Technology *and* Telecommunications

FREE *to* PROSPER

A Pro-Growth Agenda for the 116th Congress

COMPETITIVE ENTERPRISE INSTITUTE

Technology and Telecommunications

6

Few economic sectors rival the technology and telecommunications industries in terms of how rapidly—and momentously—they have evolved. Across the globe, the Internet and high-tech firms have reshaped how we work, live, and interact with one another. Just three decades ago, only a sliver of the population could afford mobile phones, and the World Wide Web had not yet been invented. Today, there are more mobile devices in the world than there are people, and more than half of the world's population uses the Internet. Massive investment in information technology and infrastructure has fueled innovation, greatly expanded global productivity, created tens of millions of high-skilled jobs around the world, and improved our lives in ways few could imagine two decades ago.

As technology evolves, new challenges invariably arise, including for policy makers. Establishing ill-conceived rules could stifle the high-tech economy, especially if lawmakers bow to pressure from influential business interests or self-proclaimed consumer advocates to saddle emerging technology markets with arbitrary regulations or draconian liability regimes. That does not mean that government officials should simply ignore disruptive innovations. To the contrary, newcomers who redefine existing markets—or create new markets—often merit a reevaluation of existing rules to eliminate governmental obstacles to innovation. As history shows, most concerns about novel technologies eventually prove unfounded or overblown, especially given our capacity to adapt to a changing world without help from central planners.

As lawmakers consider how to govern the technology and telecommunications sectors, new mandates or prohibitions should be avoided in all but the most exceptional circumstances. When new services or tools raise legitimate concerns about public health, consumer protection, or competition, lawmakers should resist the urge to act until they first observe how voluntary institutions—the marketplace and civil society—react to supposed market failures, if and when they arise. In the unlikely event that legislative intervention is necessary, Congress should change the law using a scalpel, not a sledgehammer.

At the same time, lawmakers should break out the sledgehammer when it comes to tearing down convoluted statutory and regulatory schemes devised in earlier eras—especially schemes administered by independent agencies, which in recent years have pulled out all the stops to remain relevant in a world in which they may no longer have a useful role to play.

PROTECT INTERNET FREEDOM AGAINST BURDENSOME NET-NEUTRALITY MANDATES

Beginning in the 1990s, the Internet has transformed global commerce, as American companies have led the way in developing better ways to harness the Internet's power and in building the infrastructure to enable that progress. Although the Internet economy has remained largely free from the shackles of bureaucracy and overregulation for much of the past quarter century, this freedom has come under attack in recent years. On the infrastructure side, a decade-long effort by federal regulators to dictate business models to the companies that provide broadband Internet access to consumers has been halted by the Federal Communications Commission (FCC)—for now. Firms that operate websites, apps, and mobile platforms have managed to evade a similar crackdown so far, but recent legislation portends greater regulation at every layer of the Internet.

Congress should:

- Classify the status of the provision of broadband Internet access to consumers—whether by wire or radio—as an information service not subject to common carrier regulation under the Communications Act of 1934.
- Comprehensively revise the Communications Act to deny the FCC the authority to regulate either the provision of broadband Internet access or services that use the Internet. Specifically, amend Section 706 of the Telecommunications Act of 1996 (47 U.S.C. § 1302) to clarify that it does not grant to the FCC any regulatory authority not otherwise afforded to the agency by the Communications Act, thereby reversing the D.C. Circuit Court's contrary holding in *Verizon v. FCC*, 740 F.3d 623, 637–40 (D.C. Cir. 2014).

Since taking off in the 1990s, the Internet has thrived as a platform for free expression, innovation, and experimentation. One might assume that federal agencies, having witnessed this success story, would refrain from regulatory intervention. Unfortunately, from 2008 to 2016, the FCC abandoned its restrained approach, attempting time and time again to expand its reach over the Internet. That effort initially focused on the principle of "net neutrality," which holds that broadband providers should be barred from blocking or prioritizing time-sensitive Internet traffic—such as videoconferencing or online gaming—upon the request of either broadband subscribers or companies that sit at the "edge" of the network. More recent

FCC actions under the Obama administration revealed that the agency wished not only to impose net neutrality rules on broadband providers but to seize broad powers to regulate the Internet.

