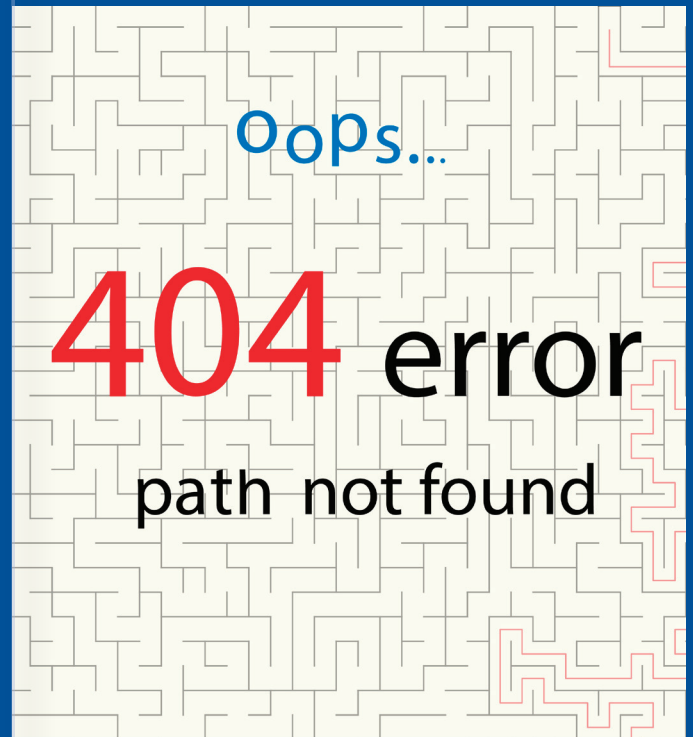


Terrible Tech 2.0

The Most Burdensome, Anti-Consumer Technology Policy Proposals in Washington

*By Jessica Melugin,
Clyde Wayne Crews Jr.,
Iain Murray, Patrick Hedger,
Ryan Young, and John Berlau*

September 2020



ISSUE ANALYSIS 2020 NO. 6

Terrible Tech 2.0

The Most Burdensome, Anti-Consumer Technology Policy Proposals in Washington

By Jessica Melugin, Clyde Wayne Crews Jr., Iain Murray, Patrick Hedger, Ryan Young, and John Berlau

Executive Summary

If you are looking for bipartisanship in Washington, D.C., the technology policy sector may be your best bet—but not in a good way. There is a bipartisan impulse to exercise control over the Internet, apps, devices, and the algorithms and artificial intelligence that make them possible. This bipartisan “consensus” seeks to replace the hands-off approach that has been mostly prevalent since the Internet’s inception with one of greater government control.

While regulatory agencies, rather than Congress, do much of the lawmaking these days, Congress has become ambitious about extending its power over the tech sector. This report spells out how dangerous these ambitions are. Executive and independent agencies have their own plans for encroaching on the Internet. The favorability toward expansion of the administrative state by Republicans in particular—under a supposedly deregulatory Trump administration—heightens the urgency, and demands a fresh look.

This report was inspired by an earlier report, “The Digital Dirty Dozen: The Most Destructive High-Tech Legislative Measures of the 107th Congress” by Wayne Crews and Adam Thierer. As was the case with the original “Digital Dirty Dozen” report, the trend toward interventionist policies threatens to lead to legal and regulatory uncertainty for entrepreneurs and potential public harm. That has resulted in new legislation and regulation covering the Internet sector.

To date, a hands-off regulatory approach has helped fuel an explosion in broadband access innovation, and, barring interference from regulators, will allow a 5G Internet to make a large positive impact on the world. But, unfortunately, there are now dozens of

proposed technology-related bills in Congress that threaten to expand the government’s reach. Not as paradoxically as it might seem, many big tech companies—seeing their market position as secure and desiring predictability—often support regulation.

This paper highlights numerous categories of interventionist policies, focuses on some of the most destructive legislative offerings within each category, and settles on the ones we consider to be the worst.

These bills address broadband deployment and access, antitrust and competition policy, bias and content controls, child protection, cybersecurity, and more. Some are retreads, like those on online marketing and privacy. There are measures to increase antitrust intervention and to regulate “biased,” “harmful,” and other forms of speech.

The 115th Congress narrowly modified Section 230 of the Communications Decency Act with respect to human trafficking. Now both parties contemplate something more like a purge of Section 230. Section 230 allows social media networks to moderate their content without being held to the liability standards of a traditional publisher or a speaker. It protects platforms from lawsuits about third-party posts by recognizing that these hosts do not supply content like a newspaper or the content’s creator does. This enables the mostly permissionless, user-driven Internet experience we enjoy online today. Without this safeguard, platforms would have to vet the enormous amount of user-driven content before displaying it because of the increased liability they would assume. This would be prohibitively time-consuming and expensive. Alternatively, and ironically for conservative critics of Section 230, platforms could take a completely hands-off approach

to curating content, but the results would likely be too violent, pornographic, or offensive to attract many eyeballs.

There are also attempts to set standards for privacy and online advertising and to address online “addiction” and hold companies accountable for it. Some seek to bring the gig economy into the regulatory maze of labor law. Meanwhile, the Federal Reserve and the Securities Exchange Commission may seek to assert their authority over the payments processing sector just as cryptocurrencies are beginning to emerge.

The pressure to regulate has intensified thanks to the emergence of two other powerful regulatory centers that are vying with America to set the gold standard for global technological regulation. While the U.S. has traditionally aimed at empowering technology users, it faces competition from two different models. The European Union aims to protect technology users in paternalistic fashion. China wants to control how people use technology. For a global industry, regulations imposed by jurisdictions that encompass a large percentage of global population and GDP will affect American companies and consumers.

We argue instead for innovation and the separation of technology and state. Policy makers, including Republicans, must pay special attention to how these various proposals would expand invasive administrative

bodies like the Federal Trade Commission, the Federal Communications Commission, the Securities and Exchange Commission, and other agencies.

Old-school telecommunications, transportation, and infrastructure have long been highly regulated, with government-supported monopoly in some instances. The Internet still offers an opportunity to show that spontaneous order can work to serve consumers and society better than lawmakers.

Market solutions, unlike legislation, better lend themselves to address the myriad problems that inevitably arise in a free, competitive economy. The Internet was not initially designed as the mass commercial and consumer medium it is today.

There is a role for law. Fraud, falsification, identity theft, hacking, and the like should be punished, but overly burdensome legislation will create legal and regulatory obstacles for small businesses—a reason some large firms favor intervention—and the development of newer technologies and services, which is one of the great hidden costs of regulation.

Bad legislation lays the groundwork for worse legislation later. Embracing regulation and central planning entail embracing collective “solutions” that will be difficult to correct later. The legislation we actually need would be a bill to prevent many of these misguided proposals.

Introduction

If you are looking for bipartisanship in Washington, D.C., the technology policy sector may be your best bet—but not in a good way. There is a bipartisan impulse to exercise control over the Internet, apps, devices, and the algorithms and artificial intelligence that make them possible. This bipartisan “consensus” seeks to replace the hands-off approach that has been mostly prevalent since the Internet’s inception with one of greater government control.¹

While regulatory agencies, rather than Congress, do much of the lawmaking these days, Congress has become ambitious about extending its power over the tech sector.² This report spells out how dangerous these ambitions are. Executive and independent agencies have their own plans for encroaching on the Internet. The favorability toward expansion of the administrative state by Republicans in particular—under a supposedly deregulatory Trump administration³—raises the urgency further, and demands a fresh look.⁴

This report was inspired by an earlier report, “The Digital Dirty Dozen: The Most Destructive High-Tech Legislative Measures of the 107th Congress” by Wayne Crews and Adam Thierer. As was the case with the original “Digital Dirty Dozen” report, the trend toward interventionist policies threatens to lead to legal and regulatory

uncertainty for entrepreneurs and potential public harm. That has resulted in new legislation and regulation covering the Internet sector.

