21. Regulation of Electronic Speech and Commerce

Congress should

- resist the urge to regulate offensive content on the Web;
- allow the market to address privacy, security, and marketing concerns;
- let technical solutions have the primary role in suppressing Internet pathologies such as spam, spyware, and unwanted pop-ups;
- make certain that ''Internet governance'' remains minimal administration of technical standards and not broad social or economic regulation;
- reject preemptive regulation of new technologies such as RFID;
- reject legislation or regulation that protects incumbent businesses or business models from competition; and
- avoid burdensome and unconstitutional Internet tax collection schemes.

One of the most important things to understand about the Internet is that it is more like a language than a tangible thing. The Internet is a set of protocols that computers use to allow people, businesses, and other entities to communicate among themselves faster than ever before. Many attempts at Internet regulation are analogous to regulating the English language because people sometimes use it to do harmful or anti-social things. The Internet is also worldwide, meaning that no country can control the content of the Internet or the behavior of the online world.

Although it is true that the Internet helps bad people to do bad things, much more important, it allows good people to do good things. Never before have consumers and citizens had so much access to information about their governments, so much diversity in the viewpoints they can

hear, and so much ability to comparison shop among service providers and sellers.

The burst of creativity, communication, and commerce that the Internet has brought in the past decade or so is only the beginning of a wave of innovation and progress that the Internet medium will foster. It should be kept an unfettered, entrepreneurial realm so that we can get the maximum benefits from creative, industrious Internet communicators and businesspeople the world over.

But the technology and telecommunications sectors are increasingly under assault at the local, state, federal, and international levels. Some common refrains are coming from U.S. lawmakers and international bureaucrats alike: They blame the Internet for the social ills it reveals. They promise their constituents ''protection'' from practices that are better cured by new technology, education, choice, and responsible use of the Internet. Likewise, they attempt to shape the Internet and its use with subsidy programs and proposals for Internet governance that are actually just social and economic regulation.

Policymakers must resist intervention in the Internet and the Internet economy. Whether governments act as regulators or promoters of high-tech, they will impose needless costs and create unintended, unwanted consequences. Solutions to problems with the Internet can be found on the Internet itself. The collective intelligence and creativity of Internet users vastly outstrip those of any governmental, quasi-governmental, or bureaucratic organization.

Offensive Content

The Internet allows people to communicate about the things that interest them, and there is no doubt that sex is a fascinating subject for many people. That means that the Internet contains a lot of frank content relating to sex and eroticism, including content that caters to some quite peculiar interests. Because of the potential exposure of children to material that many people find immoral or offensive, Congress has made repeated attempts to regulate Internet speech.

The Communications Decency Act (CDA), passed to ban pornography on the Internet, was struck down by the Supreme Court in 1997. In 2002 the Supreme Court upheld a portion of the Child Online Protection Act (COPA), passed by Congress in 1998 to shield children from online pornography by requiring that website operators verify the age of visitors. The Court held that free speech is not necessarily violated by the imposition

82978$CH21 12-08-04 07:57:31

of community standards on a national scale. But, after additional review in lower courts, the Supreme Court revisited COPA in 2004 and found that the government had not proven that COPA was the least restrictive means of accomplishing its stated purpose.

Although the Supreme Court does not reject the notion of ''contemporary community standards,'' lower courts got it right when arguing that the community standards notion lets the most squeamish dictate what all others can see on the Web. In the name of protecting children, the law interferes with content that adults should have the right to see under the First Amendment. On an Internet that is increasingly capable of direct peer-to-peer communication and broadcast, individual choices and behavior replace ''community standards.''

The best and least restrictive defense against unwanted display of sexual content is parental supervision. Helpful tools, including filtering software and filtered online services, are available in the private sector. Filtered online services can also limit the receipt of unwanted salacious e-mail, for which COPA is no use. Another tool at parents' disposal is tracking software that lets them monitor everything a child does or has done on the Internet.

In countries that do not have as strong a tradition of free speech as the United States, governments have attempted to censor controversial speakers such as racists or businesses that sell artifacts of Nazism. The cure for harmful speech is not censorship but more speech to counter obnoxious ideas. The Internet helps to make sure that even the most despicable ideas, such as racism and Holocaust denial, can be fully aired, debunked, and laid to rest.

