Technology and Telecommunications

7

In the history of human progress, few industries have grown as rapidly or as momentously as technology and telecommunications. Those global markets have upended the ways in which we communicate, transact, and live. Just a quarter century ago, mobile phones were expensive, bulky, and often unreliable; the World Wide Web was merely an untested scientific proposal. Today, nearly half the world is online, according to the International Telecommunication Union's estimates. That virtuous cycle of investment and innovation in technology and telecommunications has boosted global productivity immensely, helping create tens of millions of high-skilled jobs worldwide—many in sectors that did not even exist a few decades ago.

How lawmakers choose to govern technology and telecommunications will influence how those sectors evolve, including decisions about where to invest private capital. If lawmakers bow to pressure from entrenched interests and self-proclaimed public-interest advocates to impose prescriptive rules or onerous liability burdens on nascent technology markets, innovation and consumer choice will suffer. Although some disruptive newcomers will surely attract serious government scrutiny, most concerns expressed about novel technologies will prove unfounded or overblown—just as most of the fears once raised about now-familiar platforms, from the Internet to email to social networks, have proved manageable.

Congress should generally steer clear of enacting new mandates or prohibitions on technology and telecommunications businesses. Lawmakers should instead observe how voluntary institutions—chiefly, civil society and the marketplace—and courts and local governments react to market failures if and when they arise. Intervention will rarely be necessary; when it is, Congress should act with a scalpel, not a sledgehammer. Meanwhile, if Congress wants to ensure that technology markets realize their full potential, lawmakers should overhaul—and in some cases eliminate—outdated laws governing such areas as copyright, information privacy, wireless spectrum allocation, and wireline telecommunications.

INTERNET FREEDOM

In 1994, the Internet began to take off among U.S. consumers eager to use the platform's first "killer app"—the World Wide Web. By the late 1990s, the Internet had transformed global commerce and communications. In the United States, most companies that own the networks that compose the Internet and the applications that use it have avoided heavy-handed regulation. But a renewed push from self-styled consumer advocates urging federal regulators to impose network neutrality regulation on Internet service providers would upset that dynamic. Similarly, federal law has largely prevented states and localities from imposing onerous, discriminatory taxes on Internet access and online commerce—but existing protections against such taxes will expire if Congress fails to renew them.

Telecommunications

Congress should:

- Explicitly define the provision of broadband Internet access—both wireless and wireline—as an information service under the Communications Act.
- Deny the Federal Communications Commission (FCC) the authority to regulate any provider of any future data transmission medium, or any service operated over such a future medium, as a common carrier.
- Clarify that Section 706 of the Telecommunications Act (47 USC § 1302) confers on the FCC no independent source of regulatory authority, reversing the D.C. Circuit's contrary holding in *Verizon v. FCC*, 740 F.3d 623, 637–40 (D.C. Cir. 2014).

When Congress last overhauled the Communications Act of 1934, it passed the Telecommunications Act of 1996 (the 1996 Act), which made barely any mention of the Internet (Public Law 104-104, 110 Stat. 56; codified as amended in scattered sections of 47 USC). In the intervening 18 years, therefore, the Federal Communications Commission has operated with limited congressional guidance about how to regulate the Internet (see, for example, 47 USC § 151). Although the 1996 Act grants the FCC no express authority to regulate "information services" (47 USC § 153[24]), it does not specify whether providing Internet access is an "information service" or a "telecommunications service"—the latter of which is subject to stringent FCC regulation as a common carrier, including mandatory interconnection and rate regulation. (See Federal-State Joint Board on Universal Service, "Report to Congress," 13 FCC Rcd 11501, 11534–35, para. 69 and n.140, 1998.)

Soon after the 1996 Act's passage, the FCC encountered the question of how to treat the broadband Internet service that a growing number of cable companies were offering. In a rulemaking process commenced under Democratic FCC Chair William Kennard and completed under Republican FCC Chair Michael Powell, the FCC determined in 2002 that it would treat cable broadband as an information service—not a telecommunications service. (In 2005, the U.S. Supreme Court upheld the FCC's decision as a permissible construction of the 1996 Act.)