In the recent past, court decisions also have played a role. For example, in 2018 the Supreme Court, reversing precedent, greatly expanded the power of state governments to tax beyond their borders when it gave the go-ahead to the remote taxation of goods purchased online. Of course, there also have been more encouraging court decisions. For example, the D.C. Circuit Court of Appeals recently upheld the Federal Communications Commission’s (FCC) repeal of net neutrality regulations.⁵

To date, a hands-off regulatory approach has helped fuel an explosion in broadband access innovation, and, barring interference from regulators, will allow a 5G Internet to make a large positive impact on the world. But, unfortunately, there are now dozens of proposed technology-related bills in Congress that threaten to expand the government’s reach. Meanwhile, tech industry critics complain that we are becoming addicted to our handheld devices and warn that the computer that beat the world champions at the strategic boardgame, Go, will steal our jobs next.⁶

While the FCC has successfully worked to roll back Obama-era net

*If you are
looking for
bipartisanship
in Washington,
D.C., the
technology
policy sector
may be your
best bet—but
not in a
good way.*

Some seek to bring the gig economy into the regulatory maze of labor law.

neutrality rules that would regulate the Internet as a public utility, some of the same Big Tech or FAANG—Facebook, Amazon, Apple, Netflix, Google⁷—companies that pushed for net neutrality rules are facing calls from both the left and right for regulation of online content standards on online platforms. Not as paradoxically as it might seem, many big tech companies—seeing their market position as secure and desiring predictability—often support regulation.

This report highlights numerous categories of interventionist policies, focuses on some of the most destructive legislative offerings within each category, and settles on the ones we consider to be the worst.

These bills address broadband deployment and access, antitrust and competition policy, bias and content controls, child protection, cybersecurity, and more. Some are retreads, like those on online marketing and privacy.⁸ There are measures to increase antitrust intervention and to regulate “biased,” “harmful,” and other forms of speech. Many of these proposals center on “reform” of the “sixteen words that created the Internet.”⁹

As Box 1 shows, the 115th Congress narrowly modified Section 230 of the Communications Decency Act with respect to human trafficking.¹⁰ Now both parties contemplate something more like a purge of Section 230.¹¹

Section 230 allows social media networks to moderate their content without being held to the liability standards of a traditional publisher or a speaker.¹² It protects platforms from lawsuits about third-party posts by recognizing that these hosts do not supply this content like a newspaper or the content’s creator. This enables the mostly permissionless, user-driven Internet experience we enjoy online today.

Section 230 applies even if a platform has content standards and acts to remove materials in violation of those rules. Without this safeguard, platforms would have to vet the enormous amount of user-driven content before displaying it because of the increased liability they would assume. This would be prohibitively time-consuming and expensive. Alternatively, and ironically for conservative critics of Section 230, platforms could take a completely hands-off approach to curating content, but the results would likely be too violent, pornographic, or offensive to attract many eyeballs.

There are also attempts to set standards for privacy and online advertising and to address online “addiction” and hold companies accountable for it. Some seek to bring the gig economy into the regulatory maze of labor law. Meanwhile, the Federal Reserve and the Securities Exchange Commission may seek to assert their authority over

the payments processing sector just as cryptocurrencies are beginning to emerge.

Fortunately, it is still hard to pass laws. But overseas courts and legislators are hard at work at dismantling the open social media ecosystem.¹³ The pressure to regulate has intensified thanks to the emergence of two other powerful regulatory centers that are vying with America to set the gold standard for global technological regulation. While the U.S. has traditionally aimed at empowering technology users, it faces competition from two different models. The European Union aims to protect technology users in paternalistic fashion. China wants to control how people use technology. A survey of the various regulatory initiatives undertaken by these administrative rivals is beyond the scope of this paper, but for a global industry, regulations imposed by jurisdictions that encompass a large percentage of global population and GDP will affect American companies and consumers.¹⁴

We argue instead for innovation and the separation of technology and state. The longest journey does not merely begin with a single step; it requires not stepping backward. In the present instance, that means not enacting misguided laws and regulations. Policy makers, including Republicans, must pay special attention to how these various proposals would expand invasive administrative bodies like the Federal Trade Commission (FTC), the Federal Communications Commission, the Securities and Exchange Commission (SEC), and other agencies.

BOX 1. Major Pieces of Internet Legislation Passed Since the Heyday of AOL and Netscape.

Deregulatory

- The **Telecommunications Act**, the first significant update to telecommunications law since the 1934 Communications Act,¹⁶ created the “information services” classification, separate from telephone and cable services and not subject to regulations governing either.¹⁷
- **Section 230 of the Communications Decency Act** largely protects websites from liability over content created by third-party users, creating a safe harbor for websites that choose to moderate content. Prior to Section 230, any attempts to moderate content meant platforms could be held liable for all user-generated content.
- **Title II of the Digital Millennium Copyright Act** provides a safe harbor for Internet service providers, including websites, against liability for digital copyright infringements by third-party users. Providers must meet certain conditions to qualify for protection.¹⁸

Regulatory

- The **Children’s Online Privacy Act** prohibits websites and online services that are either directed at children or collect personal information of children under a certain age before meeting several conditions.¹⁹
- The **Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act** governs commercial emails. Among other provisions, CAN-SPAM prohibits deceptive email subject lines, requires identifying information for the sender, and mandates an opt-out feature for recipients. It preempts state laws relating to commercial email, aside from those covering fraudulent or deceptive content.²⁰
- The **Fight Online Sex Trafficking Act** scales back Section 230 immunity in several areas related to online content regarding prostitution and sex trafficking.²¹

Which will prevail, innovation or the central directives of the regulatory state?

Old-school telecommunications, transportation, and infrastructure have long been highly regulated, with government-supported monopoly in some instances. The Internet still offers an opportunity to show that spontaneous order can work to serve consumers and society better than lawmakers. Which will prevail, innovation or the central directives of the regulatory state?¹⁵

The Bleak Litany of Restrictive Proposals

In this report, we identify specific legislative or regulatory proposals that raise alarm bells. We also identify broad categories of control of which these proposals are examples. The report also stresses how a large administrative state grows at the expense of First Amendment rights, property rights, and free enterprise.

An “Internet Bill of Rights”: Proposals that Conflate Public and Private Spheres and Ignore the Dichotomy between Positive and Negative Rights

The concept of “Internet Exceptionalism” is a common theme across these proposals. It postulates that the Internet is a unique kind of technology that requires new conceptions of law and economics.²² For example, Professor Tim Wu of Columbia University, famous for popularizing the concept

of “net neutrality,” recently said that tech companies “had reinvented economics, reinvented business as we knew it.”²³ This prism of novelty allows for a circumventing of norms surrounding the concept of rights in the United States. Instead of rights guaranteed to all private actors by restrictions on government through a negative rights framework, tech utopians advocate for positive rights guaranteed by government, provided at the expense of private companies and their consumers.