More than 20 years have passed since Congress last made any major changes to the Communications Act of 1934 (47 U.S.C. § 151 *et seq.*). In 1996, Congress passed the Telecommunications Act of 1996 (Pub. L. No. 104–104, 110 Stat. 56), which contained practically no mention of the Internet. Since 1996, the Federal Communications Commission has struggled with questions of whether and how it should regulate the Internet. Although the 1996 Act made clear that the FCC could not regulate "information services" [47 U.S.C. § 153(24)], it did not expressly specify whether providing Internet access is an "information service" or a "telecommunications service." The Communications Act empowered the FCC to regulate providers of telecommunications services as common carriers, which it can subject to obligations ranging from mandatory interconnection to price regulation. (Federal-State Joint Board on Universal Service, Report to Congress, 13 FCC Rcd 11501, 11534–35, para. 69 & n. 140, 1998.)

In the aftermath of the 1996 Act's passage, the FCC exercised restraint in its approach to regulating the Internet under both Democratic and Republican administrations. In a proceeding launched by the FCC under Clinton-appointed Chairman William Kennard and completed under Bush-appointed Chairman Michael Powell, the FCC concluded in 2002 that broadband delivered by cable television companies was an information service, not a telecommunications service, and therefore should not be subject to common carrier regulation. In 2005, the U.S. Supreme Court upheld the FCC's decision as a permissible construction of the 1996 Act. (*National Cable and Telecommunications Association v. Brand X Internet Services*, 545 U.S. 967, 2005.)

A related question arose during those years: How should the FCC treat broadband services offered by incumbent telephone companies—also known as the "Baby Bells," the local telephone providers that were part of AT&T before its court-ordered breakup in the 1980s? The FCC had long regulated those legacy phone companies as common carrier telecommunications services under Title II of the Communications Act (47 U.S.C. § 201 *et seq.*). Section 101 of the 1996 Act required the Baby Bells to make their last-mile facilities available at government-regulated rates to third-party competitors. Many of those competitors, like the Baby Bells themselves, had started

offering broadband Internet access over telephone wires using a technology known as the digital subscriber line, commonly known by its acronym, DSL. In 2005, shortly after the Supreme Court's decision in *Brand X*, the FCC decided to align its treatment of broadband delivered over telephone lines with broadband over cable facilities, so it deregulated the broadband component of all wireline facilities. That decision not only freed phone companies from common carrier regulation of their broadband offerings, it also meant that they no longer had to share their private property with broadband rivals.

For a time, wireline broadband providers operated outside the FCC's legacy regulatory regime, and the Internet flourished. Firms such as Google, Facebook, Netflix, and Amazon grew into global high-tech leaders at a time when U.S. Internet service providers operated and innovated largely free from the strictures of federal bureaucracy.

The FCC's initial efforts to regulate Internet service providers—first through adjudication, then through rulemaking—did not end well for the agency. In 2010, the U.S. Court of Appeals for the D.C. Circuit invalidated the FCC's first net neutrality effort, in which the agency had ordered Comcast to stop degrading certain forms of peer-to-peer file sharing [*Comcast Corp. v. FCC*, 600 F.3d 642 (2010)]. In response, the FCC issued net neutrality rules, but they too were invalidated by the court in 2014 [*Verizon v. FCC*, 740 F.3d 623 (2014)]. (However, the D.C. Circuit accepted the agency's argument that Section 706 of the 1996 Telecommunications Act granted the FCC an independent source of authority for certain types of regulation). The court nonetheless held that the agency's no-blocking and nondiscrimination rules failed to "leave sufficient 'room for individualized bargaining and discrimination in terms.'"

In response, the FCC launched yet another effort to impose net neutrality regulation on Internet service providers. In May 2014, after a vigorous campaign by left-leaning activists and the Obama administration to influence the FCC—a putatively "independent" agency—Democratic Chairman Tom Wheeler proposed that the agency reinterpret the term "telecommunications service," as used in Title II of the Communications Act, to encompass broadband Internet access services. That reinterpretation was contrary to the FCC's earlier determinations that Internet access was an "information service." In early 2015, the FCC voted along party lines to approve the proposal.

