CATO HANDBOOK FOR CONGRESS

Policy Recommendations for the 108th Congress

CATO INSTITUTE
Washington, D.C.

14. Regulation of Electronic Speech and Commerce

Congress should

- resist the urge to regulate offensive content on the Web,
- allow the market to address privacy and marketing concerns,
- not undercut individuals' efforts to maintain anonymity on the Internet,
- not attempt to regulate adult behavior such as online gambling,
- reject attempts to impose new restrictions on encryption and new surveillance on American citizens,
- avoid replacing true diversity and democracy on the Internet with politically motivated ''Internet commons'' or ''public spaces,''
- avoid online protectionism by refusing to allow incumbent businesspeople to undercut electronic trade on the Internet, and
- avoid imposing burdensome and unconstitutional tax collection schemes on the Internet.

It seems that everybody's got a plan to tame the freewheeling Internet these days. The technology and telecommunications sectors of the American economy are increasingly under assault at the local, state, federal, and international levels. Republicans and Democrats alike are looking for ways to regulate everything from privacy to porn, while simultaneously seeking ways to subsidize access. The Progressive Policy Institute describes a ''failure of cyber-libertarianism'' that leads, naturally enough, to its ''Strategic National E-Commerce Policy'' framework. Ralph Nader would establish a World Consumer Protection Organization to counter the Internet's libertarian streak, which he finds intolerable. Countless other special interests are clamoring for increased government activism.

But policymakers must resist intervention. Whether the government acts as regulator or facilitator of the high-tech economy and the Internet, there will be unintended consequences. Industry should find self-regulatory solutions instead of looking to Washington for answers or assistance.

Protecting Kids Online

The Communications Decency Act, passed to ban pornography on the Internet, was struck down by the Supreme Court in 1997. But Washington continues efforts to regulate Internet content. In 2002 the Supreme Court upheld a portion of the Child Online Protection Act, 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 of community standards on a national scale.

Although the Supreme Court does not reject the notion of ''contemporary community standards,'' the lower court got it right when it noted that the community standard 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.'' And laws like COPA can have unintended consequences: barriers to those who seek porn voluntarily will likely increase e-mail solicitations for porn (spam), which COPA wouldn't regulate.

The best and least restrictive defense is parental supervision, and helpful tools, including filtering software and filtered online services, are available in the private sector. Filtered online services can 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.

Online Marketing and Privacy

Websites, as is well known, frequently collect information about visitors and often sell it. Some legislators want to require online and even main street firms to reveal what information they collect and share, and to allow customers to ''opt out.'' Others would require a much more restrictive

opt-in standard for ''sensitive'' consumer information; under that standard no information could be used until a consumer granted permission.

But is all the fuss over information-age marketing justified? Free-flowing information means more and cheaper stuff. Certainly, business use of personal information to move merchandise may sometimes be irritating, but federal regulation, which will hurt e-commerce and consumers, isn't the answer. Small businesses will suffer more than larger companies that have already assembled databases.

As businesses respond to consumer preferences, more stringent privacy protections are emerging. The notice and choice sought in privacy legislation already exist. Most highly trafficked sites already feature privacy policies. Users can set their Web browsers to reject information gathering. Software tools that provide for anonymous surfing or warn when information is being collected further empower consumers. The marketplace increasingly forces sites to develop online privacy policies as ever-more-efficient browser technology alerts users to the level of security provided.

Moreover, Washington itself can be the leading privacy offender. September 11, 2001, brought renewed government surveillance, authorized by the PATRIOT Act, that raises serious constitutional issues and should be the focus of any serious congressional privacy debate. We don't get to ''opt out'' of government information collection. Washington does not have a track record that inspires confidence in it as a protector of personal information.

Unsolicited E-Mail (spam) Policy

One legitimate purpose of limited government is to stop the use of force and fraud. That extends to fraudulent e-mail solicitations, the prosecution of which is the job of the Federal Trade Commission.

Peddling fraudulent merchandise or impersonating somebody else in the e-mail's header information should be punished, as should breaking a contract made with an Internet service provider (ISP) that prohibits bulk mailing. But in the debate over the outpouring of spam, it's important to avoid unintentionally stifling beneficial e-commerce. Sometimes, commercial e-mail, even if unsolicited, may be welcome if the sender is a business selling legal and legitimate products in a nonabusive manner.

Increasingly, legitimate companies are embracing permission-based, ''opt-in'' e-mail standards, which enable people to receive e-mail only from senders they have chosen. If legislation merely sends the most egregious offenders offshore, that may simply create legal and regulatory

hassles for small businesses trying to make a go of legitimate e-commerce or for mainstream companies that are not spammers. Unwise legislation could also create headaches for noncommercial e-mailers.

