even cost, safety, and secrecy are imposed by market forces and governments, which had little force in the Internet's gestation period. So there was a Garden of Eden quality to the Internet in its preconsumer days: a combination of fecundity and innocence. The network fostered experimentation and innovation, and little worry about the potential for mischief or evil.

The Garden of Earthly Delights

So we are back to the story of human creation and how we handle the knowledge of our own undiscovered capabilities. The biblical story is usually reduced to its simple outlines: a rather chaste paradise at first, then temptation and knowledge of good and evil, then shame and expulsion, followed by redemptive suffering and labor. But there is one artistic rendering of the biblical myth that interpolates a remarkable middle period. It is called *The Garden of Earthly Delights,* and it was painted in the Netherlands by Hieronymus Bosch around 1503—as it happens, just about the time the Church started taking action against heretical books (see Plate 1).

The Garden of Earthly Delights is a triptych, a central panel flanked by two smaller ones, the sort of painting that was often used as a church altarpiece. But it is hard to imagine this set of paintings in a church, despite its biblical theme. On the left is the Garden of Eden, complete with peaceful, happy animals, and a rather insignificant-looking God introducing Eve to a slightly leering Adam. On the right, under a burning cityscape and a blackened sky, is hell, full of people undergoing various forms of torture at the hands of demonic animals. The conception of hell is bizarre, but at least we can recognize what it is. But the central panel corresponds to nothing in the Bible and earns the triptych its name. It shows a frenzy of people engaged in all sorts of naughty things, none requiring clothing. Some of the groups are

multiracial, and quite a few animals and fruits are enjoying the fun too. Nobody seems to have the slightest hesitation about their cavorting or their nakedness.

This scene is a wonderful mystery—extravagantly detailed and amenable to hours or decades of study. If it were painted today, the art critics would investigate the painter's recreational drug use. There is no tradition of similar scenes by other artists, so its symbolism cannot readily be connected to better-understood analogues.

And so we are left with two possible explanations, without any middle ground. Perhaps it is a depiction of sin relating directly to the third panel's punishments: "If you do that, here is what is going to happen to you." Or else it shows some long-ago, libertine earthly paradise. The didactic interpretation, that the whole is intended as a warning, is more historically plausible; there are plenty of wages-of-sin themes in Christian narratives. And yet . . . if the objective were to warn people off from sinful activities, the artist seems to be going to extremes to document in pornographic detail the fun that will get people in trouble. And if the participants themselves are supposed to be aware that this orgy is not going to end well for them, the warnings are very muted. Based on the evidence from the panel itself, they could reasonably claim that they had no idea that what they were doing was wrong. It all looks fine—nobody is getting hurt and everybody is having a good time.

The lost-paradise interpretation has its own problems—mainly that there is no such biblical story. (Unless it is a wild extrapolation of what the Bible says about earth on the eve of the flood, when God decided to pretty much start over from scratch.) Yet, to my inexpert eye, the "earthly delights" interpretation is more plausible. The central panel simply seems more in the spirit of the paradise panel on the left than of the hell panel on the right.

Internet Liberty and Libertinism

The Internet became a garden of earthly delights when it was opened to consumer-oriented, commercial uses. It is now transitioning out of its earthly delights period, as society decides how to adjust to its potential use for sins and evils, as various cultures define them—not just pornography, of course (though that to be sure), but anonymous hate speech, privacy intrusions, political insurrection, and simple theft and character assassination.

We have seen technologically induced liberation movements before—or to be precise, I have seen one before. The sexual revolution of the 1960s was in no small measure the result of birth control technology. Reproductive control was not a new concept, any more than free speech was a new concept when the Internet engineers sat down to work. But the very sudden, widespread availability of birth control pills in particular was enormously empowering; the development of a class of professional women would have been much harder without it. This revolution was also accompanied by a period of chaotic experimentation—musical, social, pharmacological, and political as well as sexual. When I look at *The Garden of Earthly Delights,* I think of Woodstock.

We are today being overtaken by the Internet fear, fear of consequences. We are past the point of Bosch's middle panel, but just barely; even young adults remember when the Internet was not scary. Nonetheless, we are now threatened with the horrors depicted in Bosch's third panel, and in fact the alarms over personal debasement and the public shaming echo the humiliations of Bosch's hell.