Several companies and other parties immediately petitioned the U.S. Court of Appeals for the D.C. Circuit to vacate the FCC's order, arguing that the agency's decision to reclassify Internet access service as a telecommunications service was arbitrary and capricious. But in June 2016, the court upheld the agency's order in a 2-1 opinion (*U.S. Telecom Association v. FCC*, 825 F.3d 674, 2016). In response, several petitioners have asked the entire D.C. Circuit to review the panel opinion *en banc*, and some companies have publicly stated that they believe the U.S. Supreme Court will ultimately decide whether the FCC has the authority to regulate Internet service providers as common carriers.

The FCC then embarked on a "regulatory voyage" using its proclaimed authority, intervening in ways that had little to do with net neutrality. For instance, in 2016, the FCC imposed draconian rules on the privacy practices of Internet service providers that curtailed the ability of broadband providers to offer consumers lower prices in exchange for targeted advertising. That made it costlier for broadband companies to do business.

That FCC regulatory onslaught came to an abrupt halt in early 2017, when the agency's leadership changed. Under the agency's current chairman, Ajit Pai, the FCC reversed course and issued new regulations in January 2018 to restore Internet freedom (83 Fed. Reg. 7852). Among the changes, the FCC reestablished its previous treatment of Internet service providers as information services not subject to utility-style common-carrier rules. In May 2018, however, the U.S. Senate voted 52-47 to pass a Congressional Review Act resolution of disapproval regarding the FCC's order (S.J. Res. 52, 115th Congress). The House of Representatives has yet to vote on the matter. If it does, it should reject the Senate's resolution and instead pass legislation to ensure that a future FCC cannot restore the onerous regulations the current FCC has worked so hard to eliminate.

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 Comparative Law and Economics*, Vol. 6, No. 3 (2010), p. 497, 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, *Reputation: Studies in the Voluntary Elicitation of Good Conduct* (Ann Arbor, MI: University of Michigan Press, 1997).

Reinhardt Krause, "Net Neutrality Upheld: Big Win For FCC, Netflix; AT&T Vows To Appeal," *Investor's Business Daily*, June 14, 2016, https://www.investors.com/news/technology/comcast-att-stocks-fall-as-appeals-court-upholds-fcc-open-internet/.

Hal Singer, "Capital Expenditures in Broadband: 2Q-16 Update," Hal Singer blog, August 11, 2016, https://haljsinger.wordpress.com/2016/08/11/capital-expenditures-in-broadband-2q-16-update/.

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, pp. 32–46, Protecting and Promoting the Open Internet, *FCC GN* Docket No. 14-28 (released May 15, 2014), comments submitted July 17, 2014, http://docs.techfreedom.org/ICLE-TechFreedom_Policy_Comments_on_2014_FCC_Net_Neutrality_NPRM.pdf.

Philip J. Weiser, "The Future of Internet Regulation," *University of California-Davis Law Review*, Vol. 43 (2009), pp. 529, 551, https://lawreview.law.ucdavis.edu/issues/43/2/articles/43-2_Weiser.pdf.

PROTECT PRIVACY AND CYBERSECURITY BY SECURING PRIVATE INFORMATION FROM UNDUE GOVERNMENT PRYING

More and more consumers use Internet-based services such as Snapchat and Gmail for their private communications and back up sensitive files with "cloud" platforms, such as Dropbox and iCloud. Those services do not guarantee perfect security. Fortunately, for Internet users who are not celebrities or public figures, malicious actors on the Internet rarely cause catastrophic consequences, especially for people who take reasonable security precautions. But criminals and hackers are not the only adversaries threatening our privacy and security—we should also worry about government.

Evolving technologies have eroded many of the legal constraints that were designed to protect Americans from overzealous or unscrupulous officials who want to access the private information we store with third-party service providers. Numerous governmental entities, from local law enforcement to federal intelligence agencies, have a powerful arsenal of technological and legal means at their disposal for accessing our communications and our metadata—information about our communications, such as when and to whom a particular email was sent. As several high-profile leaks and recently declassified documents have revealed, the breadth of information that the U.S. government collects about its citizens is staggering—and many programs surely exist that the public is not yet aware of.

Congress should:

- Require that all law enforcement and intelligence authorities 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, in accordance with the provisions of the Email Privacy Act (H.R. 387 in the 115th Congress); or
  - Tracking the location of a U.S. person's mobile communications device.