Privacy, Security, and Marketing

In the early days of the Internet, users did not understand how information moves in this medium. They were naturally concerned to know what information they revealed when they went online, how that information was protected, and how it would be used. Government regulators have clamored to answer those questions and impose their visions of online commerce. But the best answers are emerging from competition among firms to serve consumers. It is very easy to jump among competing firms online, so consumers are highly empowered to reward and punish online businesses on the basis of their privacy, security, and marketing practices.

Without regulation, online firms have instituted the practice of posting privacy policies for interested consumers to review. One hundred percent

of legitimate retailers engage in this practice—again, without regulation requiring it. This allows individuals and activists to review and critique privacy policies. Occasionally, criticism of a company's practices hits a nerve among consumers, and their rebuke is swift. The entire universe of online retailers learns the lesson.

The best example of this is the episode several years ago when DoubleClick proposed to combine click-stream information with real-world consumer profiles. The plan was cancelled long before it was implemented because of public concern. Though often used to illustrate the privacy threat, this demonstrates how responsive Internet companies are to consumers' interests and concerns.

While many consumers are concerned about privacy, many others are relatively indifferent, and those differences are rational. The availability of consumer information to manufacturers, retailers, and marketers means that products can be better designed, more economically delivered, and appealingly offered to the public. Individuals save time and money when businesses have information they can use to customize offerings, provide good customer service, and make well-targeted offers. They rarely suffer any harm from having information about their commercial behavior available to these companies.

Market forces, similarly, dictate appropriate security practices. Companies that have lost or exposed customers' personal information as a result of security breaches have suffered devastating hits in terms of public relations and lost business. They also give up competitive advantage if customer information or business strategy is revealed to competitors.

There is no need to require companies to use security procedures that are appropriate for them. It is already in their interest to do so. If a regulation requires appropriate security measures from a company that would not otherwise have them, that just preserves a company that should go out of business.

The state of California has passed a law to require notice to consumers when a security breach has revealed customer information that is particularly susceptible to identity fraud. A rigid rule like that may have perverse results: Consumers may be needlessly agitated if a security breach ultimately has no negative consequences. Because notice may interfere with a law enforcement investigation, notice can be delayed, but then the consumer will learn of a breach long after it might have mattered.

A more sensible rule would be to make holders of personal information responsible for reasonably foreseeable harms caused by security breaches.

82978$CH21 12-08-04 07:57:31

A common law rule like this would emphasize the importance of security by placing the data holder's assets at risk. It would put the burden on the data holder to decide how best to respond to any breach on the basis of the particular facts of each case. And it would protect consumers because they could be made whole if a breach caused them harm.

The marketing practices of legitimate e-commerce companies are usually covered in their privacy policies and enforced through active consumerism. The market is converging around ''opt-in'' e-mail policies because consumers distrust and reject companies that e-mail them without permission, though some may continue to do so. Studies have shown that companies only rarely violate marketing policies. If they do so, they risk offending potential customers, drawing adverse publicity, and being sued for breach of contract or under other theories of liability.

Spam, Spyware, and Other Pathologies

Today, huge quantities of unwanted e-mail travel the Internet, forcing Internet service providers (ISPs) to overbuild their systems and expend enormous effort on filtering and blocking software. In consumers' inboxes, spam is often a waste of time, sometimes a vehicle for fraud, and, once in a while, a way to find an Internet bargain.

Spammers use a variety of techniques to avoid detection as spam and to avoid tracing of their e-mails' sources. They do this both to avoid retribution and to avoid legal liability. They have been enormously successful at both.

In particular, spammers have been able to avoid nearly every law aimed at them. By late 2003 more than half of the states had passed anti-spam laws that attempted a welter of different approaches to get at spam. Those laws had little effect other than to confuse legitimate e-mailers and in some cases expose them to draconian liability and extortive lawsuits.

To clean up the mess made by the states, particularly an awfully written California law, Congress passed the CAN-SPAM Act. CAN-SPAM placed a number of regulations on commercial e-mail and preempted state regulation of e-mail, except for anti-fraud and -deception laws. While the CAN-SPAM regulations have been tolerated so far, they and other regulations drive up legal and compliance costs, particularly for small business.

