Cato Handbook *for* Policymakers

8TH EDITION

CATO INSTITUTE

59. Technology Freedom

Policymakers should

- resist the temptation to specially regulate new technologies and technology-related business models;
- foster market regulation and apply common law principles to real problems as they arise; and
- maintain the free-speech protections of the Communications Decency Act's section 230.

Society gets the most from technology and technology-related businesses when legislators and regulators give technologists and businesspeople the maximum freedom to experiment and innovate. When problems arise, government regulation is often poorly suited to addressing them. The best solutions are most often found in market responses and common law rules. This has been true with past technology developments and is true with respect to new technologies such as virtual reality and drones; sharing-economy businesses such as Uber and Airbnb; new technologies such as Bitcoin; and continually developing issues such as privacy, Internet governance, and "net neutrality." The regulations that *are* needed in the information technology area are those that control governmental and legal incursions on free speech. Congress should maintain the protections of section 230 of the Communications Decency Act of 1996.

A Selective History of Technology Regulation

Decades into the Internet era, experience shows that it is unwise to regulate technologies and businesses in anticipation of problems. Sometimes expected problems don't materialize. When they do, additional technology development is often the solution, and prescriptive regulation may do little to address the real problems. Policymakers should address new

technologies with the circumspection that experience teaches by leaving technology alone until there are clear problems that can only be solved through law or regulation.

A cautionary tale about the impulse to regulate new technologies can be found in the excitement during the 2000s about radio frequency identification (RFID) technology. In its time, RFID was going to be a multibillion dollar industry, and RFID tags were going to be found in and on nearly everything, from shirts to water bottles. The anticipated result was the potential for intensive tracking of people through their things and a wide variety of risks and harms attendant to that tracking. But RFID technology did not take off to the extent predicted. There are certainly many uses for RFID, but if regulators had comprehensively addressed RFID in light of its anticipated omnipresence, they would have wasted their own time on problems that ultimately didn't materialize.

The lessons of the RFID vogue are clear for today's highly anticipated "Internet of Things." It may be that a massive number of new devices, from refrigerators to thermostats, get connected up to the Internet. But the future of the Internet of Things may not be so great. There will be time, if new issues arise, to address them as they occur. Regulating on the basis of what is anticipated is more likely than not to miss the mark.

Challenges produced by technology are often best addressed by additional technology development. Spam email, for example, was a scourge of the Internet for a time. In 2003, Congress passed the CAN-SPAM Act, which went far beyond targeting large-scale spammers and included a variety of broad regulations that still impose compliance costs on legitimate businesses. But it did little to stop spam. Technical and business solutions, such as spam filtering by email service providers, have curtailed spam. At the same time, the opening of additional communications channels and platforms has reduced the importance of email, and spam along with it. CAN-SPAM and all the state email regulations it preempted are irrelevant and should be repealed.

Spyware was a similar scourge of a past decade. The word "spyware" stood for a small universe of programs that might be delivered to people's computers while they were browsing the World Wide Web. Once installed, these programs might report back on the browsing or other computer activity of the user. There was little legislation could do about spyware, in part because the spyware could originate anywhere in the world. Improvements in browser and computer security—not legislation—contained the spyware problem.

The Children's Online Privacy Protection Act is an example of a federal law passed in anticipation of problems that may or may not have materialized, but that probably thwarted beneficial developments. To protect children from online advertising, the act placed onerous parental permission requirements on websites that aimed themselves at young audiences. As a result, a market for websites that would serve educational, age-appropriate content to children never really emerged. Passage of this legislation deprived our society of tools that kids in impoverished circumstances could use to learn and advance themselves. It's a cost of regulation that is hard to measure because positive developments that don't happen don't announce themselves to the world.

The history of technology regulation and development shows that technology trends are hard to predict and thus to anticipate in regulation. It is often technology and business developments that will cure or contain technology-based problems. And prescriptive regulations can cut off developments that would be good for consumers and society.

Privacy, Security, and Net Neutrality: The Need for Restraint in Regulation

Unlike spam and spyware, privacy and security issues are still being hammered out as society encounters new technologies and new information-based business ideas. Companies are discovering new uses for data that better inform and serve consumers. Sometimes those uses are concerning. But as history again shows, experimentation is superior to regulation at divining consumers' true interests. Regulation in this area is nearly impossible to craft well, and it is most likely to foreclose innovations that would serve our society and the economy very well. The federal "net neutrality" regulation, among others, is a case in point.

In 2000, the Federal Trade Commission issued a list of "fair information practices" (notice, choice, access, and security) that it thought online companies should adhere to. The commission asked Congress for authority to impose them in regulation. Had the agency succeeded, Google might have had a far more difficult time producing and sustaining its massively enriching search engine, as well as the many ancillary products it provides, such as its invaluable mapping tools.

In 2006, Facebook introduced a new feature called the "News Feed," which aggregated the activities of each user's friends on his or her wall. This was met with a privacy firestorm, because people were unused to the idea of others getting immediate updates about the things they posted.

The information in Facebook's News Feed was not newly revealed, just aggregated in a new way. Public reaction prompted Facebook to create better user controls for posted content. Today, the News Feed is the heart of the Facebook experience for most people. Had regulation foreclosed this option, people would not have the kind of access to each other through social media that they have today—a level of access that most people now appreciate. As surely as Facebook changed privacy norms, it was changed by privacy norms. And just as surely, other companies will produce other products that enhance our lives and sometimes cross privacy lines. This trial-and-error process is the way our society advances, and it should not be foreclosed by regulation.

Security is a similar area, long the subject of keen lawmaker and regulator interest. Aside from a few sectoral laws, such as in financial services, there has not been comprehensive security law or regulation. This is because the subject area is too complicated to capture. Instead, owners of business processes and holders of personal data are responsible for ensuring that they do not breach sensitive information that can be used to their detriment or to harm or mortify the subjects of private data.