To level the playing field between the government and the governed, Congress should update and expand the legal framework under which law enforcement and intelligence officials conduct surveillance and compel private companies to divulge private

information. By reaffirming the nation's commitment to individual liberty in the information age, Congress can reassure Americans that using the Internet and other cutting-edge platforms does not mean saying goodbye to privacy—and that fighting crime and protecting national security are consistent with the Fourth Amendment. In fact, 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, Pub. L. No. 99–508, tit. II, 100 Stat. 1848 (1986), codified as amended at 18 U.S.C. §§ 2701–2710 (2012)]. This 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 U.S.C. § 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 sync service. [The government must generally give a subscriber notice before accessing the contents of her records, although the government routinely delays such notice under 18 U.S.C. § 2705(a).]

Subpoenas typically are 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 on 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 U.S.C. § 2703(a)].

In 1986, when Congress crafted the Stored Communications Act, the distinction between opened and unopened mail and that between communications and other information stored electronically online made sense, given the state of technology at the time. In 2018, however, Americans reasonably assume that their digital "papers and effects" are safe from warrantless government access—an assumption that is

often inaccurate. To remedy this mismatch between perception and reality, and to assure consumers that their data in the cloud is safe from law enforcement fishing expeditions, Congress should pass legislation based on the Email Privacy Act, which passed the House of Representatives in a unanimous vote in the 114th Congress (H.R. 699) and passed the House on a voice vote in the 115th Congress (H.R. 387). Congress should also require law enforcement to obtain a warrant before tracking the location of an individual's mobile device unless a provider agrees to disclose a subscriber's information on the basis of an apparent emergency involving an imminent threat to human life, such as the kidnapping of a child.

Experts: Ryan Radia, Wayne Crews

For Further Reading

Glenn Greenwald, "NSA Collecting Phone Records of Millions of Verizon Customers Daily," *The Guardian*, June 6, 2013, http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

Orin S. Kerr, "A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It," *George Washington Law Review*, Vol. 72 (2004), p. 1208, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=421860.

EMPOWER THE MARKET TO PROTECT 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.

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 systems that could endanger human life if compromised.

Some bills introduced in Congress in recent years would have the federal government regulate private-sector cybersecurity practices. Those proposals are unwise. Any improvements they bring about in cybersecurity—if they are 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 cost—customers leave, insurers increase premiums, and trial lawyers purportedly representing injured classes of people file lawsuits against the business.

Congress should:

- Reject proposals to regulate private-sector cybersecurity practices.
- Focus on defending government systems and networks from cyberattacks.

Firms that suffer cyberattacks as a result of their lax cybersecurity practices often impose costs in the form of externalities—such as the time a consumer spends resolving disputes with banks over fraudulent credit card purchases—on third parties that may be unable to recover the losses. But the mere existence of this externality does not necessarily mean that government intervention is needed to eliminate it. Even if a systemic market failure existed in cybersecurity, 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 is prescriptive regulation.

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 (2011), pp. 39–84, http://harvardnsj.org/wp-content/uploads/2012/01/Vol.-3_Brito_Watkins.pdf.

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

Government Accountability Office, "Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented," GAO-13-187 (2013), p. 36, http://www.gao.gov/assets/660/652170.pdf.

Tyler Moore, "Introducing the Economics of Cybersecurity: Principles and Policy Options," in National Research Council, *Proceedings of a Workshop on Deterring Cyberattacks* (Washington, DC: National Academies Press, 2010), pp. 3–23, https://www.nap.edu/read/12997/chapter/3.

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/.

MODERNIZE REGULATION OF TELEVISION AND MEDIA

In recent years, Americans have increasingly augmented or even replaced traditional television viewing with Internet-based video services, such as Hulu, Netflix, Amazon Video, and HBO Now. In fact, just two of those companies—Netflix and Amazon—have as many streaming video subscribers in the United States as every cable and satellite television provider combined. Yet, the U.S. television marketplace remains fragmented because of an anachronistic set of laws and regulations that govern broadcasters, cable television providers, and satellite carriers. Not only do those outdated rules undermine the vitality of traditional media businesses, they also threaten the future of Internet-based television services.