Most important, though, the CAN-SPAM Act has had no effect so far on the amount of unwanted e-mail traversing the Internet, which appears only to have grown since the act was passed. This illustrates the difficulty

82978$CH21 12-08-04 07:57:31

of regulating a medium that is international, complex, and useable by anonymous parties.

A variety of technical approaches hold out the greatest chance of truly suppressing the spam problem. Typically used at the ISP level are services that filter out spam using a variety of techniques, including key-word scanning and IP banning. Anti-virus vendors have begun incorporating anti-spam capabilities into their software. Many Internet users have adopted white lists and challenge-response systems. A white list is a list of e-mail addresses from which the recipient is willing to receive e-mails. E-mails from addresses not on the list may be deleted or sent to a ''Junk'' file. Challenge-response systems ask the sender of a first-time e-mail to verify that he or she is a real person. Once a sender verifies him- or herself, future e-mails from that source are accepted automatically.

An anti-spam approach that has a great deal of potential is a sender verification protocol. In sender verification, e-mailers would publish a list of authorized e-mail servers from which they send. When e-mail is received by an ISP or individual, their system would check to see that it came from an authorized server. E-mails not from an authorized server are probably spam and could be sent to a ''Junk'' file or immediately deleted. Technical solutions like these are the most likely to suppress spam. Legal solutions have been no solution at all.

The same is probably true of spyware. ''Spyware'' is the colloquial name given to software that is surreptitiously downloaded or attached to other downloads and that reports user behavior or information without the user's knowledge or acceptance. To date, the spyware problem has been poorly defined, nearly guaranteeing that it will not be handled well. A few states have begun to legislate about spyware in much the same way they did spam.

As with spam, the most likely solutions to spyware problems are technical ones. There are already a number of software producers whose programs search users' computers for spyware. When these programs detect spyware, they remove or quarantine it and reverse unwanted changes to computer settings.

Though it pales in comparison with spyware and spam, the pop-up problem is another Internet pathology that is best addressed by technical solutions. Though some spyware legislation has thrown a net over pop-ups, this discrete problem is best solved by pop-up-blocking software. Internet browsers can give consumers choice about which sites to allow pop-ups from, just as consumers can decide which sites to accept cookies

from. Legislative solutions in this area will be too late for advancing technology and likely do more harm than good.

Internet Governance

''Internet governance'' is an emerging issue that goes to the core of what the Internet of the future will look like. When the Internet was a small project used by researchers to communicate with one another, there was no need for a formal governance structure. With the growth of the Internet to its present vast proportions and importance to the economy, a couple of organizations have asserted a need for central control of the Internet's functioning.

The leader has been the U.S. government, which, because it funded much of the research that brought about the Internet, has asserted the power to govern it. Though the source of this power is dubious and it has never been formalized by congressional act or otherwise, the Clinton administration handled the problem rather deftly by distancing control of the Internet from any U.S. government agency. Instead, the nominal governor of the Internet is a nonprofit organization called the Internet Corporation for Assigned Names and Numbers (ICANN) that answers to the U.S. Department of Commerce.

ICANN's most important responsibility is ensuring that the Internet's protocols are functioning and the Domain Name System is properly administered. Unfortunately, it has rapidly adopted a broader vision of its role and dabbled in economic and social regulation of both what products Internet registries and registrars may provide and what people may do on the Internet. ICANN has quickly become a bloated and confusing bureaucracy. It has sought large expansions in its budget to facilitate further regulatory behavior.

Despite those defects, ICANN is preferable to the other leading contender for control of ''Internet governance.'' The International Telecommunications Union, acting in conjunction with the United Nations, is seeking to bring the Internet under the control of those international bureaucracies. The recent World Summit on the Information Society signaled the UN's likely desire to seek control of the Internet's core architecture. That would subject the Internet to regulation by a confusing and remote bureaucracy that would surely think its mandate covered matters well beyond technical functioning. Already, UN actors have talked about worldwide rules for Internet communication and commerce, as well as taxation schemes to provide subsidies to special pleaders at the UN.

The widespread assumption that Internet governance is a problem for public law should be challenged. Ultimately, the Internet is a language, or an agreement on how computers talk to one another. It should be treated more as a contract than as an entity that is appropriate for external, formal regulation. Private agreements or arrangements like the Internet are more appropriately dealt with by contract law, which determines the scope of the agreement, implied terms, and expectations of the parties. Other than to interpret the agreement, there probably should not be a role for government bodies in saying what the terms of the Internet are.

