Cato Handbook for Policymakers

CATO INSTITUTE

7TH EDITION

30. 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 security concerns,
- let technical solutions have the primary role in suppressing spam and spyware,
- formally disavow authority over the management of Internet addressing,
- reject preemptive regulation of radio frequency identification technology, and
- decline to compel Internet retailers to collect out-of-state sales taxes.

The burst of creativity, communication, and commerce brought forth by the Internet in recent decades 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 Internet regularly comes under assault, as poorly informed lawmakers blame it for the social ills it sometimes reveals. They promise their constituents ''protection'' from practices that are better cured by new technology, education, choice, and responsible Internet use.

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 consequences. Solutions to problems with the Internet can be found on the Internet itself. The collective intelligence, creativity, and problem-solving ability

of technologists and Internet users vastly outstrip those of any government regulator.

Don't Regulate Offensive Content

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, passed to ban pornography on the Internet, was struck down by the Supreme Court in 1997. Congress then passed the Child Online Protection Act in 1998 to shield children from online pornography by requiring that website operators verify the ages of visitors. In 2004, the Supreme Court upheld a preliminary injunction barring enforcement of the law on the ground that Internet filters were likely to be a less restrictive means of protecting children from sexually explicit material. The high court remanded the case to the lower courts for a trial, and in July 2008, the U.S. Court of Appeals for the Third Circuit found COPA unconstitutional.

The government should let this ill-considered legislation die, and Congress should not make another attempt to regulate Internet pornography. COPA would have interfered with content that adults have the right to see under the First Amendment. The best and least restrictive defense against unwanted display of sexual content to children 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.

Leave Privacy and Security to the Market

Many consumers are concerned about what information they reveal when they go online, how that information is protected, and how it will be used. Government regulators have clamored to answer those questions and impose their visions of online commerce. But the best answers will emerge from competition among firms to serve consumers. Because consumers have many options online, and because they can decline to use the Internet entirely, they can reward and punish online businesses on the basis of their privacy and security practices.

Virtually every legitimate online company has voluntarily posted a privacy policy for interested consumers and activists to review and criticize.

The market has converged around ''opt-in'' e-mail policies because consumers distrust and reject companies that e-mail them without permission. Studies have shown that companies only rarely violate marketing policies. If they do, they risk offending potential customers, drawing adverse publicity, or being sued under breach of contract or other theories of liability.

A good example was the furor over Facebook's announcement of its Beacon program. Under this program, customer activities on third-party websites would have appeared on the consumer's Facebook ''news feed.'' For example, if Amazon.com had participated in the program, a Facebook user's purchases on Amazon.com might have been automatically reported to that user's Facebook friends. The concept outraged many Facebook users. The danger of lost customers forced the company to abandon the plan in a matter of days—much more quickly than government regulators could have responded.

While many users are concerned about companies' use of their private information, many others are relatively unconcerned, and those preferences are rational. With more complete customer information, businesses can offer products and advertisements that are better tailored to individual customers' needs. Consumers rarely suffer any harm from having information about their commercial behavior available to these companies, whether it's called ''behavioral tracking,'' ''psychographic profiling,'' or something else.

It would be counterproductive for regulators to limit such potentially beneficial uses of customer information, and a ''do not track'' list that has occasionally surfaced as a proposal would be nearly impossible to administer. The risk of governments' accessing information collected by businesses should be controlled by controlling governments, not businesses. Government data retention mandates on Internet businesses should be rejected.

The law should ensure that companies honor the commitments made in their privacy policies but should otherwise leave them free to experiment with new uses for customer data. When they step over the line, they will be swiftly punished by users, who wield considerable influence in the fiercely competitive market for online services.

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 public relations and lost business. 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.

A California law requiring notice to consumers when a security breach has revealed customer information has been copied by many other states. While openness is often good, excessive notification may needlessly agitate customers over minor breaches that pose little or no danger of harm. A more sensible rule would be to make holders of personal information responsible for reasonably foreseeable harms caused by security breaches. A common-law rule like this 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. It would protect consumers because they could be made whole if a breach harmed them.