Congress should:

- Amend the Copyright Act to give creators of original television programs the same exclusive rights to their audiovisual works as those afforded to other artists, regardless of whether such programming is transmitted over broadcast stations, cable systems, satellite carriers, or the Internet.
- Repeal Title VI of the Communications Act and related obligations and privileges to which multichannel video programming distributors are currently subject, except for provisions preempting states and their subdivisions from imposing unreasonable regulations on television providers.
- Eliminate ownership limits and similar economic restrictions on legacy media businesses, including the newspaper cross-ownership rule, the television duopoly rule, and limits on local marketing agreements.

Under current law, if a cable or satellite company wishes to retransmit the signal of a broadcast station, such as a local NBC affiliate, it must first secure the consent of that affiliated station's owner [47 U.S.C. § 325(b)]. In most circumstances, the station will permit the television content provider to carry its signal only if it agrees to pay the station a monthly fee based on the number of subscribers who receive the station's programming. Ultimately, consumers pay those fees as part of their monthly cable or satellite bill. Most of the fees are not retained by local stations. Instead, stations typically are obligated by contract to pay the fees they collect from cable and satellite providers to the nationwide television network with which they are affiliated. Additionally, every cable or satellite company that retransmits a broadcast signal must pay the U.S. Copyright Office a legally prescribed amount in exchange for a

compulsory copyright license to publicly transmit the underlying television programs. In turn, the Copyright Office distributes those fees to the copyright owners whose works were distributed by the television company.

In contrast to that convoluted regime, when an Internet company such as Netflix or Hulu wishes to stream a television show to its subscribers, it must secure the permission of a single entity—the owner of the show's copyright. Both sides are free to come up with mutually agreeable terms. No payments to broadcasters or to the Copyright Office are required. There is no government fee schedule to learn. Of course, Netflix does not always come to an agreement when it wishes to stream a particular television show—from time to time, certain shows disappear from the company's library, only to be replaced by new shows. Similarly, cable and satellite providers sometimes fail to reach an agreement with a broadcast station to carry its signal, resulting in a temporary "blackout" for the provider's subscribers. Neither situation is optimal, but existing law assigns the FCC a role in disputes involving broadcasters and traditional television companies, not in disputes involving Internet-based platforms. Clearly, FCC regulation has not improved market outcomes.

Many other complex regulations affect and often distort the market for television distributed by cable and satellite companies. Title VI of the Communications Act contains myriad rules that govern cable systems and satellite carriers (47 U.S.C. § 521 *et seq*). For example, cable and satellite companies are subject to "program carriage" regulations that limit their ability to strike deals with video programming vendors to obtain exclusive programming rights (47 C.F.R. § 76.1301). Yet that is precisely the type of arrangement that has been central to the success of Internet streaming platforms, many of which differentiate themselves as the exclusive source of first-run hit shows such as Netflix's *Black Mirror* and Amazon's *Jack Ryan*. In fact, the FCC has even suggested that it might reinterpret the Communications Act so that many of those legacy provisions would apply to "linear" Internet-based platforms that distribute live programming at prescheduled times.

Beyond the FCC's rules governing television, many other regulations inhibit diversity and competition in mass media. For instance, in recent years, newspapers have lost billions of dollars in revenue and millions of subscribers. In many cities, iconic newspapers have ceased printing a daily edition or closed their doors entirely. Yet FCC rules effectively bar a company from owning both a newspaper and a

broadcast television station serving the same city—despite the natural advantages of consolidating news-gathering operations across various media platforms. That regulation has undoubtedly contributed to the decline of newspapers, ultimately hurting people who live in communities that would otherwise be served by local media outlets with more funding, personnel, and other resources.

Experts: Ryan Radia, Wayne Crews

For Further Reading

Comments of the Competitive Enterprise Institute, International Center for Law and Economics, and TechFreedom to the Federal Communications Commission in the Matter of Promoting Innovation and Competition in the Provision of Multichannel Video Programming Distribution Services, Notice of Proposed Rulemaking, MB Docket No. 14-261 (2014), https://cei.org/sites/default/files/CEI-ICLE-TechFreedom%20Comments%20in%20FCC%20MVPD%20Definition%20Proceeding%2014-261.pdf.

Ryan Radia, "Regulation Killed the Video Star: Toward a Freer Market in Broadcast Television," *Federal Communications Law Journal*, Vol. 67 (2015), pp. 235–266, http://www.fclj.org/wp-content/uploads/2015/08/67.2.3_Radia.pdf.

