Technology *and* Telecom

FREE *to* PROSPER

A Pro-Growth Agenda for the 115th Congress

COMPETITIVE ENTERPRISE INSTITUTE

Technology and Telecommunications

6

Few economic sectors rival the technology and telecommunications industries in 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, while the World Wide Web had not yet been invented. Today, mobile devices outnumber people—and nearly one in two people uses the Internet. Massive investment in information technology and infrastructure has fueled innovation, enabling global productivity to grow tremendously, creating tens of millions of high-skilled jobs around the world, and making our lives better in ways few could imagine two decades ago.

As technology evolves, new challenges invariably arise, including for policy makers. Setting the wrong 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 rules to eliminate legal obstacles to innovation. And as history has shown, most concerns expressed 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. To the extent that new services or tools raise legitimate concerns about public health, consumer protection, or competition, lawmakers should resist the urge to act until they see how voluntary institutions—including not only the marketplace but also the rest of 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 schemes devised in an earlier era—especially when such schemes are administered by independent agencies, many of which are pulling out all the stops to remain relevant in a world where they no longer have a useful role to play.

PROTECT INTERNET FREEDOM AGAINST BURDENSOME NET NEUTRALITY MANDATES

Since the 1990s, the Internet has transformed global commerce, with American companies leading the way in developing better ways to harness the Internet's power and 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 era of freedom appears to be coming to an abrupt end. On the infrastructure side, a decade-long effort by federal regulators to dictate business models to companies that provide broadband Internet access to consumers appears to have finally succeeded, pending a last-ditch legal challenge or action by Congress. Firms that operate websites, apps, and mobile platforms have managed to evade a similar crackdown so far, but the early indicators portend a similar fate across the Internet's several layers.

Since taking off in the 1990s, the Internet has flourished as a platform for free expression, innovation, and experimentation—a trend that, until very recently, showed no signs of slowing down. One might assume that federal agencies, having witnessed this success story, would refrain from regulatory intervention. Unfortunately, in recent years, the Federal Communications Commission (FCC) has abandoned its restrained approach, attempting time and time again to expand its reach over the Internet. This effort initially focused on the principle of "net neutrality," which holds that broadband providers should be barred from blocking or offering paid prioritization to time-sensitive Internet traffic—such as videoconferencing or online gaming—upon the request

Congress should:

- Classify the provision of broadband Internet access to consumers—whether wirelessly or by wire—as an information service not subject to common-carrier regulation under the Communications Act of 1934.
- 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 specifically afforded to the agency by the Act, reversing the D.C. Circuit's contrary holding in *Verizon v. FCC*, 740 F.3d 623, 637–40 (D.C. Cir. 2014).
- 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.

of either broadband subscribers or companies that sit at the "edge" of the network. The FCC's actions have since revealed that the agency's true intentions go far beyond net neutrality.

Over 20 years have elapsed 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 the 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 FCC is empowered to regulate providers of telecommunications services as common carriers, subjecting them to obligations ranging from mandatory interconnection to price regulation. (See Federal-State Joint Board on Universal Service, "Report to Congress," 13 FCC Rcd 11501, 11534–35, para. 69 and n.140, 1998.)

In the aftermath of the 1996 Act's passage, the FCC adopted a relatively humble approach to regulating the Internet. In a proceeding launched by the FCC under Clinton-appointed Chair William Kennard and completed under Bush-appointed Chair Michael Powell, the FCC concluded in 2002 that broadband delivered by cable television companies was an information service, not a telecommunications services, and therefore it 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 Ass'n 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," which were local telephone providers once part of AT&T before its 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 whom, like the Baby Bells themselves, had started offering broadband Internet access over telephone wires using a technology known as the digital

subscriber line. 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, but it also meant they no longer had to share their private property with broadband rivals.

For a time, wireline broadband providers operated outside of 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 were 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 attempt, 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—even though the D.C. Circuit accepted the agency's argument that Section 706 of the 1996 Telecommunications Act conferred on the FCC an independent source of authority for certain types of regulation (*Verizon v. FCC*, 740 F.3d 623 [2014]). 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 President Obama's administration to influence the FCC—a putatively "independent" agency—Democratic Chair 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, 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 re-

classify Internet access 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.

Meanwhile, the FCC has embarked on a regulatory voyage using its proclaimed authority, intervening in ways that have little to do with net neutrality. Most notably, in 2016, the FCC launched a proceeding to regulate the privacy practices of Internet service providers, proposing rules designed to dictate how providers use information related to their subscribers' Internet usage. The agency's proposal risks curtailing the ability of broadband providers to offer consumers lower prices in exchange for targeted advertising, and it would generally make it costlier for broadband companies to do business. Indeed, as the FCC's ambition has grown, investment by providers has stagnated.