Meanwhile, the FCC was also considering how to treat broadband service offered by the incumbent telephone companies—also known as "Baby Bells," the firms that AT&T divested in 1984. Those legacy phone companies had long been regulated as common carriers under Title II of the Communications Act. Moreover, Section 251 of the 1996 Act required the Baby Bells to make their last-mile facilities available, at government-regulated rates, to their competitors—many of whom, like the Baby Bells, had started offering broadband Internet access over telephone wires using a technology known as the digital subscriber line (DSL) (47 USC § 251[c]). In 2005, observing the rapid growth of facilities-based wireline broadband competition, the FCC decided to deregulate the broadband component of *all* wireline facilities. That move not only freed phone companies from common-carrier regulation of their broadband offerings but also meant that they no longer had to share their lines with DSL competitors.

Since that time, wireline broadband providers have operated under a light-touch framework, enjoying similar freedom as companies that offer services and applications over the Internet, such as Amazon, Google, and Netflix. Under that regime, the Internet has flourished as a platform for free expression, innovation, and experimentation. That trend shows no signs of slowing down, as carriers continue to deploy more robust networks, while companies at the "edge" of the Internet—includ-

ing Amazon, Google, and Netflix—make similarly significant investments.

Yet the FCC has long sought to promulgate rules to codify a concept known as "net neutrality," which entails barring broadband providers from offering paid prioritization to time-sensitive Internet traffic—such as videoconferencing and telemedicine—either at the behest of broadband subscribers or companies at the "edge" of the network.

In 2008 and again in 2010, the FCC tried and failed to create enforceable net neutrality regulation—first through adjudication, then through rulemaking. On both occasions, the U.S. Court of Appeals for the D.C. Circuit rejected the agency's efforts, concluding that both FCC actions exceeded the authority Congress had delegated to the agency. In the more recent ruling, *Verizon v. FCC*, the D.C. Circuit accepted the agency's argument that Section 706 of the 1996 Act is an independent source of authority for FCC regulation (740 F.3d at 635). But the court nonetheless vacated the agency's no-blocking and nondiscrimination rules as impermissible, finding that the rules failed to "leave sufficient 'room for individualized bargaining and discrimination in terms.'"

Since the court handed down *Verizon* in January 2014, the FCC has embarked on yet another effort to impose net neutrality regulation. This time, many net neutrality advocates and some of their allies in Congress are pushing the FCC to adopt a radical approach floated by the agency in its May 2014 notice of proposed rulemaking ("Protecting and Promoting the Open Internet, Notice of Proposed Rulemaking," 29 FCC Rcd 5561, 5564–65, para. 10, https://apps.fcc.gov/edocs_public/attachmatch/FCC-14-61A1_Rcd.pdf). They would have the agency reverse its longstanding decision to treat wireline broadband as a lightly regulated information service, rather than as a telecommunications service subject to strict common-carrier regulation under Title II of the Communications Act of 1934 (47 USC §§ 201–21). Reinterpreting broadband providers as common carriers, net neutrality supporters argue, represents the FCC's best hope of imposing enforceable net neutrality rules that withstand judicial scrutiny.

However, should the FCC decide that broadband providers are common carriers, the agency would gain not only the authority but also perhaps the *obligation* to impose myriad new regulations on broadband access. For instance, the FCC has a statutory duty to regulate the prices that common carriers charge for service, a practice known as "tariffing." The Act requires common carriers to file with the FCC detailed price schedules; the FCC, in turn, must ensure that those prices are "just and reasonable." Such price regulation, if imposed on broadband providers, would severely undercut their incentive to continue improving their networks, and it would spook investors, potentially depriving providers of access to the capital markets that finance most U.S. private-sector investment.