Under this vision, Internet users have entitlements, while those who help make the easy-to-use commercial Internet possible in the first place have obligations that supersede their own rights. As part of the lay of the land of the tech policy debate, we see longstanding calls for a “Magna Carta” or “new contract” for the Web from pioneer Sir Tim Berners-Lee.²⁴ Worried about “fake news” and data protection,²⁵ he has called for breaking up the tech giants.²⁶ Such sentiments are shared by U.S. legislators like Rep. Ro Khanna (D-CA), who have devised versions of a highly regulatory Internet Bill of Rights, using terminology conflating public and private spheres.²⁷ Conservatives have proposed their own versions of this folly, largely in the area of content regulation.

Yet, if lawmakers were to undermine the negative-rights framework in

regards to the Internet, we will lose the kind of rapid progress that has made the Internet seem “exceptional.” Imposing positive rights obligations upon Internet service providers and platforms would result in a significant drop-off in investment and innovation in the sector. It is not hard to understand why.

Positive rights require that resources are allocated in specific ways. If resources must be allocated in certain ways, then companies and their investors no longer enjoy complete property rights, which are integral to investment. Positive rights also create a drain on available resources. Like burning a candle at both ends, positive rights obligations on firms limit the resources available for risk-taking, the key to innovation.

The impetus behind an Internet bill of rights is at least nominally pro-consumer. Yet, as economist Milton Friedman said, “One of the great mistakes is to judge policies and programs by their intentions rather than their results.”²⁸ While some users may find value in the various prescriptive guarantees, if the majority of consumers truly valued the protections or guarantees of an Internet bill of rights, the market would already be providing these features. Yet, as the data show, users actually place little value in such features.

Rep. Khanna’s Internet Bill of Rights primarily seeks to protect data privacy, with six out of 10 provisions related to data collection. When asked, Americans certainly want companies to do a better job in protecting data privacy. However, economics teaches us that human wants are limitless and what truly matters is how people value something relative to the alternatives. According a recent survey of over 3,000 American Internet users, only 26 percent said they would be willing to pay a monthly subscription fee for greater privacy protection.²⁹ Many services already provide this privacy for a small fee, and in some cases for free.³⁰ Apple recently made the privacy features of its iPhone line a major facet of its advertising campaigns. Privacy-centric search engine DuckDuckGo has grown from approximately 16 million queries in 2010 to more than 15 billion in 2019.³¹

Consumers should be free to select the products and services that best meet their privacy needs and provide the best results. Imposing positive rights obligations on the Internet sector would reduce investment and innovation. Consumers would ultimately have fewer choices in exchange for “rights” that the vast majority of consumers may not value all that much. The \$50 smartphone makes the technology available to all, at the cost of privacy. When regulation produces fewer

*Like burning a
candle at both
ends, positive
rights obligations
on firms limit
the resources
available for
risk-taking,
the key to
innovation.*

*Section 230
is largely
responsible
for the Internet
as we know
it today.*

options in the market and a lack of investment in new competition, consumers are worse off at the margin, as they lack realistic alternatives to punish companies by taking their business elsewhere.

This is why the U.S. Bill of Rights places restrictions on government and not on private actors. The market is highly responsive to what consumers value, with consumers voting countless times every second with their attention, feet, and wallets; firms grow when they provide what people value. Government, on the other hand, faces no competition, is only rarely held to account, and tends to grow unimpeded.

Censorship of Social Media Content and Bias

The safe harbor provided by Section 230 of the Communications Decency Act is a major reason why America leads the world in online technology

investment and innovation.³² Section 230 protects tech platforms from liability over content posted by third-party users. For example, if a person posts a libelous Facebook status about you, only the person who posted it, not Facebook, is legally responsible for the content.

While critics of Section 230 exist on both sides of the aisle for various reasons, the law is largely responsible for the Internet as we know it today. Without it, platforms—from online marketplaces, to social media to review sites—would either be unmoderated cesspools or simply would not exist as largely free and open to users. Prior to Section 230, any attempts to moderate content meant platforms could be held liable for all user-generated content. Section 230 addresses the impracticality and excessive risk of assuming liability for all the countless pieces of content

Where The World's Largest Tech Companies Are

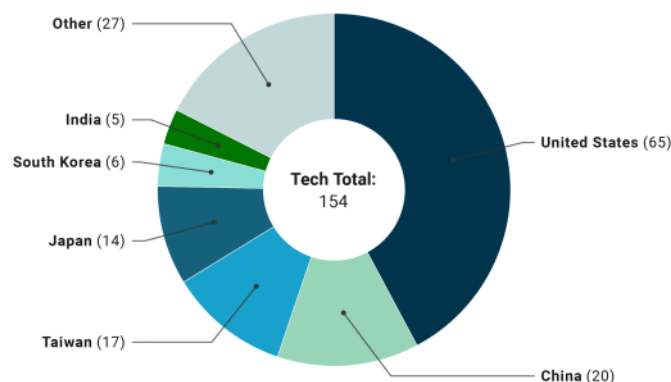


Image via Jonathan Ponciano, "The Largest Technology Companies In 2019: Apple Reigns as Smartphones Slip and Cloud Services Thrive, Forbes, May 15, 2019, <https://www.forbes.com/sites/jonathanponciano/2019/05/15/worlds-largest-tech-companies-2019/#21e4b2bc734f>.

The 10 Largest Tech Companies in the World

Rank	Company	Country	Market Value*	Assets*
1	Apple	United States	961	374
2	Samsung Electronics	South Korea	272	304
3	Microsoft	United States	947	259
4	Alphabet	United States	863	233
5	Intel	United States	263	128
6	IBM	United States	125	131
7	Facebook	United States	512	97
8	Cisco Systems	United States	248	102
9	Tencent Holdings	China	472	105
10	Oracle	United States	186	109

*In billions of U.S. dollars

Image via Jonathan Ponciano, "The Largest Technology Companies In 2019: Apple Reigns as Smartphones Slip and Cloud Services Thrive, Forbes, May 15, 2019, <https://www.forbes.com/sites/jonathanponciano/2019/05/15/worlds-largest-tech-companies-2019/#21e4b2bc734f>.

uploaded by users by granting tech companies the ability to moderate content as they see fit.

Meanwhile, conservatives accuse tech giants of using content moderation under Section 230 to promote online bias and censor right-leaning voices, and in response they seek compulsory redress. Yet, the Internet is actually one of the few realms, like talk radio, not dominated by left-leaning views, and the drive to change that is at the root of some liberals' calls to regulate it.³³ Still, right and left agree on one thing: The federal government should lord over speech, with the First Amendment's free speech guarantees thrown by the wayside. Instead of a free online marketplace of ideas, we would get one regulated by agencies like the Federal Trade Commission.

One side would partner with government to ban "harmful speech," while the other would compel and then certify political neutrality. Some companies cater to this mindset, glossing over the distinction between government and private parties.³⁴ Collectively, all ignore the fact that, as noted, First Amendment speech and association rights are negative rights that constrain the government, not private parties, from restricting or compelling your speech.