A smarter approach is e-mail filtering, such as setting the owner's screen to receive only from recognized and approved e-mail addresses. That standard is particularly appropriate for children's e-mail accounts. Emerging ''handshake'' or ''challenge and response'' systems capable of totally blocking spam show promise: since the most offensive spam is sent by automatic bulk mailing programs that aren't capable of receiving a reply, spam no longer appears in the inbox. Identifiers or ''seals'' for trusted commercial e-mail could be another means of helping ISPs block unwanted e-mail.

As the market works to shift costs of commercial e-mail back to the sender, we must be on guard against legislative confusion: How might the definition of ''spam'' expand beyond ''unsolicited'' and ''commercial'' e-mail, and would such expansion be a good thing? What about unsolicited political or nonprofit bulk e-mailings, or press releases, resume blasts, and charitable solicitations? What about newsletters that contain embedded ads or link back to for-profit websites? Would pop-up ads become suspect in the aftermath of spam legislation? They're not e-mail, but they are unsolicited and commercial.

Another piece of proposed legislation would grant ISPs the power to decide what is spam and to unilaterally block it with ''good faith'' immunity and sue the spammer. It is appropriate for consumers and ISPs to effect complete blackouts of spammers if they like; computers, wires, servers, and routers are private property. But it's not necessary to federalize such contracts.

Finally, legislative bans on false e-mail return addresses, as well as bans on software capable of hiding such information, have worrisome implications for free speech and anonymity for individuals—not just misbehaving businesses. Individuals can use ''spamware'' to create contemporary versions of the anonymous flyers that have played such an important role in our history. Individuals must retain the ability to safeguard their anonymity even in (or perhaps especially in) a mass communications tool like e-mail. In an era in which so many people are concerned about online privacy, legislation that impedes a technology that can protect privacy would be strange indeed.

Given the perfectly understandable desire to stop unsolicited mail, it is all too easy for Congress to undermine legitimate commerce, communications,

and free speech. And crippling Internet commerce would be especially pointless if spam continued pouring in from overseas.

The Internet and Anonymity

Anonymous speech is as old as America. Gentlemen calling themselves ''Publius'' wrote the *Federalist Papers.* Thomas Paine's *Common Sense* was signed by ''An Englishman.'' Today, e-mail encryption is an important example of the tradition of speaking freely and anonymously.

But encryption technology in the hands of people bent on destruction can be deadly. Some observers believe that the terrorists who attacked America communicated via encrypted messages. Fear of this indisputable threat led to renewed proposals to give government a ''back door key'' to encryption products. Similarly, calls for a national ID card exemplify new urges to shine a federal light on individuals. But calls for prohibitions on encryption products are a nonstarter in the sense that trying to prohibit bad actors from acquiring hardware or software is futile in today's global, integrated marketplace.

Government's job is to restrict the liberty of dangerous criminals and enemies—not that of innocent citizens, or to treat everyone as a suspect. The USA PATRIOT Act has set up a new law enforcement infrastructure that can easily increase surveillance of nonterrorists, but that is clearly beyond the stated intent of combating terrorism. New powers should apply only to terrorism, not to routine criminal investigations. While surveillance can and likely will be enhanced to respond to the new realities of instant electronic communications, the Fourth Amendment's protections against unreasonable and warrantless searches must not suffer.

Proposals to reregulate encryption are the digital equivalent of seizing grandma's nail clippers at the airport; terrorists would simply resort to illegal encryption. Congress decided in the mid-1990s that the benefits of readily available access to encryption technology are significant. Like proposals to mandate that everyone carry a national ID card, reregulation of encryption is a needless undermining of anonymity and privacy.

It's important to remember that the root of the terrorist threat America faces does not lie entirely in cyberspace, so fighting encryption is a misplaced priority. Despite the intense Internet privacy debate of recent years, the real dispute isn't about whether such privacy is achievable; it's about whether government will allow it where the capability finally exists. Encryption is essential, not just for keeping intact a pure version of the principle of free speech, but for such ''mundane'' needs as private

communication, secure online commerce, and business-to-business exchanges. Restrictions would damage the security of America's financial systems, making it easier for the everyday hacker, not to mention the terrorist, to invade personal information and tinker with the financial infrastructure. One of the imperatives in combating terrorism is to secure sensitive and critical systems from attack. Since encryption is essential for self-protection of companies and individuals, misguided legislation undermining it hampers sensible, private security measures.