We are past the point of innocence, and moralists and governments and law enforcement urge us to expect information nightmares if we do not get the communications revolution under control. Ironically, Bosch depicts the horrors of hell as effected by technological instruments of pleasure—musical instruments, to be precise. One man is strung up on a harp, another is sucked into a horn, a third is bound to

a lute. Only in the third panel does civilization appear, and only to be destroyed by its own devices. In the same way, the forces of fear are threatening us with torture by Facebook, character assassination by RateMyProfessors.com, terrorism by Google Earth, pillage by Kazaa.

We must, we are told, protect ourselves, our children, and our society from technologically enabled evils. And thus we have a variety of laws and regulations, proposed and enacted, fed by fear and aimed at restraining evils—be they political, personal, or commercial.

- Censorship: It is hard to censor the Internet, because of its diffuse, decentralized architecture. But it is easier to censor content from an entire nation than, for example, to allow content to reach adults but not children. China, where Internet use is very widespread, has a robust censorship regime, aimed at controlling access to both sexual and political content (Deibert et al. 2008, 2010). But the United States has its own censorship forces at work: The Communications Decency Act and the Child Online Protection Act both limited speech among adults—in ways the Supreme Court ultimately found unconstitutional—as a byproduct of their efforts to protect children.
- Piracy: In just a few years the Internet has radically altered many business models that functioned well for decades. Travel agencies and newspapers are both casualties of the electronic decentralization of information. But no industry has been protected by legislation the way the recording industry has been—not that the protections have been very effective. Armed with effective lobbying, the Recording Industry Association of America (RIAA) effected the passage of the Digital Millennium Copyright Act, which imposes severe financial penalties for copying digital music files. The act is unprecedented in the size of the fines, the use of a strict liability standard, and the assignment to the RIAA itself of responsibility for policing its violations. As a result, cases almost never come to trial—instead, defendants pay up without a fight,

fearing larger penalties if the cases are tried. The strictness of the standard is not only frustrating to the consuming public but injurious to creativity—the very thing that copyright is intended to enhance. The U.S. Constitution says nothing about protecting profits or business models—only about the intent "to promote the progress of science and the useful arts."

- The preferred solution for the recording industry is cooperation from ISPs—cooperation in the form of surveillance of what is flowing through the network, with violations punishable by denial of Internet service to the guilty party. Pressure for such practices is being put on universities, which have captive audiences—students do not get to choose who supplies the bits to their dormitory rooms. This makes as much sense as asking universities to open all packages coming through the postal mail to students in search of pirated CDs. In the United States, about as basic a principle as we have is that there should be specific reasons to believe that individuals are involved in illegal activities before monitoring their communications. And yet the Motion Picture Association of America wants Congress to encourage ISPs to filter Internet content (Kravets 2009) and to sign a treaty that would establish such filtering as a matter of international obligation (Glickman 2009).
- Child safety: The difficulty of reliable identity verification on the Internet has combined with a handful of *Dateline*-style child abduction horror stories to give rise to legislative proposals in the United States for measures to limit adult-child contact. The most developed of these proposals is the Deleting Online Predators Act, originally introduced in 2006 but never enacted into law. It would require school libraries receiving federal funds to disable social networking sites unless an adult was monitoring and supervising their use. Though very popular when voted on in the House during a midterm election campaign, it would have been largely ineffective, since children have so many other points of access to

Myspace and Facebook, including their cell phones as well as computers at Starbucks and at home.