Net neutrality supporters dismiss those concerns, claiming that the FCC can and will exercise its statutory authority to "forbear" from tariffing and other especially onerous forms of common-carrier regulation. But it remains unclear whether the FCC is willing to broadly forbear from those rules—and, perhaps more importantly, *whether courts will permit the agency to do so*, given the agency's recent repudiation of its prior approach toward forbearance. The Internet's future is far too important to be gambled away by a risky bet on the FCC's willingness and ability to forbear from public utility-style regulations.

The FCC has suggested that it might pursue net neutrality without reinterpreting Title II of the Act to encompass broadband providers (29 FCC Rcd at 5610–12, paras. 142–47). That too would be a mistake. Even absent common-carriage mandates, net neutrality regulation is unnecessary and harmful on its own merits. Since the dawn of the net neutrality debate, American consumers have used myriad apps and services over myriad broadband providers—yet only two violations of net neutrality have been substantiated. In the more noteworthy instance, Comcast admitted to degrading some BitTorrent peer-to-peer traffic that it claimed was causing congestion for some of its other subscribers. That practice may have harmed Comcast's BitTorrent users, but what of the other subscribers whose experiences Comcast sought to improve? In the six years since it issued its Comcast order, the FCC has yet to conduct a real economic analysis of why an Internet service provider might manage its network such that certain traffic is prioritized—or degraded—relative to other data.

The virtues of paid prioritization by broadband providers are especially promising given the "two-sided" nature of the broad-

band market, wherein companies at the edge—for instance, Netflix—may have an incentive to help shoulder the costs that broadband providers bear in delivering Netflix traffic to consumers across the nation. Wireline broadband competition among two or more providers exists throughout the vast majority of U.S. markets, while wireless broadband is increasingly viable as a substitute to wireline service.

Experts: Ryan Radia, Wayne Crews

For Further Reading

Gary S. Becker, Dennis W. Carlton, and Hal S. Sider, "Net Neutrality and Consumer Welfare," *Journal of Competition Law and Economics*, Vol. 6, No. 3 (2010): 497519, http://faculty.chicagobooth.edu/dennis.carlton/research/pdfs/NetNeutralityConsumerWelfare.pdf.

Haley Sweetland Edwards, "Net Neutrality Campaign Claims Victory in 'Battle for the Net,'" *Time*, September 10, 2014, http://time.com/3319344/net-neutrality-congress-fcc/.

Robert Ellickson, *Order Without Law: How Neighbors Settle Disputes*, Cambridge, MA: Harvard University Press, 1994.

Daniel B. Klein, ed., *Reputation: Studies in the Voluntary Elicitation of Good Conduct*, Ann Arbor: University of Michigan Press, 1997.

Philip J. Weiser, "The Future of Internet Regulation," *UC Davis Law Review*, Vol. 43 (2009): 529–590.

For a comprehensive discussion of why forbearance is unlikely to avert pervasive Title II regulation of broadband providers, see "Comments of TechFreedom and International Center for Law and Economics on Protecting and Promoting the Open Internet," FCC GN Docket no. 14-28, July 17, 2014, 32–46, http://www.laweconcenter.org/images/articles/tf-icle_nn_legal_comments.pdf.

Taxation of Internet Access and E-Commerce

Congress should:

- Make the Internet Tax Freedom Act permanent.
- Reject the Marketplace Fairness Act.
- Enact legislation that bars states from requiring out-of-state online sellers to remit sales or use taxes on the basis of the remote seller's relationship with passive in-state affiliate websites.

Internet Tax Freedom Act. In 1998, Congress enacted the Internet Tax Freedom Act (ITFA), which bars states and their political subdivisions from imposing "[t]axes on Internet access" and "[m]ultiple or discriminatory taxes on electronic commerce" (Internet Tax Freedom Act, Public Law 105-277, div. C, Title XI, 112 Stat. 2681–719 [1998]; codified as amended at 47 USC § 151 note). ITFA allows states to tax online purchases—an option most states have exercised—but it bars states from imposing a higher tax rate on goods purchased online than on comparable goods purchased through other means. And ITFA bars states from imposing taxes on Internet access, except for Internet-access taxes already in force at the time of ITFA's enactment. ITFA was originally scheduled to sunset in 2001, in part because the Internet was still quite new to the public in 1998. Fortunately, Congress extended ITFA in 2001, 2004, 2007, and most recently during the 2014 lame-duck session—albeit only through October 2015.