Repeal Anti-Spam Legislation, Which Failed

Today, huge quantities of unwanted e-mail travel the Internet, wasting bandwidth, disk space, and recipients' time. Large-scale spamming is a serious nuisance that imposes millions of dollars in costs on third parties. This occurs in the face of anti-spam legislation like the federal CAN-SPAM Act, which passed in late 2003. CAN-SPAM placed several regulations on commercial e-mail and preempted state regulation of e-mail, except for anti-fraud and anti-deception laws. CAN-SPAM went far beyond targeting large-scale spammers and included a variety of broad regulations that impose compliance costs on legitimate businesses while doing little to stop spam.

Ultimately, legal sanctions will be less important than technology in the fight against spam. Most e-mail applications and services now come with powerful spam filters. Although such filters are never perfect, they have become effective enough to make the spam problem manageable. CAN-SPAM and all the laws it preempted are irrelevant and should be repealed.

Don't Enact New Spyware Regulations

Congress should be equally cautious about regulating ''spyware,'' the colloquial term given to software that is installed on a user's computer without the user's knowledge or consent. Government has a legitimate role in prosecuting companies engaged in fraudulent behavior, but it has proved difficult to craft a precise definition of spyware. Overly broad legislation could cause headaches for many legitimate software vendors. Most spyware is already illegal under a variety of laws against fraud and computer hacking, and the Federal Trade Commission has prosecuted

several spyware vendors under existing laws. New regulations are unnecessary.

As with spam, the most effective anti-spyware measures will be technical, rather than regulatory. There are already several 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.

Fully Privatize ICANN

The phrase ''Internet governance'' is commonly used to describe the responsibilities of the Internet Corporation for Assigned Names and Numbers, but the phrase is misleading. In reality, Internet governance is radically decentralized, with thousands of network owners independently negotiating interconnection agreements. ICANN's primary function is a narrow one: managing the allocation of Internet names and addresses so that no two computers share the same identifier. This is an important task, but it is better described as ''coordination'' rather than ''governance.''

ICANN was created by the Clinton administration and placed under the authority of the Department of Commerce. It is officially a private, nonprofit organization, but it has proved susceptible to pressure from the U.S. government. For example, under pressure from the Bush administration, it rejected a proposal for a ''.xxx'' domain that would have been designated for pornographic materials.

Despite its flaws, ICANN is preferable to the other leading contender for control of Internet addressing. The International Telecommunications Union, acting in conjunction with the United Nations, is seeking to bring the Internet under the control of those international bureaucracies. That would be a mistake. Maintaining the integrity and stability of the Internet's addressing scheme is a technical problem, not a political one. A UN ''Internet governance'' body would be unlikely to confine itself to the narrow technical issues that are ICANN's bread and butter.

The U.S. government should preempt calls for UN control of Internet addressing by converting ICANN into a fully private, independent organization. ICANN has a complex governance structure designed to ensure that the organization's board includes representatives from a broad spectrum of interested parties and geographic regions. By formally disavowing authority over ICANN, the U.S. government can lay to rest accusations that it is pulling strings behind the scenes. That would take wind out of the sails of those pushing for a UN takeover of ICANN's functions.

Don't Regulate RFID

The last decade saw the emergence of radio frequency identification (RFID) technology, small chips that can be embedded in everyday objects and used for wireless tracking of those objects over relatively short distances. RFID has the potential to increase economic efficiency by rationalizing and streamlining the movement of objects on factory floors, in stores, on trucks and trains, and in warehouses. However, integrating the technology into supply chains has proved more difficult than expected, and it will take many years before the devices are ubiquitous.