UPDATE COPYRIGHT FOR THE INTERNET AGE

From television shows to music to movies, the United States is home to many of the world's most celebrated artists and creative industries. The nation's legal environment has helped content providers contribute to this cornucopia of creativity.

U.S. copyright law confers upon creators of original expressive works an attenuated property right in their creations. Copyright serves important societal interests, enriching not only artists but also consumers, who benefit from works that might not have been created but for copyright protection. The Internet has made it easier than ever to sell copies and licenses to original works, but it has also facilitated the unauthorized distribution of such works on an unprecedented scale. Therefore, Congress should amend copyright laws to address provisions that inhibit consumers' ability to enjoy original works while also considering reforms to better protect creative works from infringement.

Congress should:

- Amend the U.S. Copyright Act so that it:
  - Bans tools that circumvent technological protection measures only if they are likely to undermine the value of the underlying creative works they seek to protect;
  - Affords users of copyrighted works an affirmative defense to charges of infringement if they cannot find the copyright holder despite conducting a good faith, reasonable search for the owner; and
  - Enhances the ability of copyright owners to ensure that infringing copies of their works on the Internet are permanently taken down without imposing undue burdens on online service providers that host or index content.

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. [Pub. L. No. 94–553, 90 Stat. 2541 (1976) (codified as amended at 17 U.S.C. §§ 101–810)]. For the most part, that regime works well, enabling artists who create popular works to earn a commensurate return on their efforts.

However, the Copyright Act could be improved in certain ways. For instance, its prohibition of tools that are designed to circumvent digital rights management (DRM) is overly broad. Although effective DRM can be invaluable, in enabling content owners to better combat the infringement of their expressive works, not all forms of DRM circumvention are illegitimate or unlawful. Yet Section 1201 of the Copyright Act makes it illegal to create or distribute technologies that are primarily designed to "circumvent a technological measure that effectively controls access" to a work or to circumvent "protection afforded by a technological measure that effectively protects a right of a copyright owner" in a copyrighted work (17 U.S.C. § 1201).

In general, companies and individuals who sell or create tools that contribute to copyright infringement are *not* liable for those infringing acts if 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). Similarly, for firms that distribute tools that are designed to circumvent technological protection measures, courts should assess on a case-by-case basis 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 use (17 U.S.C. § 107).

Congress should also address the "orphan works problem" that plagues the ongoing enjoyment of millions of copyrighted works. The Copyright Act protects the exclusivity of each original 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 U.S.C. § 302–04). People eventually die, and corporations are regularly acquired or cease to exist. Yet many works created by persons who are now deceased or corporations that are now defunct remain subject to copyright protection, making it difficult or impossible to ascertain who holds the copyright for those works. Companies that wish to monetize and distribute those so-called orphan works often forego the opportunity, out of 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 against changes of copyright infringement if he could not find the copyright holder after

conducting a good faith, reasonable search for the owner. This reform would not resolve the orphan works problem entirely, but it would mark a major step toward allowing consumers to enjoy a wealth of protected works with unknown owners.

Creators seeking to prevent the online infringement of their works regularly make use of the Copyright Act's notice-and-takedown regime, which Congress created in 1998 (17 U.S.C. § 512). Under that process, online service providers that store digital files on behalf of users—such as video hosting sites—or provide tools for locating information on the Internet—such as search engines—are eligible for a safe harbor from copyright infringement liability if they expeditiously remove content or links to infringing materials on receiving notification from a copyright owner regarding the unauthorized work. Although that system has proven to be invaluable for creators seeking to protect their exclusive rights in their original works, many artists—especially those without the resources of larger content companies—struggle to effectively combat the unlawful dissemination of their creations. Therefore, Congress should carefully explore potential revisions to the Copyright Act's notice-and-takedown provisions to ease the burden on copyright owners whose works are repeatedly reposted after being taken down from the same provider's site.

In considering such reforms, lawmakers should resist calls to impose technological mandates on online service providers that could greatly increase the cost of operating user-centric platforms or encourage the use of tools that indiscriminately filter content without regard to whether it is protected by fair use.

Experts: Ryan Radia, Wayne Crews

For Further Reading

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.

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), p. 75, 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 (2004), p. 37.