- As in the case of copyright law, the U.S. government has delegated to a nongovernmental entity the job of enforcing certain child safety laws. The official list of "child pornography" Web sites is the province of the National Center for Missing and Exploited Children, a private organization whose practices are beyond the reach of Freedom of Information Act disclosures. Questioning the tactics of those trying to protect children from sexual slavery is unpopular—but overreactions do happen. For example, the cover of the heavy metal album *Virgin Killer* was classified as child pornography in the United Kingdom years after the album was released—temporarily causing the album's Wikipedia page to be blocked in England.
- Defamation and bullying: Web 2.0, the participatory Web, promises public engagement and discussion, a step away from the "broadcast" model of journalism. Alas, the power of anonymous commentary is abused destructively. Measures proposed to fight defamation and bullying include limiting anonymity, in spite of its strong history in the United States going back to the pamphleteering of the founding fathers of the American democracy. No less a person than Jefferson himself was the object of an anonymous caricature as a cock strutting with a hen representing his slave, Sally Hemmings. While the cartoon was shocking, it did not lose him the election—but it turns out to have been on the mark.
- Cyberterrorism and cyber war: In June 2010, a bipartisan bill sponsored by senators Lieberman and Collins (S. 3480, Protecting Cyberspace as a National Asset Act of 2010) was introduced into the U.S. Senate to give the president emergency power over the Internet—in essence, the authority to declare cyber war and to marshal the power of the U.S. government to fight it on private cyber territory as a matter of homeland security. The announcement drew skeptical reaction from advocates for privacy and other civil liberties.

The Fight against Fear

In a campaign for public opinion, fear is an easier sell than freedom. We overestimate the probability of unlikely events. Many of us prefer driving to flying for our travels, especially if a horrific plane crash has been in the news. We do not stop to ask ourselves how many people have died in ones and twos in automobile accidents. The answer is that we are safer flying—it just sounds worse to die in a plane crash because so many people die all at once. In the same way, well-publicized Internet horrors create public outcries for regulatory interventions, with little statistical analysis of the incidence of the alleged problem behaviors or the cost to the public, over time, of incursions on freedom of speech and action.

A common argument for "making the Internet safe" is that preventing even one horrible crime is worth any price. Connecticut Attorney General Richard Blumenthal, for example, arguing for age verification on Myspace and Facebook to prevent predators from luring children into unsavory liaisons, said, "This is a basic issue of safety. These kinds of Web sites have created this complete delusion that this is a private world that an outsider does not get into, but it is a total misnomer. Anyone can get in." When confronted with practical arguments against Web site age verification—that it is awfully hard to tell whether someone without any form of government-issued identification is an adult or a child—Blumenthal would snort, "if we can put a man on the moon, we can verify someone's age" (Medina 2007).

Fearmongering is politically popular. One of the basic reasons we have a government is to keep us safe, so when a government official assures us that something, be it the bombing of Baghdad or registration to use Web sites, is necessary to protect us, we are inclined to sympathize. But sometimes the truth does not comport with the alarms. For example, the Internet Safety Technical Task Force (2008) established that the Internet was not a significant cause of child sexual abuse. Child sex abuse cases actually decreased 50 percent between 1990 and

2005, and most sexual propositions to youth come from peers, not adult strangers. Child sexual abuse has gone down while child Internet use has gone up—as a consequence of more vigilant policing and greater public awareness of the problem. But it is politically more profitable to attack a technology than to focus on an awkward social problem. Attorney General Blumenthal, promoting Internet fear in anticipation of his campaign for U.S. Senate, dismissed the report's finding that online social networks "do not appear to have increased the overall risk of solicitation" with an anti-intellectual punch to the public gut: "Children are solicited every day online. . . . That harsh reality defies the statistical academic research of the report" (Stone 2009b).

Indeed, this example demonstrates another unhappy fact about human fear: we much prefer to look for dangerous, mysterious demons and find magic technologies with which to strike at them than to confront problems closer to home. There is a thriving business in tools to prevent children from wandering off to pornographic Web sites or from being seduced by forty-year-old strangers from out of state. But while those things do happen, they account for a small minority of juvenile sexual misadventures. Childhood sexual exploitation is almost always at the hands of people the victims know, often relatives—uncles and cousins, for example. The age difference is often small, not large. And the children are generally on the older edge of childhood and already sexually aware. They enter relationships inappropriately but not innocently. The problem of fifteen-year-old girls having sex with eighteen-year-old cousins is uncomfortable to discuss; many who are alarmed about the *Dateline* scenarios would deny that the cousin scenario ever happens, when in fact it predominates. We prefer to search under the streetlight rather than explore the dark zone where the real crimes occur.