Like many new technologies, RFID has attracted criticism from activists who fear that substantial privacy invasions will come from the technology. Although that is certainly possible, their fears have not been borne out so far. Without experience, it is impossible to know how technologies like RFID may be used and what consequences they may have for good or ill. The likely privacy harms from RFID are relatively modest, so it would be counterproductive to enact preemptive regulations before the costs and benefits of the technology are fully understood.

Say No to Internet Taxes

In April 2008, the state of New York announced that it would require Amazon.com and some other online retailers to begin collecting sales taxes on behalf of New York customers. Under federal law, a firm cannot be compelled to collect sales taxes for a state unless it has a physical presence there. Amazon.com is based in the state of Washington and has no physical facilities in New York, but New York officials have argued that the presence of Amazon ''affiliates''—third parties that advertise Amazon's products—in New York is sufficient to force Amazon.com to collect New York sales taxes. Amazon.com has vowed to fight the new requirement in court.

New York's initiative is more aggressive than most, but a number of states have banded together to create a ''streamlined'' sales tax system that would require Internet-based retailers to collect sales taxes from all American customers based on the buyer's location. About 20 states have signed on to the proposal, but it would require congressional action to make it apply nationally.

Advocates of forcing Internet retailers to collect sales taxes for out-of-state customers frame the issue as a matter of fairness, claiming that brick-and-mortar retailers are put at a competitive disadvantage by the need to

collect sales taxes from their customers. However, they ignore two important points. First, the sales taxes collected by brick-and-mortar retailers help cover the costs of infrastructure and public services that those retailers use. Traditional retailers benefit from local roads, sewers, police and fire protection, and other public services. The same is not true of Internet retailers who collect sales taxes for out-of-state customers. They pay taxes for the services they receive in their own states, of course, but they receive no benefits from the out-of-state revenues they collect.

More important, any given brick-and-mortar retail store has to be familiar with the tax laws in its own jurisdiction only. In contrast, there are thousands of distinct sales tax jurisdictions in the United States. Not only do these jurisdictions have different tax rates and different lists of items to be taxed, but many have varying definitions of common categories, such as food and clothing. The streamlined sales tax system has made some progress in standardizing such definitions, but its rules are still fiendishly complex and would only get more so as more states joined the project. That means that even the smallest online retailers would be forced to become experts on the minutiae of sales tax law in order to properly classify their products. That would be far more unfair to them than the status quo is to brick-and-mortar firms.

Congress should refuse to sanction any effort to force Internet retailers to collect sales taxes on behalf of out-of-state customers. And in the unlikely event that the courts uphold New York's revenue grab, Congress should step in and make clear that merely allowing third parties in a state to advertise one's products is not sufficient to establish a physical presence there.

Suggested Readings

Bell, Tom W. ''Internet Privacy and Self-Regulation: Lessons from the Porn Wars.'' Cato Institute Briefing Paper no. 65, August 9, 2001.

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.

Harper, Jim. ''Understanding Privacy—And the Real Threats to It.'' Cato Institute Policy Analysis no. 520, August 4, 2004.

_____. ''Federal Spyware Legislation: Some Lessons from Antiquity.'' Cato Institute TechKnowledge no. 89, October 1, 2004.

_____. ''When Data Security Regulations Fail, There Is an Alternative.'' Cato Institute TechKnowledge no. 97, March 29, 2005.

_____. *Identity Crisis: How Identification Is Overused and Misunderstood*. Washington: Cato Institute, 2006.

Lee, Timothy. ''Beacon Lessons.'' Cato Institute TechKnowledge no. 112, February 8, 2008.

Plummer, James. ‘‘‘Data Retention’: Costly Outsourced Surveillance.’’ Cato Institute TechKnowledge no. 99, January 22, 2007.

Thierer, Adam, and others. Brief of *amici curiae* Center for Democracy and Technology and Adam Thierer of the Progress and Freedom Foundation in the case of *FCC v. Fox Television Stations*. August 8, 2008. http://pff.org/issues-pubs/filings/2008/080808FoxSupremeCourtBrief.pdf.

—Prepared by Timothy B. Lee and Jim Harper