DO NOT EMPOWER STATES TO BE ABLE TO TAX OUTSIDE THEIR BORDERS

The rapid growth of online retailing over the past two decades has been met by calls from state and local officials for greater authority to capture more sales tax revenue, including from consumers residing in other states. Similarly, big-box retailers have spent decades asking Congress to "level the playing field" by removing physical nexus standards for collecting state sales tax, which they claim gives an advantage to online retailers. All of this culminated in this year's overturning of longstanding taxing restrictions in the case *South Dakota v. Wayfair*, decided by the Supreme Court in the summer of 2018.

Congress should:

- Prevent states from exporting their taxation regimes outside their geographic borders.
- Codify longstanding rules for physical nexus requirements of state taxation.
- Support origin-based approaches to remote state sales tax.

Before *South Dakota v. Wayfair*, the *Quill v. North Dakota* precedent required a seller to have a physical presence, or "nexus," in the buyer's state before it could become subject to the latter state's sales tax. Far from a tax loophole, this is the principle of "No taxation without representation" in action. The seller, not the buyer, calculates and remits sales tax. Although that arrangement can lead to different sales tax treatment among different types of retailers, it greatly benefits consumers by preserving healthy tax competition among states.

However, *Quill*'s default rule is no longer in control. States are now free to expand their remote taxation powers to an unprecedented extent. The overturn of *Quill*'s physical presence by the Supreme Court in *South Dakota v. Wayfair* makes it critical and urgent for Congress to impose a moratorium on states acting on their own to expand their remote taxation powers. Then Congress should go on to legislate a federal origin-based regime for online sales taxes.

Allowing states to expand their taxing powers unchecked 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.

That would hurt the thriving online retail industry, which has benefited tremendously from low barriers to entry and minimal regulatory burdens. And it would constitute 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. Congress must act swiftly and decisively to stem the chaos that the Court's reversal will bring.

Although politically challenging, an origin-based approach to remote sales is the only solution that balances federalism, economic efficiency, and tax equity among different types of retailers. Online retailers, like their peers in the brick-and-mortar world, would be taxed at the point of sale, not on the basis of the destination of the product or the residence of the buyer. That keeps taxing authorities politically accountable to whom they are taxing, avoids costly compliance costs of a destination-based system, and treats all sellers equally.

The Marketplace Fairness Act (MFA, S. 976, 115th Congress) passed the Senate in 2013 and was reintroduced in the 114th Congress, but companion legislation stalled in the House. The MFA empowers states to reach across their borders and collect sales tax from companies based in other states. It would impose high compliance costs on businesses, by requiring them to calculate taxes for approximately 10,000 distinct jurisdictions, each with its own rates, definitions, exemptions, and tax holidays. It also would subject businesses to audits by out-of-state tax authorities. It would lessen downward pressure on sales tax rates from tax competition and threaten consumer privacy through states' data sharing.

The Remote Transaction Parity Act (RTPA, H.R. 2193, 115th Congress) adopts the same approach as the MFA. It gives states unprecedented new powers to reach across their borders to tax out-of-state businesses for online sales, but it includes a few tweaks. Presumably to address concerns about cross-state audits, the RTPA creates an option for sellers to use state-employed tax compliance agents. It attempts to protect sellers with gross receipts of less than $5 million from being audited by other states but then creates a loophole whereby a state can trigger an audit on a remote seller of any size by claiming "intentional misrepresentation." The draft also contains a boiling frog–style rolling small seller exemption. In the first year, it exempts businesses with less than $10 million in gross receipts for combined remote and in-state sales in the previous year. In the second year, the threshold drops to $5 million, and in the third year, it permanently drops to $1 million.

In August 2016, House Judiciary Committee Chairman Bob Goodlatte (R-Va.) released a discussion draft of a hybrid-origin sourcing model as an alternative to the MFA and RTPA approach. Under his plan, the seller applies his home domicile's sales tax base and the buyer's home state's sales tax rate to remote purchases. The seller then remits the tax to his home state's tax authority. That authority then forwards the money to a clearinghouse that channels revenue back to the buyer's home taxing authority by formula. This approach avoids the high compliance costs for sellers in the MFA and RTPA and eliminates their threat of cross-border audits and the resulting consumer privacy concerns. Unfortunately, it also undermines beneficial interstate tax competition by allowing states to export their tax rates to sellers wholly located in other states. It also requires non–sales tax states' businesses to collect and remit sales taxes, thereby compromising those states' autonomy.