Internet fear has three legs. The first leg is our desire to protect ourselves, our families, our employees, and anyone else for whom we have legal or moral responsibility. The second leg is corporate interest in protecting profits, market sector, and intellectual assets. The third leg

is government interest in protecting individuals, institutions, and society from harm. Sometimes the three interact in complex ways. When the RIAA warns teenagers, "You can click but you can't hide," it is protecting its business interests by creating fear in the minds of individuals about prosecution under a federal statute they persuaded Congress to enact and for which they are the enforcers.

All three of these fear engines deserve dispassionate analysis and a reflection on the larger context in which they are visible. It may be possible to monitor constantly what children are doing online and to prevent them, as Socrates hoped, from contact with bad people and corrupting information. Yet for every child caught talking to a pedophile online, hundreds would be discouraged from searching the Internet's vast electronic library for truths their parents will not tell them. Controlling every word children are saying and hearing[1] isn't child protection or social conservatism. It is the perfect preservation of human prejudice and ignorance.

Education

The antidote to fear is knowledge. Education, in the long run, wins against terror. In the final analysis, the right responses to words are more words; the right response to bad information is good information; the right response to falsehoods is the truth.

Looking at cyberspace from 50,000 feet, we are going to be choosing between two alternative worldviews. In one view of the world, information ubiquity is the natural state; the bits will always leak. There are digital tools, such as encryption and anonymous routing, to make the flows of bits less dangerous to us and less conducive to surveillance and commercial exploitation. But fundamentally, in this worldview, people must be responsible for themselves. They need to learn home-

1. According to its Web site (as of August 3, 2010), one software product, PC Tattletale (http://www.pctattletale.com/), "records *everything* your child does when they go online."

spun safety lessons: Don't give away data about yourself if you don't want it abused. Don't believe what you read on a Web site if it's anonymous and can't be traced. Don't believe that anyone, even the government, can collect vast amounts of information and keep it all secret forever.

In spite of the costs of bullying and defamation, we need to remember the difference between words and images on the one hand and sticks and stones on the other. In this worldview the most important thing society can do is to teach people how to take care of themselves, how not to overreact to misfortunes, how to capitalize on the potential of the revolution without assuming its risks.

In the alternative view, information, for all its usefulness, is a fundamentally dangerous substance. It must be bottled up, dammed, diverted, and origin labeled, or packaged and sold for money, even if it is a century old. This is the world of *1984,* except that the information sources are in private hands, not just government hands, and the information users are commercial as well as governmental. This is the world in which the response to every problem is a regulation, or an agency, or perhaps a hardware feature. This is the world of Green Dam spyware and censorship software—China's modern *Index Librorum Prohibitorum* (Mooney 2009). It is also the world of central Internet monitoring in Australia (for obscenity) and France (for copyright infringement, in spite of the provision in article 19 of the UN General Assembly's 1948 "Universal Declaration of Human Rights" to "receive and impart information and ideas through any media and regardless of frontiers"). It is the world in which the most open societies use the tools of the most repressive, and citizens of democracies are grateful for the safety and prosperity they are promised.

~

An ancient technological cycle is being repeated today. One generation creates a technology, responding to an immediate problem and vaguely foreseeing a better future. To the next generation, the world looks very different; the solved problems are forgotten or are eclipsed

—-1
—0
—+1

by the technology's downsides. Commercial and governmental forces make it easy to forget how much power we have over how technologies will shape our future. All of us who live in free societies share that power, and especially the young, who can decide what kind of world they want to inhabit.

We can help make that choice through the political process, by watching what laws are enacted by state and national governments. We can help make it by our choices as consumers, by what we say about the features present in, and missing from, the devices and technologies we buy. We can make it by what we have to say about the workings of the institutions and businesses of which we are a part. We can resist those expurgated dictionaries and those Web sites that want to know things you do not want to tell them. We can speak up. We can leave the box on the shelf. We can click "I don't agree."

Whatever we choose, we should not let one world or the other evolve because others—especially governments and corporations—have made the choice for us. The revolution has its delights, but we need to think beyond them—think how they work, who has the data, and what they can do with it. We need to use our rationality, our knowledge, and our education to shape the world in which we and our children and our children's children will live.