If ITFA is allowed to expire on that date, many states will likely enact Internet-access taxes—which could cost U.S. consumers $14.7 billion annually, if existing state and local telecommunications taxes are merely applied to Internet access, according to estimates by William Rinehart of the American Action Forum. States might also respond to ITFA's expiration by imposing additional sales taxes on goods and services that their residents purchase online. Congress can prevent both of those harmful outcomes by passing the Permanent Internet Tax Freedom Act (H.R. 3086 in the 113th Congress), which would permanently codify ITFA, thus eliminating the political battle that occurs every few years when ITFA is about to expire.

Marketplace Fairness Act. Large brick-and-mortar retailers are urging Congress to pass the Marketplace Fairness Act (S. 743 in the 113th Congress), which the Senate passed in 2013, but which has stalled in the House. The bill would allow any state to force out-of-state domestic Internet retailers such as Overstock and Amazon to collect sales taxes on goods shipped to customers in that state.

The Marketplace Fairness Act would impose substantial new burdens on small and medium-sized businesses across the country, many of which employ few staffers and rely primarily on the Internet to sell goods across state lines. Those burdens would hurt the thriving e-commerce sector, which has ben-

efited tremendously from low barriers to entry and minimal regulatory burdens. And it would enable many states to impose a de facto tax increase, as existing state laws that require residents to pay a "use tax" on goods they buy remotely for in-state consumption are rarely enforced.

Experts: Ryan Radia, Jessica Melugin, Wayne Crews

For Further Reading

Joseph Henchman, "The Marketplace Fairness Act: A Primer," Background Paper no. 69, Tax Foundation, 2014, http://taxfoundation.org/article/marketplace-fairness-act-primer.

"64 Days to a Tax Increase," editorial, *Wall Street Journal*, October 9, 2014, http://www.wsj.com/articles/64-days-to-a-tax-increase-1412810890.

PRIVACY

Increasingly, we use online services such as Gmail and Facebook for our private communications, while we store and back up sensitive personal documents in the "cloud" with Internet storage providers, such as Dropbox and Apple iCloud. Although criminals occasionally breach those services to access individuals' private information for nefarious purposes—from credit card fraud to offensive voyeurism—hackers pose only a modest threat to most Internet users, especially users who take reasonable security precautions online. And when such breaches do cause serious harm, stiff criminal penalties await those hackers who are caught and prosecuted.

Yet there is one adversary against whom existing laws offer limited relief: the government. Technological change has rendered obsolete the legal regime that Congress crafted to protect us against unwarranted government access to the private information we store electronically with third-party providers. From law enforcement to intelligence agencies, many government entities, however noble their intentions, possess powerful legal and technical tools for gaining access to our communications and "metadata" about them (metadata include information such as the date and time of a phone call, or the "to" and "from" addresses of an email, but do not include content-specific information).

As several recent leaks and newly declassified documents have revealed, the breadth of information secretly collected by the U.S. government from its citizens is staggering.

Therefore, Congress should require that all law enforcement and intelligence authorities do the following:

- Obtain a search warrant before compelling a provider to divulge the contents of a U.S. person's private communications or other personal information stored with a third-party provider.
- Obtain a search warrant before tracking the location of a U.S. person's mobile communications device.
- Obtain a court order on the basis of individualized, reasonable suspicion before it can compel a provider to divulge a U.S. person's call detail records under 18 USC § 2703 or Section 215 of the USA PATRIOT Act.