1. The Ending Support for Internet Censorship Act, sponsored by Sen. Josh Hawley (R-MO) would require "tech companies to moderate content without political bias as a condition of civil immunity."³⁵ This policy would deny property rights, compel speech,

*First Amendment
speech and
association rights
are negative
rights that
constrain the
government, not
private parties,
from restricting
or compelling
your speech.*

The definition of a Good Samaritan is subjective, as are the definitions of what would constitute “bad actors” or “abuse” in regard to Section 230.

and add considerably to an already large administrative state bureaucracy. In order to retain immunity from liability for user-generated content under Section 230, a “covered company” would have to obtain an “immunity certification” every two years from the FTC by assuring a majority of the (unelected) commissioners that it does not moderate content provided by others in a politically biased way.³⁶

It also mandates arbitrary thresholds regarding which parties it would regulate. A “covered company” needing objectivity certification would be one with more than 30 million active U.S. monthly users, 300 million worldwide users, or \$500 million or more in annual global revenue. Along with the false premise of private censorship in the bill’s title, one cannot prove the negative of non-bias, so the bill is inoperable and susceptible to partisan disputes over the meaning of objectivity. That is a battle that conservative proponents will ultimately lose, since what will be regarded as politically objective by a future FTC will not necessarily match Hawley’s—and many other conservatives’—vision.³⁷

2. The Limiting Section 230

Immunity to Good Samaritans Act was also introduced by Sen. Hawley.³⁸ To understand this legislation, it is necessary to get an understanding

of Section 230 of the 1996 Communications Decency Act. Part of what makes Section 230 special is not what it does but rather what it does not do. The relatively short law provides “Protection for ‘Good Samaritan’ Blocking and Screening of Offensive Material.”³⁹ The law’s title states as its purpose: “To amend the Communications Act of 1934 to provide accountability for bad actors who abuse the Good Samaritan protections provided under that Act, and for other purposes.” The text does not define the term “Good Samaritan,” which suggests that the law’s authors acknowledge a simple truth: The definition of a Good Samaritan is subjective, as are the definitions of what would constitute “bad actors” or “abuse” in regard to Section 230.

In other words, the Limiting Section 230 Immunity to Good Samaritans Act seeks to accomplish the impossible and define what constitutes being a Good Samaritan, or at least a Web service acting in “good faith.” For Web services that are seen to be acting in bad faith by selectively enforcing their terms of service on content moderation, the bill allows for civil liability of up to \$5,000. Like the Ending Support for Internet Censorship Act, the bill also sets arbitrary thresholds over which entities it covers. Specifically, it outlines that it only applies to services with over 30 million U.S. users, 300 million

global users, or \$1.5 billion in global revenue.⁴⁰

There are several problems with this approach. First, just as the definition of a Good Samaritan is subjective, many decisions on content moderation come down to subjective judgements. The spirit of the bill thus essentially disincentivizes moderation at the margins for fear of exposure to liability. This would mean more offensive and objectionable content online where there was none before.

Second, the bill has a huge loophole that renders it essentially futile. It would allow for Web services to include a right to selectively enforce said terms in their terms of service. As *Gizmodo*'s Dell Cameron notes, "the changes to Section 230 of the Communications Decency Act proposed by Hawley do not appear to place any new restrictions on how companies define their own moderation policies—only that they stick to, and evenly apply, whatever rules they ultimately decide upon."⁴¹

Third, by stipulating that the bill only applies to the largest Web services, it provides an incentive for these services to become even larger and more dominant over online discourse. Upstart competitors approaching any of the bill's three metrics would be incentivized to sell to larger competitors that already exceed those thresholds—

and have the compliance personnel to deal with that.

3. The Stop the Censorship Act, introduced by Rep. Paul Gosar (R-AZ), would limit moderation of "objectionable" content by only granting immunity when companies act in "good faith" to remove "unlawful content."⁴² Under such a regime, companies would be forced to host endless amounts of content against their will—regardless of whether or not they would be deemed in compliance with the impossible non-bias standard in Hawley's bill. This would amount to a violation of the speech and association rights of the covered firms.

Rep. Gosar has frequently made the claim, common among critics of Section 230, that tech companies are unlawfully acting as both a "publisher" and a "platform." In a tweet from September 18, 2019, he wrote: "Facebook makes a judicial admission it is a publisher not a platform. As a publisher it can assert editorial control. But it can also be sued for defamation and tortious interference. Sec. 230 of the CDA protects platforms. Not publishers."⁴³ No part of the actual law makes this distinction.

Professor Jeff Kosseff, a cybersecurity law professor at the U.S. Naval Academy and perhaps the nation's leading expert on Section 230, said on the platform-publisher distinction:

Just as the definition of a Good Samaritan is subjective, many decisions on content moderation come down to subjective judgements.

While cyberspace may seem unlimited, it is not. Tremendous resources are dedicated to hosting all the data uploaded to the Internet.

I'm not quite sure what their parameters are for publisher or platform. Are they saying you don't do any moderation at all? A free for all? I seriously would not want to be on the internet at all if that was the case. ... I don't know where these people are drawing the line between platforms and publishers. All I can say is that Congress, at least at the time, did not intend that distinction.⁴⁴

Yet an Internet Kosseff seriously would not want to be on would be the default setting for tech platforms and other websites under the Stop the Censorship Act, as consumers would be forced to choose to opt in to see or receive moderated content. Should a social media page filled with hateful, violent, and sexually explicit content really be the default setting?

4. The Biased Algorithm Deterrence Act would effectively abolish Section 230 immunities by commanding that:

[A]n owner or operator of a social media service that displays user-generated content in an order other than chronological order, delays the display of such content relative to other content, or otherwise hinders the display of such content relative to other content ... shall be treated as a

publisher or speaker of such content.⁴⁵

This bill literally puts others' words in the platforms' mouths, by declaring the platform to be the speaker. It also mandates a chronological presentation of content. Algorithms that learn what you are interested in are actually useful to readers. Anyone who has tried installing a social media plug-in that forces the display of content in chronological order will know what happens when a friend has uploaded an album of holiday photos—endless scrolling to get to the next interesting item.

These proposals' violations of private companies' speech and association rights alone, not to mention the impossibility of policing objectivity when government agents have plenty of their own biases, render these proposals problematic, to put it lightly. Forcing companies to host content against their will goes beyond simple control over their platforms. There are significant implications for the tangible property of these firms under each of these supposed anti-censorship proposals. While cyberspace may seem unlimited, it is not. Tremendous resources are dedicated to hosting all the data uploaded to the Internet. In 2019, an estimated \$210 billion was spent worldwide on data centers.⁴⁶ Forcing companies to host any and all

lawful content would dramatically increase the physical infrastructure needs of tech platforms, a *de facto* tax of potentially hundreds of billions of dollars.

Ironically, the tremendous resource costs related to hosting content, under these anti-censorship proposals, could lead to forced limiting of online speech due entirely to resource constraints. In this way, all sorts of spam, violent, sexual, and other objectionable content that is otherwise discarded could impose a sort of heckler's veto over the political content Hawley, Gosar, and their allies are trying to protect.

Congress should not stand in judgment of others' acceptable or unacceptable bias or speech. Regardless of all the various legal and practical problems with implementing such policies, progressives have already teed up an abundance of subjective, ill-defined, and open-ended categories of speech to be regulated, including misinformation, disinformation, harmful content, and hate speech.

One likely effect of content restraint would be a clampdown on anonymous speech and criticism of unorthodox views. In fact, in a self-regulatory move, Facebook has decided to allow more political content on the platform in exchange for stricter rules to ensure the true identity of the speaker can be identified.⁴⁷ Moreover, if content rules are good for social media, why they are not also good for government websites, mainstream media, and publicly funded university curricula?