Further Reading

This chapter is based on the final lecture in spring 2009 of my Harvard course "Quantitative Reasoning 48: Bits." My book with Hal Abelson and Ken Ledeen, *Blown to Bits: Your Life, Liberty, and Happiness after the Digital Explosion* (Reading, MA: Addison-Wesley Professional, 2008) is based on the course material and can be downloaded at http://www.bitsbook.com/thebook/. It includes many of the particulars of the course not elaborated in this essay.

General Bibliography

John Barlow's 1993 essay, "The Economy of Ideas," *Wired* 2.0, retrieved August 3, 2010, from http://www.wired.com/wired/archive/2.03/economy.ideas_pr.html, is worth reading in its entirety; this is an early manifesto on the collapse of the copyright and patent system due to digital reproduction by the former lyricist for the Grateful Dead.

John Barlow's utopian manifesto, "Declaration of Independence of Cyberspace," http://w2.eff.org/Censorship/Internet_censorship_bills/barlow_0296.declaration, was written with dramatic flourish in 1996 in response to the censorship provisions of the Telecommunications Act of 1996. Invoking the spirit of the American Revolution, Barlow declares cyberspace ungovernable without the consent of the governed.

Carr, Nicholas. 2009. *The Big Switch: Rewiring the World, from Edison to Google*. New York: Norton.

A light, journalistic history of centralization and decentralization of computing services, and the effect of system architecture on information control.

Lessig, Lawrence. 2006. *Code v2*. New York: Basic Books. (See also http://codev2.cc/.)

The updated edition of Lessig's classic analysis of the way "East Coast Code" (law) and "West Coast Code" (computer programs) have intertwined and evolved to control the world of information.

Post, David G. 2009. *In Search of Jefferson's Moose: Notes on the State of Cyberspace*. New York: Oxford University Press.

A wonderful analysis of the state of governance of the Internet, with deep parallels to the spirit of the early American state. (While he was ambassador to France, Jefferson had a stuffed moose erected in the lobby of his residence as a symbol of the weird and largely unexplored possibilities of the new world.)

Zittrain, Jonathan. 2009. *The Future of the Internet and How to Stop It*. New Haven, CT: Yale University Press.

The definitive argument on whether the Internet will evolve into a safe but relatively sterile technology or can continue to be "generative," as the book calls it—a seedbed of unanticipated, but not always welcome, inventions and adaptations.

Works Cited

"Australia to Implement Mandatory Internet Censorship." 2008. *Herald Sun* (Australia), October 29. Retrieved August 3, 2010, from http://www.dslreports.com/forum/r21341775-Australia-To-Implement-Mandatory-Internet-Censorship.

Blakely, Rhys. 2008. "Google Earth Accused of Aiding Terrorists." *London Sunday Times Online,* December 9. Retrieved August 3, 2010, from http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article5311241.ece.

boyd, danah, Urs Gasser, and John Palfrey. 2010. "How the COPPA, as Implemented, Is Misinterpreted by the Public: A Research Perspective." Statement to the U.S. Senate Subcommittee on Consumer Protection, Product Safety, and Insurance of the Committee on Commerce, Science, and Transportation, April 29. Retrieved August 3, 2010, from http://cyber.law.harvard.edu/publications/2010/COPPA_Implemented_Is_Misinterpreted_by_Public.

Deibert, J., John G. Palfrey, Rafal Rohozinski, and Jonathan Zittrain. 2008. *Access Denied: The Practice and Policy of Global Internet Filtering.* Cambridge, MA: MIT Press.

———. 2010. *Access Controlled: The Practice and Policy of Global Internet Filtering.* Cambridge, MA: MIT Press.

Federal Communications Commission et al. v. Fox Television Stations, Inc., et al., 07 U.S. 582 (2009). Retrieved August 3, 2010, from http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=US&vol=000&invol=07–582.

Fowler, Geoffrey A. 2009. "Kindle's Orwellian Moment." *Wall Street Journal,* July 17.

Glickman, Dan. 2009. Testimony before the Subcommittee on Government Management, Organization, and Procurement, Committee on Oversight Reform, December 9. Retrieved August 3, 2010, from http://oversight.house.gov/images/stories/Hearings/Government_Management/Intellectual_Property_Rights/DGlickman_Dec_2009_final.pdf.