By modernizing existing privacy protections to reflect current technological realities, Congress can reaffirm its commitment to individual liberty in the information age and can ensure that the Internet remains a powerful engine of economic growth. Reforming those laws need not endanger crime victims or national security. Indeed, Congress can strengthen our privacy while preserving most of the tools that law enforcement and intelligence agencies need to do their important jobs.

The Stored Communications Act is the primary federal statute governing law enforcement access to private information stored by, or transmitted through, a third-party communications service (Electronic Communications Privacy Act of 1986, Public Law 99–508, Title II, 100 Stat. 1848 [1986]; codified as amended at 18 USC §§ 2701–10 [2012]). The law, enacted in 1986 as part of the broader Electronic Communications Privacy Act, provides for varying degrees of protection for information stored electronically with third parties. Some of those protections are fairly noncontroversial.

For instance, law enforcement may compel a provider to divulge so-called basic subscriber information, including a subscriber's name and address, with a standard subpoena (18 USC § 2703[c][2]). Yet the same standard applies when law enforcement wishes to access the *contents* of private data stored with a cloud backup provider or folder synchronization service. (The government must generally give a subscriber notice before accessing the contents of his or her records, although the government routinely delays such notice under 18 USC § 2705[a].) Those subpoenas are typically issued by a prosecutor and receive no judicial review whatsoever. On the other hand, the Stored Communications Act requires law enforcement to obtain a warrant issued upon a showing of probable cause before it may compel a provider to divulge the contents of a person's unopened emails stored remotely, provided that such emails are no more than 180 days old (18 USC § 2703[a]).

In 1986, when Congress crafted that law, the distinction between opened and unopened email—and between communications and other information stored electronically online—made sense, given the state of technology at the time. In 2014, however, Americans reasonably assume that their digital "papers and effects" are safe from warrantless government access—an assumption that is often

inaccurate. To remedy that mismatch between perception and reality, and to assure consumers that their data in the cloud are safe from law enforcement fishing expeditions, Congress should pass legislation based on the Email Privacy Act (H.R. 1852 in the 113th Congress), which enjoyed 270 cosponsors in the House—including most Republicans and nearly 100 Democrats. Congress should also require law enforcement to obtain a warrant before tracking the location of an individual's mobile device, except in emergencies that involve imminent threats to life, such as the kidnapping of a child.

Congress should also address the blanket warrantless surveillance of Americans' telephony metadata and other electronic information by the National Security Agency (NSA). That issue is distinct from law enforcement access, as U.S. intelligence agencies operate under a legal regime that parallels—but is largely distinct from—the Electronic Communications Privacy Act framework described above. Instead, the NSA's intelligence collection inside the United States is governed by the Foreign Intelligence Surveillance Act of 1978 (Public Law 95–511, 92 Stat. 1783 [50 USC §§ 1801–11]); and the USA PATRIOT Act of 2001 [Public Law 107–56, 115 Stat. 272]).

Unlike civilian law enforcement agencies, which must seek warrants, orders, and convictions through state and federal courts of general jurisdiction, the NSA and other intelligence agencies are overseen by the Foreign Intelligence Surveillance Court (known as the FISA Court) (50 USC § 1803). That specialized federal court hears only those matters involving national security and intelligence operations. Unlike most hearings held by civilian courts, the FISA Court's hearings are closed to the public, and most documents filed with the court are sealed as a matter of law. Until former NSA contractor Edward Snowden disclosed numerous classified documents to the *Guardian* and *The Washington Post* in 2013, little was publicly known about the substance of the FISA Court's opinions, or the activities it had authorized.

Among those documents was a FISA Court opinion interpreting Section 215 of the USA PATRIOT Act, a controversial provision that authorizes the Federal Bureau of Investigation to secretly seek a court order requiring a person or company to produce any "tangible things" related to an authorized investigation (50 USC § 1861). On the basis of that authority, the FISA Court issued an order that required Verizon's business unit to divulge to the NSA *all domestic telephony metadata* in the company's possession—including mobile phone data. The FISA Court has since renewed the Verizon order on numerous occasions, along with similar orders for information from an unknown number of other telephone companies.