If the FCC continues on its current path, its agglomeration of powers will eventually transform the agency into an Internet regulation commission. As companies increasingly offer both facilities-based and edge services, as Google and Verizon already do, it seems unlikely that the FCC will resist the temptation to micromanage the terms by which Internet service providers and companies at the edge do business with one another.

Experts: Ryan Radia, Clyde Wayne Crews Jr.

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), pp. 497–519, http://faculty.chicagobooth.edu/dennis.carlton/research/pdfs/NetNeutrality ConsumerWelfare.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: University of Michigan Press, 1997).

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/.

Philip J. Weiser, "The Future of Internet Regulation," *University of California-Davis Law Review,* Vol. 43 (2009), pp. 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 ICLE, July 15, 2014, pp. 32–46, *Protecting and Promoting the Open Internet, FCC GN* Docket No. 14-28, https://ecfsapi.fcc.gov/file/7521706377.pdf.

OPPOSE TAXATION OF INTERNET ACCESS AND E-COMMERCE

Large brick-and-mortar retailers are urging Congress to pass the Marketplace Fairness Act (S. 698 in the 114th 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 online retail industry, which has benefited 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.

Congress should:

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

Experts: Jessica Melugin, Ryan Radia, and Clyde Wayne Crews Jr.

For Further Reading

Joseph Henchman, "The Marketplace Fairness Act: A Primer," *Background Paper* No. 69, Tax Foundation, July 14, 2014, http://taxfoundation.org/article/marketplace-fairness-act-primer.

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

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 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 government entities, from local law enforcement to federal intelligence agencies, have at their disposal a powerful arsenal of technological and legal means for accessing our communications and our metadata—that is, 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 the U.S. government collects about its citizens is staggering.

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. 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, Pub. L. No. 99-508, Title II, 100 Stat. 1848 [1986]; codified as amended at 18 U.S.C. §§ 2701–10

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. 699 in the 114th Congress).
  - Tracking the location of a U.S. person's mobile communications device.

[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 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 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 U.S.C. § 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 U.S.C. § 2703[a]).

In 1986, when Congress crafted this law, the distinction between opened and unopened email—and that between communications and other information stored electronically online—made sense, given the state of technology at the time. In 2016, however, Americans reasonably assume that their digital "papers and effects" are safe from warrantless government access—an often inaccurate assumption.

To remedy this 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. 699 in the 114th

Congress), which already enjoys 314 cosponsors in the House—including most Republicans and several Democrats. 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 because of an apparent emergency involving an imminent threat to human life, such as the kidnapping of a child.

Experts: Ryan Radia, Clyde Wayne Crews, Jr.

For Further Reading

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.

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

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 those 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, 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, and lawsuits are filed by trial attorneys in the business of finding purportedly injured classes of people to represent.

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 this externality does not

Congress should:

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

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, 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.

Experts: Ryan Radia, Clyde Wayne Crews, Jr.

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), 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.

Tyler Moore, "Introducing the Economics of Cybersecurity: Principles and Policy Options" in *Proceedings of a Workshop on Deterring Cyberattacks* (Washington, DC: National Academies Press, 2010), pp. 3–24, https://www.nap.edu/catalog/12997/proceedings-of-a-workshop-on-deterring-cyberattacks-informing-strategies-and.

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/.

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

OPPOSE BURDENSOME INTERNET SALES TAXES

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 are 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.

Currently, under the Supreme Court's decision in *Quill v. North Dakota* (1992), a seller must have a physical presence, or "nexus," in the buyer's state to 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 this 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, several state and local governments and big-box retailers are lobbying Congress and the administration to enact in the Marketplace Fairness Act (MFA) and Remote Transaction Parity Act (RTPA), both of which would (a) impose burdensome—in some cases lethal—compliance costs for small and midsize sellers, (b) reduce interstate tax competition, (c) decrease political accountability in cross-border audits, and (d) subject consumers to potential privacy violations.

The Marketplace Fairness Act (MFA) 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 would also subject businesses to audits by out-of-state tax authorities. It would lessen downward pressure on sales tax rates from tax competition and would threaten consumer privacy through states' data sharing.

The Remote Transaction Parity Act, introduced in the 114th Congress by U.S. Rep. Jason Chaffetz (R-Utah), adopts the same approach as the MFA, by giving 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-

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.

state audits, the RTPA creates an option for sellers to use state-employed tax compliance agents. It attempts to protect sellers with gross receipts under $5 million from being audited by other states, but it 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 and subsequent years, it drops to $1 million.

In August 2016, House Judiciary Committee Chair 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 businesses in states with no sales tax to collect and remit sales taxes, thereby compromising those states' autonomy.