These proposals violate the spirit of the First Amendment by restricting private citizens'

Trial Ballooning a Sweeping Federal Takeover of the Internet

In July 2018, the *Columbia Journalism Review (CJR)* reported on a leaked draft white paper from Sen. Mark Warner (D-VA) that contained a wide-ranging slate of proposals to treat tech companies as essential facilities and to regulate content and speech.⁴⁸

The white paper, titled **"Potential Policy Proposals for Regulation of Social Media and Technology Firms,"** cited anonymity using trolls, misinformation, and election interference as justification. Warner expressed alarm that "bots, trolls, click-farms, fake pages and groups, ads, and algorithm-gaming can be used to propagate political disinformation."⁴⁹ Proposed solutions, which Warner refers to as "guard rails," include:

- Labeling of automated "bot" accounts;
- Requiring location verification;
- Limiting certain elements of anonymity;
- Limiting Section 230 immunity for re-uploaded content;
- Imposing liability for defamation, false light, and deep fakes;
- Audits of tech company algorithms, and
- Defining certain services to be essential facilities.⁵⁰

Reason correspondent Elizabeth Nolan Brown called it "plans for a government takeover of the Internet."⁵¹

The loss of the civil right of anonymous online speech is an unexplored vulnerability in the various social media regulatory campaigns, with Warner leading the charge.⁵² The *CJR*'s Matthew Ingram notes:

When it comes to misinformation, the Warner paper says one possible proposal is that platforms be required to label automated bot accounts, and also do more to identify who is behind anonymous or pseudonymous accounts. If there's a failure to do these things, it says, the Federal Trade Commission could step in with sanctions.⁵³

If companies like Facebook grew thanks to the protections of Section 230, newly formed social media companies have the right to do the same, and politicians the duty not to interfere. Future networks that do not yet exist deserve the same clear path.

The Internet has given individuals power over their speech, providing a platform for both popular and unpopular ideas. It is a good thing that the Internet allows the questioning of orthodoxies and the bypassing of gatekeepers. Yet, attempts are now under way to reestablish gatekeepers. For all the talk of regulating algorithms, such efforts seek to certify government "algorithms" while demonizing those of the private sphere.

In Hawley's perspective, parents are not competent to supervise the purchase of digital weapons for junior's Fortnite game and need the help of the nanny state.

speech and leaving the government not only unshackled, but more powerful.

Helicopter Government: Saving Children from Parents' Failure in the Duty to Supervise Online Activities

5. Sen. Josh Hawley teamed with two Democrats, Sens. Richard Blumenthal of Connecticut and Ed Markey of Massachusetts, to sponsor the **Protecting Children from Abusive Games Act** (S. 1629).⁵⁴ Targeting what he calls the “addiction economy,” Hawley alleges, “When a game is designed for kids, game developers shouldn’t be allowed to monetize addiction.”⁵⁵ And when kids play games designed for adults, they should be walled off from compulsive microtransactions. Game developers who knowingly exploit children should face legal consequences.”⁵⁶ Games would be banned from having loot boxes, defined as “microtransactions offering randomized or partially randomized rewards to players.” (If you ever bought a Cracker Jack box hoping for a good prize, you might be familiar with the concept.) The bill also targets “pay-to-win” mechanics that “manipulate a game’s progression system ... to induce players to spend money.”⁵⁷

The Entertainment Software Association argues that loot boxes do not constitute gambling, and describes

tools the sector provides “that keeps the control of in-game spending in parents’ hands. Parents already have the ability to limit or prohibit in-game purchases with easy to use parental controls.” In Hawley’s perspective, parents are not competent to supervise the purchase of digital weapons for junior’s Fortnite game and need the help of the nanny state.

6. The **Protecting Children from Online Predators Act** (S. 1916), also sponsored by Hawley, would prevent companies like YouTube from recommending videos featuring minors.⁵⁹ As *Reason’s* Elizabeth Nolan Brown describes it:

Teen video makers couldn’t rely on algorithms to recommend any of their content. Sites like Facebook would be prohibited from recommending family videos featuring children to grandma and grandpa.⁶⁰

Relatedly, a Federal Trade Commission rulemaking on the **Children’s Online Privacy Protection Act (COPPA)** is underway.⁶¹ The bill was passed 20 years ago to prevent online data collection from children under 13 years of age. The FTC oversees enforcement and issues fines to websites that are not in compliance with the regulations. As CEI noted in comments submitted to the FTC, COPPA “exceeds its mandate and

ultimately harms children by creating disincentives towards the production and distribution of content directed towards children while not providing any additional privacy protections.”⁶² As noted, outcomes are far more valuable than intent in measuring public policy. Meanwhile, Google has reached a settlement with the FTC and promises to improve the protection of children’s data on YouTube.⁶³ Yet, there is still no substitute for parents’ supervision, not just in tech concerns, but everywhere.

Helicopter Government, Continued: Saving Dumb Adults from Online Addiction, Manipulation, and Nuisance

7. The Social Media Addiction Reduction Technology (SMART) Act (S. 2314), also sponsored by Hawley, is filled with extremely specific paternalistic rules aimed at stemming online addiction, including banning autoplay videos and infinite scrolling, and limiting social media use to 30 minutes a day.⁶⁴ The latter clock would be reset every month even if one chooses to change it. But why stop there when there are TVs and newspaper subscriptions to ban?⁶⁵ The SMART Act would also require a make-work report:⁶⁶

Not less frequently than once every 3 years, the [Federal Trade Commission shall submit to Congress a report on the issue

of internet addiction and the processes through which social media companies and other internet companies, by exploiting human psychology and brain physiology, interfere with free choices of individuals on the internet (including with respect to the amount of time individuals spend online).

Every generation has faced new threats to the moral order. It was comic books’ effect on youth in the 1960s, Guns ‘n Roses in the 1980s, and now it is online addiction. It seems technology is no barrier for puritans seeking to ruin someone else’s fun. The SMART Act managed to attract no cosponsors.

8. The Deceptive Experiences to Online Users Reduction (DETOUR) Act (S. 1084), sponsored by Sen. Mark Warner (D-VA) and Sen. Deb Fischer (R-NE), seeks “to prohibit the usage of exploitative and deceptive practices by large online operators and to promote consumer welfare in the use of behavioral research by such providers.” Specifically, it would grant new powers to the Federal Trade Commission to police “unfair” and “deceptive” acts by sites with more than 100 million active monthly users:

... to design, modify, or manipulate a user interface with the purpose or substantial effect of obscuring, subverting, or

*Technology is
no barrier for
puritans seeking
to ruin someone
else’s fun.*

*Apparently,
the Internet
is a giant
haunted house
manipulating
everyone to give
up personal data
and information
via “dark
patterns.”*

impairing user autonomy, decision-making, or choice to obtain consent or user data; [or] to subdivide or segment consumers of online services into groups for the purposes of behavioral or psychological experiments or studies, except with the informed consent of each user.

This refers to prompting users to take actions they presumably otherwise would not. Examples include yes or no buttons of different sizes, suggestions that others are about to buy an item in hopes of closing a sale, making alternative settings difficult to access, and luring kids to ask their parents for in-app purchases.⁶⁷ The problem, allegedly, is the possibility of websites goading people into giving up more information than intended, through “prompts to access phone and email contacts in order to keep using the platform.”⁶⁸ Warner points to fake smudges tricking users to click on an ad.⁶⁹ Sen. Hawley is on board, too, since dark patterns “feed tech addiction.”⁷⁰ Apparently, the Internet is a giant haunted house manipulating everyone to give up personal data and information via “dark patterns.”