Even if some small percentage of the telephony metadata collected by the NSA pertains to bona fide national security and intelligence-gathering operations, the digital dragnet authorized by the FISA Court cannot be reconciled with the principles codified in the Fourth Amendment to the U.S. Constitution—to outlaw the "general warrants" that British officials had used to search colonists' persons and papers without individualized suspicion. And although the Supreme Court has held that the Fourth Amendment does not implicate the collection of telephone records, Congress retains the ability to protect the American people by imposing limits on government officials that go beyond the bare minimum required by the Constitution.

Since the Snowden disclosures, the Obama administration has placed some limits on how officials may search the NSA's telephony metadata database, providing for judicial review of such queries in most circumstances. Yet those protections sidestep the fundamental problem with domestic surveillance. What matters most is not *how* the data are queried, but that the government forces companies to *divulge* their bulk records in the first place. Although the law should enable intelligence agencies to obtain telephony and other metadata from U.S. companies about individuals reasonably suspected to have direct involvement with a national security threat, such collection should be targeted and precise, not indiscriminate and suspicionless.

Experts: Ryan Radia, Wayne Crews

For Further Reading

Glenn Greenwald, "NSA Collecting Phone Records of Millions of Verizon Customers Daily," *Guardian*, June 5, 2013, http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

For a broader discussion of the Stored Communications Act and its various legal protections, see Orin S. Kerr, "A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It," *George Washington Law Review* 72 (2004): 1208, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=421860.

CYBERSECURITY

Companies and consumers are increasingly worried about securing their digital information. A single data breach that compromises a firm's trade secrets or customer information can cost $1 billion or more in identity theft, lost business, system repairs, legal fees, and civil damages. Although cybersecurity is primarily a technological and economic challenge, laws and regulations also shape the choices that firms and individuals make about how to secure their systems and respond to intrusions.

Congress should:

- Reject proposals to regulate private-sector cybersecurity practices.
- Amend federal privacy statutes to remove impediments to the sharing of cyberthreat information among private firms.
- Focus on defending government systems and networks from cyberattacks.

The federal government has two primary roles in cybersecurity. First, it should enforce laws against accessing computers and networks without authorization by investigating suspected intrusions and prosecuting such offenses. Second, it should better secure its own computers and networks—with a particular focus on those systems that could, if compromised, endanger human life.

Some bills introduced in Congress would have the federal government regulate private-sector cybersecurity practices. Those proposals, however, are unwise, for any improvement they bring about in cybersecurity—if one is even realized—would likely be offset by countervailing economic burdens. Although many businesses have experienced costly cybersecurity intrusions, those businesses also tend to bear much of the ensuing costs—customers leave, insurers increase premiums, lawsuits are filed, and so forth.

Firms that suffer cyberattacks because of their lax cybersecurity practices often impose costs—externalities—on third parties who may be unable to recover the resulting losses, such as the time a consumer spends resolving disputes with banks over fraudulent credit card purchases. But the mere existence of that externality does not necessarily merit government intervention to eliminate it. Instead, such regulation is desirable only if it induces firms to take additional cost-effective precautions.

Even if a systematic market failure existed in cybersecurity, assuming that regulators are properly equipped to remedy that failure is folly. Why should regulators be expected to know how a firm should allocate its cybersecurity budget or how much it should spend on cybersecurity? Adjusting liability rules so that companies bear a greater share of the costs resulting from their cybersecurity behavior is far more likely to enhance social welfare than prescriptive regulation.

In addition, Congress could amend several federal laws to improve cybersecurity, albeit perhaps only marginally. For instance, various federal statutes limit the authority of a provider to intercept communications that traverse its own network or to share data that rest on its servers. Although those provisions aim to protect subscriber privacy, they also impede providers' ability to understand cyberthreats and to share their knowledge with other providers. Those statutes do contain exceptions that permit interception and sharing in certain circumstances—for instance, with the subscriber's "lawful consent" or to protect the provider's property—but those exceptions do not go far enough to ensure that contractual arrangements between a provider and its subscriber will suffice to enable interception and sharing.