While Congress debates the issue, many states have taken it upon themselves to expand the definition of nexus in order to trigger sales tax collection. Those attempts are working their way through the courts with varying results and are likely to continue until Congress acts.

Polling shows that attempts to expand sales taxes on the Internet remain unpopular in the U.S., especially among young adults. A 2013 Gallup poll found 57 percent of

all adults opposed an Internet sales tax, whereas 73 percent of 18- to 29-year-olds opposed one.

Proponents of MFA-style legislation include state and local governments and the associations that represent them. Expanded sales tax collection would be a boon to their coffers and would spare them from politically unpopular budget cuts. Big-box retailers with a physical presence that triggers sales tax obligations in every state stand to gain a competitive advantage from the MFA's disproportionate compliance cost burdens on smaller retailers.

Attempts to expand states' ability to tax online sales outside their borders are wildly unpopular with voters and fly in the face of constitutional principles of federalism. 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: Jessica Melugin, Ryan Radia

For Further Reading

Jessica Melugin, "Facts on the Marketplace Fairness Act (S. 743, formerly S. 336)," *Web Memo* No. 20, Competitive Enterprise Institute, April 18, 2013, https://cei.org/web-memo/facts-marketplace-fairness-act-s-743-formerly-s-336.

———, "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.

———, "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.

———, "Understanding an Internet Sales Tax," *Web Memo* No. 31, Competitive Enterprise Institute, November 20, 2015, https://cei.org/content/understanding-internet-sales-tax.

Michael S. Greve, Testimony on "Internet Sales Taxation" 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.

———, *Sell Globally, Tax Locally: Sales Tax Reform for the New Economy* (Washington, D.C.: AEI Press, 2003).

———, "The Internet Sales Tax Rush," editorial, *Wall Street Journal*, April 21, 2013, http://www.wsj.com/articles/SB10001424127887324493704578432961601644942.

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 Instant Video, and HBO Now. 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. Those outdated rules not only undermine the vitality of traditional media businesses, they also threaten the future of Internet-based television services.

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 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 those fees are not retained by each local station. Instead, stations are typically 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, each 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

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.

Office distributes those fees to the copyright owners whose works were distributed by the television company.

In contrast to this 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 the Copyright Office are required. No government fee schedule must be examined. 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 and movies disappear from the company's library and are replaced by new ones. 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 in many cases distort—the market for television programs distributed by cable and satellite companies. Title VI of the Communications Act contains myriad rules governing 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 *House of Cards* and Amazon's *The Man in the High Castle*. In fact, the FCC has even suggested that it might reinterpret the Communications Act in such a way 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, the newspaper industry has lost billions of dollars in revenue and millions of subscribers. In many cities, iconic newspapers have ceased printing a daily edition or have 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 media outlets with more funding, personnel, and other resources.

Experts: Ryan Radia, Clyde Wayne Crews, Jr.

For Further Reading

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

"Comments of CEI, ICLE, and TechFreedom to the FCC 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.

UPDATE COPYRIGHT FOR THE INTERNET AGE

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 of 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 that would better protect creative works from infringement.

Article I of the U.S. Constitution empowers Congress to "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; codified as amended at 17 U.S.C. §§ 101–810). For the most part, this regime works well, enabling artists who create popular works to earn a return on their efforts. From television shows and movies to music, the United States is home to many of the world's most celebrated artists and creative industries.

But 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 over-

Congress should:

Amend the U.S. Copyright Act to

- Ban tools that circumvent technological protection measures only if they are likely to undermine the value of the underlying creative works they seek to protect.
- 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.
- Enhance 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 online content.

broad. Although effective DRM can be invaluable, 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 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, in the case of firms that distribute tools 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 upon 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. §§ 302–4). People eventually die, of course, whereas corporations are regularly acquired or cease to exist. Yet many works created by deceased persons or defunct corporations remain subject to copyright protection, making it difficult or impossible to ascertain who holds the copyright in such works. Companies that wish to monetize and distribute these 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 this reform 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.

Creators seeking to prevent the infringement of their works on the Internet 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 that 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 upon receiving notification from a copyright owner regarding the unauthorized work. Although this system has proved 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 examining such reforms, however, lawmakers should resist calls to impose technological mandates on online service providers that could materially 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, Clyde Wayne Crews, Jr.

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* 12, No. 1 (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* 71, No. 1 (2004): 37–56.

COMPETITIVE ENTERPRISE INSTITUTE

The Competitive Enterprise Institute promotes the institutions of liberty and works to remove government-created barriers to economic freedom, innovation, and prosperity through timely analysis, effective advocacy, inclusive coalition-building, and strategic litigation.

COMPETITIVE ENTERPRISE INSTITUTE
1310 L Street NW, 7th Floor
Washington, DC 20005
202-331-1010
cei.org