The DETOUR Act retains government’s protected-class status. Not only does it expand the power of the FTC, it hypocritically fails to restrain

politicians’ purchase of online political ads and grassroots rallying for election.⁷¹

Lawmakers Threaten the Right to Anonymous Speech

The tech regulatory proposals described above threaten the right of anonymous speech, which is elemental to our right to speak and petition for redress of grievances, since sometimes speaking can make one a target for retaliation. Indeed, anonymous political speech was integral to America’s founding, with the publishing of the *Federalist Papers* initially under the pseudonym “Publius.” This stands in contrast to current policy makers’ professed concerns over our data privacy in commercial contexts.

9. The Honest Ads Act proposal (S. 1356) from Sens. Amy Klobuchar (D-MN) and Mark Warner (D-VA) aims “to enhance the integrity of American democracy and national security by improving disclosure requirements for online political advertisements.”⁷² The bill would expand the power of the Federal Election Commission and require tech companies to disclose how they target online political ads and the cost of those ads. Both Facebook and Twitter have endorsed it.⁷³

Facebook founder Mark Zuckerberg proclaimed that election “interference is a problem that’s bigger than any one

platform, and that's why we support the Honest Ads Act. This will help raise the bar for all political advertising online."⁷⁴ Echoing that, Facebook Ads Vice President Rob Goldman wrote:

[W]hen it comes to advertising on Facebook, people should be able to tell who the advertiser is and see the ads they're running, especially for political ads. ... That level of transparency is good for democracy and it's good for the electoral process.⁷⁵

Russia did not buy that many ads, in the grand scheme of things. Yet, the bill includes an exemption for "a communication appearing in a news story, commentary, or editorial distributed through the facilities of any broadcasting station or any online or digital newspaper, magazine, blog, publication, or periodical," unless a political body controls it—all this because Russia bought \$100,000 worth of ads.⁷⁶ If people are that malleable, they may not be suited for voting in the first place.

The bill is not limited to candidates, but encompasses issue advocacy as well. Section 8 (4) (III) requires individuals purchasing political advertisements on social media to disclose their name, address, and phone number (and those of associates) and requires online platforms to keep a record of anyone spending \$500 on

political ads. In that sense, the bill contradicts its original intent. It was intended to keep tabs on potential Russian-style interference in elections, but Section 8(1)(A) could expose private information to public inspection in a machine-readable format, which in turn could make individuals vulnerable to online harassment.⁷⁷

10. Related in spirit is Sen. Diane Feinstein's (D-CA) **Bot Disclosure and Accountability Act** (S.2125).⁷⁸ It prohibits candidates, campaigns, and political organizations from using "social media bots in political advertising, which is intended to deceive voters and suppress human speech." The legislation would empower the Federal Trade Commission to enforce social media transparency requirements regulating "the use of automated software programs intended to impersonate or replicate human activity on social media."⁷⁹

"Fake news" does not undermine democracy until governments assume the authority to label information as such and to squelch speech.

Anonymous speech is a cornerstone of our republic: After all, Thomas Paine signed *Common Sense* "An Englishman" and the *Federalist Papers* authors used pseudonyms as did John Trenchard and Thomas Gordon when they penned *Cato's Letters*.⁸⁰

*Anonymous
speech is a
cornerstone of
our republic.*

Compulsory Disclosure of Internal Business Processes and Monetization of Data

11. The Designing Accounting Safeguards to Help Broaden Oversight and Regulations on Data

(DASHBOARD) Act (S.1951) would require social media platforms to disclose how much their user data is worth, presumably to determine for how much big tech is selling, or would sell, their data. Specifically, it would require any “commercial data operator” with more than 100 million unique monthly users to, at least every 90 days, “provide each user of the commercial data operator with an assessment of the economic value that the commercial data operator places on the data of that user” and describe the types of data collected and any tangential uses of it. The bill would also impose limits on data retention and the ability to delete it.⁸¹ The Federal Trade Commission would enforce all these requirements. The Securities and Exchange Commission would oversee annual or quarterly filings (parallel to financial filings) related to the value of aggregate data, and develop accounting schemes to attempt an impossible calculation of the “value” of the data that tech firms gather or collect from users.

Internet Privacy

Top-down privacy proposals would generally force online operations to

reveal their collection policies, secure that information, and allow users to control its use. Advocates want the federal government to supersede states in order to avoid a patchwork of rules. Aside from the federalism counterarguments, former Federal Trade Commission Chairman Tim Muris long ago noted that privacy abuses are lessened by the fact that national companies like Visa require sites with which it does business to adopt privacy policies.⁸²

Large players have often supported legislation, while small businesses are hurt more by onerous regulation than large operations with plenty of legal assistance. Facebook’s Mark Zuckerberg invited a data privacy law and further regulation in 2018 Senate testimony:

I actually am not sure we shouldn’t be regulated. I think in general technology is an increasingly important trend in the world and I actually think the question is more, what is the right regulation rather than “Yes or no, should it be regulated?”⁸³

Zuckerberg, whose company argues that sharing on social media forfeits any expectation of privacy,⁸⁴ later stated:

I also believe a common global framework—rather than regulation that varies significantly by country

and state—will ensure that the internet does not get fractured, entrepreneurs can build products that serve everyone, and everyone gets the same protections.⁸⁵

12. The Do Not Track Act (S. 1578), also introduced by Hawley, calls for the government to establish a national “Do Not Track” system “to provide consumers a legally enforceable right to browse the internet privately, without data tracking.”⁸⁶ This system will allow users to attach a “signal” to their devices that all websites and online applications must be able to recognize and therefore not target ads at them. Without providing any detail on how this system will work on a technical level, the bill demands that it be up and running in just six months. In addition, the legislation would require websites and applications to inform users about the Do Not Track system if they are not already enrolled, requiring a notification from each website and application the first time a signal is not detected and each subsequent 30th time.

The Do Not Track Act illustrates the fundamental problem with privacy legislation. Acceptable privacy means something different to everyone.

Government’s role is not to dictate the terms of privacy contracts, but to *enforce* companies’ promises.

Governments need not mandate privacy, but allow it.⁸⁷ A world where

people have control of their information cannot be reconciled with government being in control of what information can be created and communicated.

13. The American Data Dissemination (ADD) Act, sponsored by Sen. Marco Rubio (R-FL), would apply the Privacy Act of 1974, which covers government agencies, to private Internet service providers.⁸⁸ Like most privacy legislation, it would impose onerous requirements on virtually all businesses, yet do nothing to actually protect privacy. As Will Rinehart, then with the American Action Forum (now with the Center for Growth and Opportunity at Utah State University), described it:

In total, every business in the United States would be subject to an onerous privacy regime. And because the ADD Act is based on the Privacy Act of 1974, it too will commit the same errors by focusing on data collection and disclosure. But collecting and disclosing data isn’t especially problematic. What is worrying is how a company might use information in a way that could be harmful to consumers.⁸⁹

14. The Social Media Privacy Protection and Consumer Rights Act of 2019 (S. 189), sponsored by Sen. Amy Klobuchar, would mandate that behavioral data collected on social media after registration be

*Acceptable
privacy means
something
different to
everyone.*

The marvelous thing about the Internet is that one can contact and learn about anyone and anything.

flagged to users as being used and shared.⁹⁰ The marvelous thing about the Internet is that one can contact and learn about anyone and anything. The downside is that the reverse is often true. Of course, websites have long collected and marketed information about visitors. Behavioral marketing firms “watch” user clickstreams to develop profiles or inform categories to better target future advertisements. While inarguably beneficial, the process stokes understandable privacy concerns. Privacy policies need to be filtered through the lens of the entire society’s needs. We must consider the impact on 1) consumers; 2) e-commerce and commerce generally; 3) broader security, cybersecurity, homeland security and critical infrastructure issues; and finally 3) citizens’ Fourth Amendment protections.⁹¹

15. The Own Your Own Data Act, sponsored by Sen. John Kennedy (R-LA), would force social media companies to disclose to individuals how they were using their data and create a property right in data “that an individual generates.”⁹² The inherent properties of data make creating an individual property right legislatively in the area difficult, costly, and detrimental to innovation.⁹³ Privacy is a relationship, not a thing.⁹⁴ There is an infinite range between anonymity and full authentication. It is incoherent to say there is an automatic property right in privacy, that no one can say

anything or use any information about somebody else, any more than we can be forbidden to gossip. But it is conceivable that in various contexts—such as the medical, insurance, and financial fields—contracts are created regarding certain information and its disclosure that can be considered a property right of sorts (as intellectual property may be), but not a blanket property right in “personal info.”