Therefore, Congress should amend federal law to clarify that companies are generally free to monitor their own networks and systems for cybersecurity threats. To that end, in 2012 and again in 2013, the House of Representatives passed the Cyber Intelligence Sharing and Protection Act to liberalize the sharing of cyberthreat information (CISPA, H.R. 3523 in the 112th Congress; H.R. 624 in the 113th Congress). However, both versions of CISPA afforded companies exceedingly broad liability protection for cyberthreat information sharing, sweeping away not only federal statutes but also state common-law remedies as well.

In reforming federal laws to improve cybersecurity, lawmakers should respect contracts between private entities, some of whom may bargain for information-sharing regimes that differ from the statutory baseline. For that matter, cybersecurity legis-

lation should disavow any preemption of common-law principles—including the sanctity of contract and the duty to abstain from unreasonably causing harm to strangers—so that judges can adapt those doctrines to cyberthreats through case-by-case adjudication.

Experts: Ryan Radia, Wayne Crews

For Further Reading

Jerry Brito and Tate Watkins, "Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy," *Harvard National Security Journal,* Vol. 3, No. 1 (2011) 39–84, http://harvardnsj.org/wp-content/uploads/2012/01/Vol.-3_Brito_Watkins.pdf.

Center for Strategic and International Studies, "Securing Cyberspace for the 44th Presidency," December 2008, http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf.

Eli Dourado, "Is There a Cybersecurity Market Failure," Working Paper, no. 12-05, Mercatus Center, January 2012, http://mercatus.org/sites/default/files/publication/Cybersecurity_Dourado_WP1205_0.pdf.

Richard Epstein, "The Virtues of Simplicity," in *Simple Rules for a Complex World*, 21–36, Cambridge, MA: Harvard University Press, 1997.

Government Accountability Office, "Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented," GAO-13-187, February 2013, http://www.gao.gov/assets/660/652170.pdf.

Tyler Moore, "Introducing the Economics of Cybersecurity: Principles and Policy Options," in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, 3–24, Washington, DC: National Academies Press, 2010, http://goo.gl/dIuPTq.

Paul Rosenzweig, "Cybersecurity and the Least Cost Avoider," *Lawfare* (blog), November 5, 2013, http://www.lawfareblog.com/2013/11/cybersecurity-and-the-least-cost-avoider/.

Ryan Radia and Berin Szoka, "CISPA Shouldn't Infringe on Freedom of Contract," *RedState*, April 16, 2013, http://www.redstate.com/2013/04/16/cispa-shouldnt-infringe-on-freedom-of-contract/.

COPYRIGHT

In the United States, federal copyright law confers on creators of original expressive works an attenuated property right in their creations. Like other forms of property rights, copyright serves important societal interests. It benefits not only creators but also consumers, who benefit from access to many works that might not have been created but for copyright protection. Thanks to the Internet, selling copies and licenses of those works is easier than ever. Yet so too is distributing them without authorization. Congress should therefore consider strengthening copyright laws to better protect creative works from infringement. At the same time, however, some protections afforded by copyright law actually inhibit consumers' ability to enjoy original works—and artists' ability to build on earlier works.

Congress should amend the U.S. Copyright Act to do the following:

- Provide a mechanism to deny foreign websites that facilitate copyright infringement but do not abide by the Digital Millennium Copyright Act's Section 512 safe-harbor access to the U.S. payments system.
- Proscribe tools that circumvent technological protection measures only if they are likely to undermine the value of the underlying creative works protected.
- Afford users of copyrighted works an affirmative defense to infringement if they could not find the copyright holder, despite conducting a good-faith, reasonable search for the owner.