The encryption genie is out of the bottle. Not only can malevolent programmers create their own strings of ones and zeros capable of encrypting communications, so can legitimate companies overseas. And requiring the deposit of an encryption ''key'' at a central governmental location creates a ''honey pot'' for hackers to attack, reducing our security. Encryption legislation to deliberately reduce our privacy would have been unthinkable only recently, given widespread concerns about privacy. As Rep. Bob Goodlatte (R-Va.) has pointed out, we need more encryption, not less. New encryption techniques are critical to the protection of intellectual property, such as digital distribution of books, movies, and music, on which a rising share of America's wealth creation depends.

Moreover, encryption plays a key role in the struggle for human liberty itself. It has aided political dissidents shielding themselves from brutal governments, helping democracy and individual liberty flourish overseas. Regulating encryption could encumber us far more than the terrorists, who can still encrypt as well as use other means of communication. Legal encryption may not be essential for terror, but it is essential for our advanced economy.

Internet Gambling

Some members of Congress want to stop online gambling by banning the acceptance of credit cards or other instruments for processing gambling transactions. It's understandable that politicians would be concerned about gambling operations being used as tools for terrorist money laundering.

But in this privacy-sensitive era, the question arises: if you were gambling on the Internet, how would the government ever know about it? For the government to know about such personal, consensual behavior requires spying. But to impose federal surveillance of consumer financial transactions before consumers have even widely embraced Internet banking and commerce has serious implications for people's willingness to welcome online finance.

Banks and ISPs would be drafted as snoops to sift all financial transactions. Not surprisingly, credit card companies don't want to be held responsible for ensuring that companies for which they process card services are not involved in gambling operations.

Other rationales for gambling restrictions are to target shady dealers who run phony, fraudulent operations and to protect people from addiction to gambling. That is paternalism: Consumers should screen any gambling operations with which they transact and avoid fly-by-night operators. And gambling adults are responsible for their own behavior.

What constitutes ''gambling'' is often in the eye of the legislator. Fantasy sports get a limited exemption in proposed legislation, as do horseracing and jai alai. And investing in certain technical financial instruments can be a ''gamble'' in the sense that ''the opportunity to win is predominantly subject to chance''—as proposed legislation defines gambling. Yet the anti-gambling proposals exempt ''any over-the-counter derivative instrument,'' though these clearly are not for the squeamish.

Once we travel down the road of regulating behavior on the Internet, there's basically no limit to government's ability to regulate voluntary speech and interaction and to substitute its moral vision for that of individuals.

Protecting an Internet ''Commons''

Some scholars and organizations are clamoring for creation of ''public spaces'' on the Internet. For example, University of Chicago law professor Cass Sunstein worries that the individual's habit of personalizing or filtering his Web experiences thwarts the ''unanticipated encounters'' and ''common experiences'' that should unite us as a democracy. Where the private sector doesn't come through, he wants the government to ''pick up the slack,'' requiring sites to disclose their biases and link to opposing views. And he wants popular sites to act as a ''public sidewalk,'' providing links ''designed to ensure more exposure to substantive questions.'' Presumably the government would decide if a site is guilty of ''failure to attend to public issues.'' According to this view, free speech doesn't mean saying what you want but providing a platform for other views.

Acting on similar beliefs, former leaders of the Public Broadcasting System and the Federal Communications Commission set up the Digital Promise project to ''halt the encroachment of purely market values'' on the Internet. They propose the establishment of a Digital Opportunity Investment Trust fund program, or ''DO IT,'' to fund ''the development

of online courses, training materials, archives, software, civic information, quality arts and cultural programs, and other digital resources and services of the highest standards to meet the needs of all citizens and help them gain access to the best minds and talents in our society.''

DO IT might best be thought of as a sort of ministry of cyber culture, the fusion of the National Endowment for the Arts, PBS, and the ''E-Rate'' program (or Gore tax). The $18 billion program would be funded by revenues from wireless spectrum auctions. Legislation has already been introduced to make DO IT a reality.

Despite those worries, a torrent of ''shared experiences'' bombards us despite personalization and filtering. As one critic put it, given Sunstein's view, ''these sort[s] of chance encounters should be happening to me less and less on the Internet. Instead, they seem to be happening more and more.'' Sources of exposure have ranged from the early bulletin boards of the 1980s to the peer-to-peer networks of today. And in between they encompass Web pages, search engines, chat rooms, e-mail, auctions, Internet phones, instant messaging, and more.

The Internet is already a public space, in the proper sense of the term. The public shouldn't be compelled to subsidize content deemed appropriate for cyber citizenship. Nothing in government's legitimate scope qualifies it as a fountain of superior, purer information or a source of social cohesion. Governments are well-known for censorship and control, such as the mandating of library filters and ratings for movies, music, and videogames.

Most fundamentally, the public spaces premise fails because it rests on the notion that capitalism and freedom are inimical to, rather than prerequisites for, civil society and the diffusion of ideas. We cherish a free press, dissent, and debate because governments can threaten those values. We need markets to maximize output, including that of true and useful ''public'' information.