The Online Sales Simplicity and Small Business Relief Act (H.R. 6824, 115th Congress), introduced by Rep. Sensenbrenner (R-Wisc.) in September of 2018, would go a long way toward stemming the damage and chaos for smaller online retailers resulting from the *Quill* reversal in *Wafair*. Specifically, it would:

- Prevent states from collecting taxes retroactively;
- Prevent states collecting from until January 1, 2019; and
- Institute a remote small business exemption for firms with less than $10 million in gross annual receipts.

The No Regulation without Representation Act (H.R. 2887, 115th Congress), also sponsored by Rep. Sensenbrenner, requires that a business have a physical presence before a state can regulate it. Reestablishing the physical nexus principle would be an important step toward righting the ship on extraterritorial actions at the state level. Legislation codifying into law a physical presence standard similar to that embodied in the *Quill* precedent is also sensible.

Polling shows that attempts to expand sales taxes on the Internet remain unpopular among Americans, especially among young adults. A March 2018 poll from the National Taxpayers Union found that 65 percent of Americans opposed an Internet sales tax.

Attempts to expand states' ability to tax online sales outside their borders are unpopular with voters and fly in the face of fiscal conservative principles. By contrast,

an origin-based sales tax approach would address the inequities of the current regime without any of the negative consequences of allowing state governments to tax nonresidents.

Experts: Ryan Radia, Wayne Crews, Jessica Melugin

For Further Reading

Jessica Melugin, "The Marketplace Fairness Act Would Create a State Sales Tax Cartel and Hurt Consumers," *OnPoint* No. 180, Competitive Enterprise Institute, July 30, 2012, https://cei.org/onpoint/marketplace-fairness-act-would-create-state-sales-tax-cartel-and-hurt-consumers.

Jessica Melugin, "Understanding an Internet Sales Tax: A Primer on Leading Proposals and the Political State of Play," *Web Memo* No. 31, Competitive Enterprise Institute, November 30, 2015, https://cei.org/content/understanding-internet-sales-tax.

Jessica Melugin, "How Amazon Wins if Internet Sales Tax Goes Into Effect," CNBC.com, April 3, 2018, https://cei.org/content/how-amazon-wins-if-internet-sales-tax-goes-effect.

Jessica Melugin, "The Real Reason Amazon Flip-Flopped on Internet Sales Taxes," Forbes.com, June 3, 2013, http://www.forbes.com/sites/realspin/2013/06/03/the-real-reason-amazon-flip-flopped-on-internet-sales-taxes/#47eb8301104b.

Jessica Melugin, "Supreme Court's Wayfair Decision Will Hurt Online Shopping," *New York Times*, June 21, 2018, https://www.nytimes.com/2018/06/21/opinion/supreme-court-wayfair-south-dakota-online-shopping.html.

Jessica Melugin and Jonathan Williams, "Online Sales Taxes Won't Solve States' Budget Problems," *Washington Examiner*, June 12, 2018, https://www.washingtonexaminer.com/opinion/op-eds/online-sales-taxes-wont-solve-states-budget-problems.

Michael S. Greve, *Sell Globally, Tax Locally: Sales Tax Reform for the New Economy* (Washington: AEI Press, 2003).

Michael S. Greve, Testimony submitted to the U.S. Senate Committee on Finance on Internet Sales Taxation, August 1, 2001, http://www.finance.senate.gov/imo/media/doc/080101mgtest.pdf.

"The Internet Sales Tax Rush: Harry Reid and Wal-Mart Hope Nobody Will Notice Their Online Revenue Raid," *Wall Street Journal*, Editorial, April 21, 2013, http://www.wsj.com/articles/SB10001424127887324493704578432961601644942.

National Taxpayers Union, "Poll: Strong Opposition to Internet Sales Tax Schemes Across Partisan, Ideological Lines," March 14, 2018, https://www.ntu.org/library/

doclib/Poll-Strong-Opposition-to-Internet-Sales-Tax-Schemes-Across-Partisan-Ideological-Lines.pdf.

Ryan Prete, "Many State Online Sales Tax Laws Leave Door Open for Retroactivity," BloombergTax, July 3, 2018, https://www.bna.com/state-online-sales-n73014477104/.