Article I of the U.S. Constitution empowers Congress "[t]o promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries." Since the nation's founding, Congress has enacted a series of federal copyright statutes—including, most recently, the Copyright Act of 1976 (Public Law 94–553, 90 Stat. 2541 [1976]; codified as amended at 17 USC §§ 101–810). For the most part, that regime works well, enabling artists to earn a living insofar as they create works that the public enjoys. From television to music to movies, the United States is home to many of the world's most celebrated artists and creative industries.

But the Copyright Act is not perfect. For instance, it contains an overbroad prohibition of tools that are designed to circumvent digital rights management (DRM). Although effective DRM can be invaluable, enabling content owners to better protect their expressive works from unlawful infringement, many legitimate and lawful reasons exist to circumvent DRM, such as making fair use of a creative work by removing digital copy restrictions. Yet Section 1201 of the Copyright Act bars technologies that are primarily designed to "circumvent a technological measure that effectively controls access" to a work or "circumvent[] protection afforded by a technological measure that effectively protects a right of a copyright owner" in a copyrighted work (17 USC § 1201).

Companies and individuals who sell or create tools that materially contribute to copyright infringement should be liable for those infringing acts—unless, that is, the tools are "capable of commercially significant non-infringing uses," to borrow a line from the U.S. Supreme Court's famous "Betamax" opinion in 1984 (*Sony Corp. of America v. Universal City Studios, Inc.*, 464 U.S. 417). With regard to firms that distribute tools designed to circumvent technological protection measures, courts should assess case by case whether those tools are designed and marketed primarily to *infringe on the underlying work*, as opposed to merely facilitating noninfringing uses of the work—including fair uses (17 USC § 107).

Congress should also address the "orphan works problem," which affects tens of millions of copyrighted works. The Copyright Act protects each work for the life of its author plus 70 years, or for works of corporate authorship, for 120 years after creation or 95 years after publication, whichever endpoint is earlier (17 USC § 302–4). People die, and corporations are acquired or cease to exist. Therefore, for many works that remain subject to copyright protection, determining who holds the copyright to those works is difficult or even impossible. Companies that wish to monetize and distribute those so-called orphan works often forgo the opportunity, for they fear that the true owner might emerge out of nowhere and sue the company for copyright infringement.

To encourage copyright holders to come forward, and to protect firms that genuinely cannot find the owner of a work despite reasonable efforts to do so, Congress should amend the Copyright Act to create a new defense to copyright infringement lawsuits. A person who uses a copyrighted work should enjoy an affirmative defense to copyright infringement if he or she could not find the copyright holder despite conducting a good-faith, reasonable search for the owner. Although that statutory change would not resolve the orphan works problem entirely, it would mark a major step toward ensuring that consumers can enjoy the wealth of protected works whose owners are unknown.

Finally, Congress should address the problem of offshore rogue websites, such as BitTorrent trackers and certain cyberlockers, that facilitate piracy of copyrighted works on a massive scale with impunity. Specifically, Congress should "follow the money" and provide for a mechanism whereby the United States may petition a federal court to order U.S.-based payment systems and advertising networks to stop doing business with the rogue site. By passing narrow legislation that provides procedural due process to websites accused of facilitating infringement, Congress can make it harder for those sites to exploit creative works without compensating their owners.

Experts: Ryan Radia, Wayne Crews

For Further Reading

Jerry Brito and Bridget C. E. Dooling, "An Orphan Works Affirmative Defense to Copyright Infringement Actions," *Michigan Telecommunications and Technology Law Review,* Vol. 12 (2005): 75–113, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=942052.

John F. Duffy, "The Marginal Cost Controversy in Intellectual Property," *University of Chicago Law Review,* Vol. 71, No. 1 (Winter 2004): 37, 42–46.

Ryan Radia, "Congress Isn't Ready for a Big Change. Here Are Some Smaller Ones," *Cato Unbound*, January 25, 2013, http://www.cato-unbound.org/2013/01/25/ryan-radia/congress-isnt-ready-big-change-here-are-some-smaller-ones.