New Internet Technologies

The Internet we know today is mostly used to connect computers to one another so that individuals, businesses, and governments can communicate with each other—that is, share information from organization to organization. The most prominent next generation of Internet communications will bring communication among machines, devices, and products. Radio Frequency Identification technology (RFID) is poised to create Internet connections (of a sort) for the billions of durable goods, machines, consumer goods, and spare parts that constantly flow through our economy.

By rationalizing and streamlining the movement of objects on factory floors, in stores, on trucks and trains, and in warehouses, RFID may bring substantial new efficiencies to the economy. Logistics managers know how much time and effort are wasted just finding things and moving them from Point A to Point B so that they can be put into service. RFID will use connections across the Internet to give managers information they need to manufacture and deliver the goods that consumers want and need at lower cost.

Unfortunately, the excitement and hype about the substantial benefits of RFID have caused some activists to believe that substantial privacy invasions will come from the technology. While that is certainly possible, it is less likely than is often assumed. Nonetheless, some activists, pro-regulatory groups, and legislators have called for prospective regulation of this entire suite of technologies, before anything more than experimental implementations have been put in place.

To win the substantial consumer benefits that RFID promises, it should be deployed and tested while all effects on consumer interests, such as privacy, low cost, and convenience, are considered. Should there be privacy consequences to certain implementations of RFID, economic incentives probably hold the solution, as consumers will refuse to buy products

82978$CH21 12-08-04 07:57:31

with unwanted RFID tags, or refuse to shop at stores that use RFID in unwanted ways.

Without experience, it is impossible to know how technologies like RFID may be used and what consequences they may have for good or bad. They should move forward and their adverse and beneficial consequences should be considered in real-world contexts. They should not be the subject of regulation based on speculation or projections about worst-case scenarios.

State and Local Restraints of Electronic Trade

New York Times reporter John Markoff noted in a December 2000 column, ''In a remarkably short period, the World Wide Web has touched or has promised to alter—some would say threaten—virtually every aspect of modern life.'' Of course, not everyone has enthusiastically embraced the changes the Internet has brought, *especially* those who feel threatened by it. That is particularly true in the business marketplace where many well-established industries and older institutions fear that the Net is displacing their businesses or perhaps entire industry sectors by bringing consumers and producers closer together.

That older industries fear newer ones is nothing new, of course. Any new and disruptive technology will attract its fair share of skeptics and opponents. Steamboat operators feared the railroads; railroaders feared truckers; truckers feared air shippers; and undoubtedly horse and buggy drivers feared the first automobiles that crossed their paths.

Fear of technological change is to be expected; the problem is that older industries often have clout in the political marketplace and can convince policymakers to act on their behalf. State licensing or franchising laws are often the favored club for entrenched industries that are looking for a way to beat back their new competitors. Demanding that producers comply with a crazy-quilt of state and local regulations will often be enough to foreclose new market entry altogether.

That is simply old-fashioned industrial protectionism. But requiring national or even global commercial vendors—as is clearly the case with e-commerce and Internet sellers—to comply with parochial laws and regulations is antithetical to the interests of consumers and the economy in general. Consumers clearly benefit from the development of online commercial websites and value the flexibility such sites give them to do business directly with producers and distributors. More important, the development of a vibrant online commercial sector provides important

82978$CH21 12-08-04 07:57:31

benefits for the economy as a whole in terms of increased productivity. The Progressive Policy Institute has estimated that protectionist laws and regulations could cost consumers more than $15 billion annually in the aggregate.

Lawmakers must be flexible in crafting public policies so as to not upset the vibrant, dynamic nature of this marketplace and be willing to change existing structures, laws, or political norms to accommodate or foster the expansion of new technologies and industry sectors. The fact that some ''old economy, manufacturing-age'' interests may not like the emergence of the new economy, information-age sectors and technologies does not mean policymakers should seek to accommodate older interests by stifling the development of the cybersector. Such a Luddite solution will hurt consumers and further set back the development of the online marketplace. Congress must exercise its powers under the Commerce Clause of the Constitution to protect interstate electronic commerce when it is seriously threatened by state and local meddling.