Net neutrality is an area of long dispute in which the Federal Communications Commission has made undesirable regulatory inroads. After years of struggle, the commission finally issued a regulation in 2015 that could survive court challenge. The agency's "Open Internet Order" purports to protect against wrongful behavior on the part of Internet service providers (ISPs), but offenses against the open tradition of the Internet have been rare, and they should not be against the law. Regulating ISPs prevents them from experimenting with technologies and business processes that may deliver better Internet service to more customers.

ISPs should be just as free to innovate and compete as any other technology-related business. The structure of the ISP market tends toward centralization, but that problem is better resolved by inviting new competition, such as by allowing novel uses of electromagnetic spectrum that could deliver wireless high-speed Internet access to consumers.

The Latest Wave of Innovations

Experience demonstrates that restraint is the best approach for lawmakers and regulators addressing themselves to technology and the Internet. This is just as true for the latest wave of innovative technologies and business models.

The prevalence of handheld devices with location awareness and downloadable applications has fostered the creation of a number of exciting new "sharing economy" businesses, such as Uber, Lyft, Airbnb, TaskRabbit, and Thumbtack. These companies act as connectors between independent service providers and consumers. They bring otherwise underutilized assets like cars and apartments into use and allow individuals to run small businesses that earn extra income. Their reputation systems create incentives for excellent service that easily surpass the consumer protections offered by existing regulators, such as taxicab commissions.

Being superior to preexisting services in almost every dimension does not mean businesses in the sharing economy are without controversy. The taxi industry has tried to portray car-sharing as unsafe, though it is not. The hotel industry and hotel workers' unions have sought to undercut apartment-sharing and to ensure that travelers staying in shared housing pay taxes as heavy as those staying in hotels. Rather than saddling new business models with old-school regulations, the regulations that prevent the existing taxi or hotel industry from providing excellent, cost-efficient service should be cleared away.

A variety of new technologies should get the same hands-off treatment that experience favors. Privately owned, unmanned aerial vehicles (drones) have many exciting uses, and more are invented all the time. Concerns about their safe operation and the privacy consequences of drone photography can be addressed without creating heavy-handed and deadening regulation that puts dampers on the benefits of distributed aerial experimentation. Virtual reality is another field that may burgeon if regulators do not capitalize on anecdotal negative experiences.

Fascinating technologies like Bitcoin also should be spared the full regulatory treatment that weighs down the existing financial services industry (as New York tried to do with its notoriously ill-thought-out "BitLicense"). Rather, the cryptocurrency market should be allowed to develop so that people around the world can get access to financial services like those enjoyed in America and Europe. Bitcoin's technology combined with new business models and practices can foreclose risks that are inherent in traditional banking. Real-time, cryptographically proven statements of assets, for example, mean that Bitcoin businesses do not have to be as opaque to their customers as banks naturally are.

The technology sector is working to deliver many more improvements. Driverless cars offer not only the huge benefit of safer transportation for millions of people, but they will have environmental benefits and permit

cities to reduce parking congestion. Anecdotes about incidents should not combine with fear of the unknown to slow the adoption of driverless car technology, which can be vastly and provably more safe than human-operated vehicles.

Having regulators examine each technology with an eye toward "consumer protection" and a properly formed-up marketplace is not the best system. The superior option is to make use of common law, basic rules that apply to everyone in the United States whether they work in technology or not.

Common law is a legal inheritance from England in which the rules that govern our interactions have arisen from years of experience over generations: avoid violence and injury to others, stick to promises, and allocate things in an orderly way. The law of battery, tort law, contract law, and property law all emerged as common practice solidified into common law. Common law requires drone operators and authors of driverless-car software to ensure that they do not injure others. It requires Bitcoin companies to provide promised services to their customers. And it permits people to interact commercially any way they like, so long as they don't violate the rights of others. Common law supplies consumer protection without the cost and intrusion of bureaucratic regulation.

Protect Internet Speech

Had it been given time to work its will, common law would almost certainly have found that individuals who post material on websites and services are responsible for their own speech and that operators of websites are not responsible for the speech of others. This rule is one of the most important after the First Amendment for protecting the vibrant marketplace of ideas that can be found on the Internet.

It was made law in the Communications Decency Act, federal legislation that Congress passed in 1996. Controversial anti-indecency provisions in the law were struck down as unconstitutional, but section 230 of the act remained. It holds that interactive computer services are not publishers or speakers of any information that others provide when using the services. That means a website or service is not legally responsible for the material that others post if, for example, that material is libelous.

Without section 230, operators of online services would probably have allowed only tightly controlled and monitored interactions among users. The rollicking, interactive Internet we know today would have been sharply curtailed.

Section 230 has come under attack from groups who would like to see it reversed. They want websites and similar services to be treated as responsible for content they host—placed there by others—and thus to control the speech of users. But that would be hugely expensive to administer and would undercut many websites and Internet services.

The protection of the Communications Decency Act keeps lawsuits from taking down highly valuable, interactive online services. The general policy of allowing technology and technology-related business to develop in freedom is the surest way to get the many, many material and social benefits of technology for all the world's people.

Suggested Readings

Downes, Larry. "A Rational Response to the Privacy 'Crisis.'" Cato Institute Policy Analysis no. 716, January 7, 2013.

Feeney, Matthew. "Is Ridesharing Safe?" Cato Institute Policy Analysis no. 767, January 27, 2015.

Harper, Jim. "Remember the Common Law." *Cato Policy Report*, March/April 2016.

Thierer, Adam D. *Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom.* Arlington, VA: Mercatus Center at George Mason University, 2016.

—Prepared by Jim Harper