Gruber, John. 2009. "Ninjawords: iPhone Dictionary, Censored by Apple." *Daring Fireball,* August 4. Retrieved August 3, 2010, from http://daringfireball.net/2009/08/ninjawords.

Heacock, Rebekah. 2009. "No More Namibia: China Blocks Search Results for Entire Country." *OpenNet Initiative,* July 22. Retrieved August 3, 2010, from

-1—
0—
+1—

http://opennet.net/blog/2009/07/no-more-namibia-china-blocks-search-results-entire-country.

Information Sciences Institute. 1981. "Internet Protocol: DARPA Internet Program Protocol Specifications." Retrieved August 3, 2010, from http://www.ietf.org/rfc/rfc791.txt.

Internet Safety Technical Task Force. 2008. *Enhancing Child Safety and Online Technologies: Final Report of the Internet Safety Technical Task Force to the Multi-State Working Group on Social Networking of State Attorneys General of the United States*. Harvard, MA: Berkman Center for Internet and Society at Harvard University. December 31. Retrieved August 3, 2010, from http://cyber.law.harvard.edu/pubrelease/isttf/.

Jefferson, Thomas. 1813. [Letter to Isaac McPherson, August 13.] Reprinted in *The Founders' Constitution, Volume 3, Article 1, Section 8, Clause 8, Document 12*. Chicago: University of Chicago Press. Retrieved August 3, 2010, from http://press-pubs.uchicago.edu/founders/documents/a1_8_8s12.html.

Kahn, Gabriel. 2010. "Comcast Official Touts Logic of Marrying Content, Distribution." *Wall Street Journal,* June 2.

Katz v. United States, 389 U.S. 347 (1967). Retrieved August 3, 2010, from http://scholar.google.com/scholar_case?case=9210492700696416594.

Kravets, David. 2009. "MPAA Wants Congress to 'Encourage' 3 Strikes, Filtering." *Wired,* November 4. Retrieved August 3, 2010, from http://www.wired.com/threatlevel/2009/11/mpaa-filtering/.

Lankarani, Nazanin. 2009. "A Push in Law Schools to Reform Copyright." *New York Times,* December 1.

Medina, Jennifer. 2007. "States Ponder Laws to Keep Web Predators from Children." *New York Times,* May 6.

Meier, Barry, and Robert F. Worth. 2010. "UAE to Bar BlackBerry Data Services, Citing Security." *New York Times,* August 2, A1.

Mooney, Paul. 2009. "Beijing's Abortive Censorship Push." *Far Eastern Economic Review* 172: 50–52.

Olmstead et al. v. United States; Green et al. v. same; Mcinnis v. same, 277 U.S. 438 (1928). Retrieved August 3, 2010, from http://scholar.google.com/scholar_case?case=5577544660194763070.

Plato. 1888. *The Republic,* Book II, trans. Benjamin Jowett. Oxford: Clarendon Press.

Protecting Cyberspace as a National Asset Act of 2010, S. 3480, 111th Congress, 2nd Session. June 10, 2010.

—-1
—0
—+1

Stone, Brad. 2009a. "Amazon Erases Orwell Books from Kindle." *New York Times,* July 17.

———. 2009b. "Report Calls Online Threats to Children Overblown." *New York Times,* January 13.

"The Telegraph Monopoly; What the People Pay for and What They Get. Mr. Gardiner G. Hubbard Describes the Methods of the Western Union to the Senate Postal Committee." 1884. *New York Times,* February 9, 3. Retrieved August 3, 2010, from http://query.nytimes.com/gst/abstract.html?res=9D04E7DD1238E033A2575AC0A9649C94659FD7CF&scp=7&sq=The+Telegraph+Monopoly&st=p.

UN General Assembly. 1948. "Universal Declaration of Human Rights." December 10, 1948, 217 A (III). Retrieved August 3, 2010, from http://www.un.org/en/documents/udhr/index.shtml.

Williams, Timothy. 2009. "Iraq Censorship Laws Move Ahead." *New York Times,* August 3.