Internet Taxation

A remarkably contentious battle has taken place in recent years over the Internet Tax Freedom Act of 1998 and the federally imposed moratorium on state and local taxation of the Internet. The ITFA moratorium does not prohibit states or localities from attempting to collect sales or use taxes on goods purchased over the Internet; it merely prohibits state and local government from imposing ''multiple or discriminatory'' taxation of the Internet or special taxes on Internet access. What pro-tax state and local officials are really at war with is not the ITFA but 30 years of Supreme Court jurisprudence that has not come down in favor of state or local government. The Court has ruled that states can require only firms with a physical presence, or ''nexus,'' in those states to collect taxes on their behalf.

The effort to tax the Internet is a classic case of misplaced blame. In their zeal to find a way to collect taxes on electronic transactions to supposedly ''level the (sales tax) playing field,'' most state and local officials conveniently ignore the fact that the current sales tax system is perhaps the most unlevel playing field anyone could possibly have designed. Several politically favored industries and sensitive products receive generous exemptions from sales tax collection obligations or even from the taxes themselves. And the vast majority of ''service-sector''

82978$CH21 12-08-04 07:57:31

industries and professions receive a blanket exemption from sales tax obligations.

Citizens should be cognizant of the deficiencies of the current system and not allow state and local policymakers to trick them into thinking that the Internet is to blame for the holes in their sales tax bases. Electronic commerce sales have never represented more than 2 percent of aggregate retail sales according to U.S. Department of Commerce data. In light of this, it's hard to see how the Internet is to blame for the declining sales tax base.

Congress must also take an affirmative stand against efforts by state and local governments to create a collusionary multistate tax compact to tax interstate sales. Other options exist that state and local government can pursue before looking to impose unconstitutional tax burdens on interstate commerce. Of course, getting runaway state spending under control would go a long way toward solving many of their supposed problems. But if lawmakers really want to find a way to ''level the playing field'' and tax Internet transactions, an origin-based sales tax system would allow them to do so in an economically efficient and constitutionally sensible way. In the meantime, however, Congress would be wise to permanently extend the existing ITFA moratorium on multiple and discriminatory taxes, as well as Internet access taxes, and let Supreme Court precedents continue to govern the interstate marketplace for electronic commerce transactions.

Suggested Readings

Bell, Tom W. ''Internet Privacy and Self-Regulation: Lessons from the Porn Wars.'' Cato Institute Briefing Paper no. 65, August 9, 2001. www.cato.org/pubs/briefs/bp-065es.html.

Corn-Revere, Robert. ''Caught in the Seamless Web: Does the Internet's Global Reach Justify Less Freedom of Speech?'' Cato Institute Briefing Paper no. 71, July 24, 2002. www.cato.org/pubs/briefs/bp-071es.html.

Crews, Clyde Wayne Jr. ''Human Bar Code: Monitoring Biometric Technologies in a Free Society.'' Cato Institute Policy Analysis no. 452, September 17, 2002. http://www.cato.org/pubs/pas/pa-452es.html.

_____. ''Why Canning 'Spam' Is a Bad Idea.'' Cato Institute Policy Analysis no. 408, July 26, 2001. www.cato.org/pubs/pas/pa-408es.html.

Harper, Jim. ''Understanding Privacy—And the Real Threats to It.'' Cato Institute Policy Analysis no. 520, August 4, 2004. http://www.cato.org/pubs/pas/pa-520es.html.

Singleton, Solveig. ''Privacy as Censorship: A Skeptical View of Proposals to Regulate Privacy in the Private Sector.'' Cato Institute Policy Analysis no. 295, January 22, 1998. www.cato.org/pubs/pas/pa-295.html.

_____. ''Will the Net Turn Car Dealers into Dinosaurs? State Limits on Auto Sales Online.'' Cato Institute Briefing Paper no. 58, July 25, 2000. www.cato.org/pubs/briefs/bp-058es.html.

82978$CH21 12-08-04 07:57:31

Thierer, Adam, and Clyde Wayne Crews Jr. *Who Rules the Net? Internet Governance and Jurisdiction.* Washington: Cato Institute, 2003.

Thierer, Adam, and Veronique de Rugy. ''The Internet Tax Solution: Tax Competition, Not Tax Collusion.'' Cato Institute Policy Analysis no. 494, October 23, 2003. http://www.cato.org/pubs/pas/pa-494es.html.

—Prepared by Jim Harper and Adam Thierer