16. The Information Transparency and Personal Data Control Act, from Rep. Suzan DelBene (D-WA) and with 24 cosponsors, directs “the Federal Trade Commission to promulgate regulations on sensitive information.”⁹⁵ What counts as sensitive? The government will decide, with said standards not applied to itself, of course. The legislation would give users the option to opt in to the collection, storage, and sharing of their data. It also would require companies to inform consumers if and with whom their sensitive information will be shared. However, the bill stops short of empowering consumers to sue companies or letting states experiment with their own approaches to data privacy.⁹⁶

17. The Balancing the Rights of Web Surfers Equally and Responsibly (BROWSER) Act, sponsored by Sen. Marsha Blackburn (R-TN), a vocal advocate for federal privacy legislation, would require both Internet

service providers (ISP) and edge providers to obtain opt-in consent from consumers in order to use their data.⁹⁷ The bill also preempts state privacy laws and would at least avoid the interstate commerce clause violation of a patchwork of 50 state privacy regimes—which would be a costly and complicated compliance nightmare for ISPs and edge providers.

Privacy Mandates on the Frontier: Home Devices and Public Surveillance via Facial Recognition and Biometrics

Privacy concerns have moved from marketing and online tracking into larger realms like real-time surveillance in cities.⁹⁸ Since these realms involve public property and infrastructure, the dangers are real and bring the issue of government information collection to the forefront.⁹⁹ This offers a chance to make the proper value assertions, but seemingly Washington will have no part of that. One in four Americans now owns a voice-activated smart speaker of one kind or another.¹⁰⁰ And there is always the ultimate opt-out of not buying or using these features.

18. The Commercial Facial Recognition Privacy Act, sponsored by Sens. Roy Blunt (R-MO) and Brian Schatz (D-HI), purports to “strengthen consumer protections by prohibiting commercial users of facial recognition technology (FR) from collecting and re-sharing data for identifying or

tracking consumers without their consent.”¹⁰¹ While government may use technology to identify a match to a wanted individual in a database for whom they had already undertaken Fourth Amendment safeguards to identify, incidental recognition data on other individuals “passing by” must not be retained by authorities. On the private sector side, people may be willing to give up “privacy” in exchange for services they want. Competition and avoidance of data breaches, backed by companies’ reputations for security and safeguarding, are more powerful than regulation by the quarter most eager to invade privacy and track everyone: the government itself.

Antitrust Regulatory Manipulation and Corporate Breakup

Antitrust regulation is likely to be one of the highest-stakes regulatory battles in the technology sector.¹⁰² President Trump and members of Congress from both parties have threatened antitrust actions against Google, Amazon, and Facebook over political grievances often unrelated to competition. In March 2019, the European Commission fined Google €1.49 billion (\$1.7 billion) for violating EU antitrust laws in the firm’s search business.¹⁰³ State attorneys general in the United States and federal regulators have threatened to bring their own cases.

Competition and avoidance of data breaches are more powerful than regulation by the quarter most eager to invade privacy and track everyone: the government itself.

A company's critics almost invariably assume that its relevant competitive market is smaller than it actually is.

In the Google cases, progressives tend to object to Google's market share in online advertising, search, and that of its Android operating system. Conservatives often attack the company claiming its search results have an anti-conservative bias.

In a potential Amazon case, progressives are concerned with Amazon's market share in retail and its labor relations. President Trump seems to have a personal grudge against Amazon founder Jeff Bezos, who separately owns *The Washington Post*, which often runs coverage critical of Trump. The paper is unaffiliated with Amazon.

Regarding Facebook, progressives focus on the company's dominance in social networking, its tendency to buy out competitors, and privacy issues. Conservatives believe Facebook's algorithms and software designers are biased against conservatives and censor conservative viewpoints.

None of these cases have merit. Most of the reasons are addressed in a 2019 CEI paper, "The Case Against Antitrust Law."¹⁰⁴ That paper focuses more on general theory than on specific cases. This section will apply those arguments to today's Google, Amazon, and Facebook antitrust debates.

The Relevant Market Fallacy. The relevant market fallacy is one of the most common misconceptions behind antitrust policy. A company's critics almost invariably assume that its relevant competitive market is smaller than it actually is. Google's share of Internet search is actually much smaller than many antitrust advocates believe. Common searches ranging from Netflix recommendations to match-finding algorithms on online dating sites rely on search engines other than Google. In fact, their proprietary search algorithms are often a competitive selling point. The only area of Internet search where Google truly has a monopoly is on Google searches. Amazon controls roughly half of online retail, for example, but only about 5 percent of total retail. Which is the proper relevant market? Facebook dominates social networking. But as a way to use leisure time, it competes with television, movies, YouTube, books, music, friends, families, and more.

Solving problems and continuing to innovate may require "collusion" among service providers of the very sort that is going to enrage the "open Internet" and antitrust advocates. "The Case Against Antitrust Law," goes into greater detail about the productive case for some forms of collusion.¹⁰⁵ CEI has also detailed how these large firms are

actually fiercely competing with each other across a number of fronts.¹⁰⁶

Net Neutrality Mandates and the Denial of Property Rights in Complex Assets

It has been two years since the repeal of heavy-handed title II regulation of the Internet, known as net neutrality regulations, and none of the dire predictions of net neutrality supporters have come to pass. The Internet is not just intact, but is thriving.

19. The Open Internet Act of 2019 (H.R. 1006), sponsored by Rep. Robert Latta (R-OH) would “amend title I of the Communications Act of 1934 to provide for internet openness.”¹⁰⁷

20. This bill is similar to The Promoting Internet Freedom and Innovation Act of 2019,¹⁰⁸ sponsored by Rep. Cathy McMorris Rodgers (R-WA) and untitled legislation introduced by Rep. Greg Walden (R-OR).¹⁰⁹ With some nuances, this category of bills involves reinstituting bans on blocking content online; slowing data, a practice known as throttling; and preventing so-called “fast lanes” that prioritize certain traffic across the network, presumably for an increased fee. Those practices were legalized in the Federal Trade Commission’s repeal of net neutrality regulations, along with ending the

Internet’s classification as a Title I information service.¹¹⁰

Distortion via Government Ownership, Subsidies, and Industrial Policy in Tech R&D and Production

Some legislation in the 116th Congress was aimed at promoting broadband and 5G, but this is best carried out by regulatory liberalization and easing permitting restrictions. And unfortunately, while the FCC has been eliminating cumbersome net neutrality regulations and working to bring more spectrum to market, it also has been pushing unwise federal funding of broadband deployment in certain sectors.¹¹¹

21. The Accelerating Broadband Development by Empowering Local Communities Act of 2019, introduced by Rep. Anna Eshoo (D-CA), would nullify rules issued by the Federal Communications Commission that revoke state and local authority to regulate telecommunications equipment deployment.¹¹² It would seem to be the dead opposite of needed federal preemption, which would eliminate the patchwork maze of costly and complicated state and local regulatory regimes.