In practice, a public spaces regime would simply deteriorate into congressional mandates and funding of ''approved'' sites. But funding is the role of venture capitalists, who have learned that not every Internet venture makes sense. Government programs would be failure proof in the sense that politics rather than competition for eyeballs would matter. Whereas the unalloyed Internet constitutes a real free press, a potpourri of information people seek (or that the unpopular post on their own dime), public spaces will consist of ''worthy'' things people are forced to pay for or link to.

Online Free Speech and the Rising Threat of Global Internet Regulation

As countries across the globe become more aware of the power of the Internet as a communications medium and channel for global commerce, they grow more interested in regulating what takes place online.

The most prominent example of such international regulatory mischief so far has been the efforts by the French courts to force the American-based Web portal company Yahoo! to remove, or at least block from the view of French citizens, those portions of its website where Nazi memorabilia are for sale. Although a lower district court in California held in November 2001 that the French ruling could not be extraterritorially enforced here in America, the Paris Criminal Court held in February 2002 that the case could go forward. Many other countries also have extraterritorial speech regulations. If such parochial speech controls were enforceable across the globe, it would obviously force content providers and network operators to restrict their speech so as to avoid potential liability or penalties.

But can parochial standards really be applied to the Web? Or is the Web truly a borderless medium that cannot be regulated in any workable sense by local authorities? Many important legal issues are at play, especially when you expand the discussion beyond free speech to include commercial regulation of the Internet. Some scholars have suggested that international treaties could be the answer. Others are calling for a ''UN for the Internet,'' or some sort of global regulatory body to resolve such questions. Still others suggest that the best answer is to do nothing, since anarchy, at least so far, has the advantage of broadening the range of free speech globally.

Although Americans have good reason to ignore the French ruling in the Yahoo! case, the question remains: how will these disputes be decided in the future? As Net connectivity across the globe grows, and human communication and interaction bridge the geographic divides between countries and continents, governments will attempt to force this new technology into old regulatory paradigms. Defenders of free speech would be wise to start thinking about ways to convince them to do otherwise.

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.

This 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 path.

Fear of technological change is to be expected; the problem is that older industries often have significantly more 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 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 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 cyber sector. 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 their favor. The Court has ruled that states can require only firms with a physical presence, or ''nexus,'' in their 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 politically sensitive products receive generous exemptions from sales tax collection obligations or even from the taxes themselves.

Sales tax collection was fairly effective in the post–World War II period when a sizable portion of the American economy was still goods based and subject to the tax.

But as America began a gradual shift to a service-based economy in subsequent decades, serious strains were placed on the sales tax system since sales taxes had traditionally not been collected on services. Therefore, the vast majority of ''service-sector'' industries and professions receive a blanket exemption from sales tax obligations.

So, as the service sector became a larger portion of the American economy, the overall sales tax base shrank accordingly. Limited efforts have been made by some states to expand sales tax coverage to include services, but those efforts have met with staunch corporate and consumer opposition. Regardless, the combined effect of the service-sector exemp-

tions and exemptions for ''special'' goods-producing industries, such as agriculture and clothing, has been the gradual diminution of the sales tax base in America.

In fact, in a December 2000 study in the *National Tax Journal,* economists Donald Bruce and William F. Fox of the University of Tennessee Center for Business and Economic Research estimated that the sales tax base as a percentage of personal income has fallen from roughly 52 percent in the late 1970s to less than 42 percent today. Worse yet, evidence suggests that, as the sales tax base has been gradually eroding in recent decades, average sales tax rates have been going up. In other words, we now have a rising average tax rate over a shrinking tax base. That is the textbook definition of an inefficient tax. Optimally, economists want a low tax rate over a very broad tax base.

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 constituted a surprisingly low 1.1 percent of aggregate retail sales in 2001 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.

Before state or local officials beg Congress to save them from the massive sales tax drain brought on by the Internet, they need to clean up the mess they've created. And if they 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 Gambling: Popular, Inexorable, and (Eventually) Legal.'' Cato Institute Policy Analysis no. 336, March 8, 1999, www.cato.org/pubs/pas/pa-336es.html.

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

Lukas, Aaron. ''Tax Bytes: A Primer on the Taxation of Electronic Commerce.'' Cato Institute Trade Policy Analysis no. 9, www.freetrade.org/pubs/pas/tpa-009es.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.

Wallace, Jonathan D. ''Nameless in Cyberspace: Anonymity on the Internet.'' Cato Institute Briefing Paper no. 54, December 8, 1999, www.cato.org/pubs/briefs/bp-054es.html.

—Prepared by Clyde Wayne Crews Jr. and Adam Thierer