22. The Office of Rural Broadband Act, sponsored by Sen. Kevin Cramer (R-ND), would create an office at the FCC to coordinate rural broadband

While the FCC has been eliminating cumbersome net neutrality regulations and working to bring more spectrum to market, it also has been pushing unwise federal funding of broadband deployment.

deployment efforts.¹¹³ This is as the FCC itself fights to shrink the regulatory underbrush, not expand it.

Government Subsidies and Intervention in the Gig Economy, Tech Workforces, and Education

23. The Championing Apprenticeships for New Careers and Employees in Technology (CHANCE in Tech) Act would provide industry intermediaries, like state tech associations, the ability to receive federal grants to develop apprenticeships within the technology sector.¹¹⁴ These are baby versions of grander schemes for “free college.”

24. The Protecting the Right to Organize (PRO) Act of 2019, sponsored by Rep. Bobby Scott (R-VA), would likely cripple gig economy firms by destroying their business model. Specifically, it creates a federal version of the “ABC” test in AB5, the recently enacted California law that seeks to reclassify large numbers of independent contractors as employees eligible for unionization. The many thousands who work for sharing economy platforms because they value flexibility or extra income would lose their gigs. The millions of dollars of consumer surplus added to the economy by these firms would vanish. The PRO Act passed the House in 2019 but has so far languished in the Senate. It is likely that future administrations might attempt to

reclassify workers by administrative fiat, as the Obama administration attempted.

California’s AB5 was an attempt to force gig economy firms like Uber, Lyft, and Taskrabbit to classify independent contractors as employees, giving them full benefits and the right to unionize. AB5 uses what is called an ABC test to determine if a worker is an independent contractor or a formal employee. It consists of three questions:

- A. How closely is each worker supervised or directed? Do they check in with a boss every day? Or do they work mostly on their own and have wide discretion on how to do their job?
- B. Is their work part of the company’s core business? (For an Uber driver, the answer is yes. For an accountant or a maintenance worker, maybe not.)
- C. Is the hiring company the contractor’s sole or dominant customer? Is the job mostly in the contractor’s area of specialty or expertise?¹¹⁵

The bill text is vaguely worded.¹¹⁶ In practice, nearly any freelancer qualifies as a formal employee under AB5, but a lot of job arrangements are somewhere in between. While those firms have so far successfully resisted

the effort, many thousands of independent contractors in California have lost their jobs, been dropped from in-state work, or been forced to move out of state.¹¹⁷

25. The Gig Is Up Act, sponsored by Rep. Debra Haaland (D-NM), also targets gig economy firms. It would require businesses to pay employer and employee portions of Social Security and Medicare taxes when they contract with at least 10,000 independent contractors and gross at least \$100 million in a calendar year. While not as existential a threat to gig economy firms as AB5 or the PRO Act, it would still impose significant costs on national firms, reducing the attractiveness of their business model and probably reducing the amount they are able to pay workers.

Moves Toward the Regulation of Virtual Currencies

For more than three years, the Securities and Exchange Commission has been lording over the cryptocurrency and blockchain technology sectors, including in areas over which it has no jurisdiction granted from Congress. It has been doing so via arbitrary enforcement actions and “regulatory dark matter”—agency issuances, including guidance documents bulletins, memos, and even blog posts that do not go through the notice-and-comment

rulemaking process, as required by the Administrative Procedure Act, yet carry regulatory weight.¹¹⁸

In short, without changes in the law, stated intent of Congress, or a formal rule, the SEC has been sending signals through enforcement actions and statements from officials that new issuers of cryptocurrency may be required to go through the same cumbersome securities registration process as do issuers of stocks and bonds.

The SEC has been regulating products under its jurisdiction, such as exchange-traded funds, or ETFs, more stringently if they involve cryptocurrency. Since 2017, the commission has rejected proposals for more than 10 Bitcoin-based exchange traded funds, sparking a strong dissent in 2018 from Commissioner Hester Peirce. Peirce wrote that the SEC’s rejection “signals an aversion to innovation that may convince entrepreneurs that they should take their ingenuity to other sectors of our economy, or to foreign markets.”¹¹⁹

Most troubling is the SEC’s assertion of jurisdiction over cryptocurrency products that clearly do not fit the definition of a “security” from either Congress or the courts. A 2019 guidance document from the SEC—properly classified as “regulatory dark matter,” since it was never submitted

*Bad legislation
now lays the
groundwork
for worse
legislation later.*

to Congress for review as a rule—states that even in cases where cryptocurrency can be used in a functional market for goods and services, “there may be securities transactions if ... there are limited or no restrictions on reselling those digital assets.”¹²⁰

This overly broad definition of a security could set a precedent for the SEC to regulate not just cryptocurrency, but everyday consumer goods, as “securities.” In an interview for a CEI study, prominent FinTech attorney Georgia Quinn said after reading the SEC guidance, “I think airline miles and retailer points could be considered securities,” noting that some of these items are transferable and therefore could be deemed to have a secondary market. For instance, the website [points.com](https://www.points.com) enables users to manage and exchange rewards points, creating what could be deemed a secondary market.¹²¹ And then there are the numerous physical goods, from comic books to baseball cards, that are often bought in part as investments and can be sold in secondary markets.

For cryptocurrency and other new technologies to flourish, consumers, investors and entrepreneurs must be protected from the overreach of the SEC. The Trump administration and Congress need to rein in “regulatory dark matter” at the SEC (as well as other agencies) and curb any efforts

by the SEC to stretch the definition of “security” beyond recognition. Furthermore, Congress should update the nation’s securities laws to more clearly and narrowly define federal agencies’ jurisdiction over cryptocurrency.

INFORM Act

The Integrity, Notification and Fairness in Online Retail Marketplace for Consumers (INFORM) Act (S. 3431) would force online marketplaces like Amazon, eBay, and the like to verify the government ID, tax ID, bank account, and contact information of all their third-party sellers that make at least 200 sales amounting to \$5,000 or more in one year. Platforms would also be obligated to make that information available to customers. The bill seeks to thwart sales of counterfeit and stolen items online by third-parties, but platforms are already working to solve those problems for consumers.

Just as there is a certain amount of fraud in bricks and mortar retail, there is also fraudulent activity online. But a lack of perfection should not be the rule for when to regulate. Market failure should be the only justification for government intervention.

Retail platforms that host third-party sellers have every incentive to protect their reputations by protecting their

customers. eBay has won awards for its cooperation with rights holders to address the sales of fakes online.¹²² Amazon is the nation's largest online retailer and Americans rank the company among the most trusted brands.¹²³ That trust is a competitive advantage that Amazon saw fit to spend \$500 million protecting in 2019. The retail platform also devoted the efforts of 8,000 employees to combat these problems on its platform last year.¹²⁴ The company vets new third-party sellers, monitors their offerings, and proactively notifies and even refunds consumers when fraud has been detected. Amazon offers a Brand Registry program,¹²⁵ a Transparency service,¹²⁶ a Counterfeit Crimes Unit, and other security services that the company has instituted on its own.¹²⁷

All of this appears to be money well spent because, according to testimony from Amazon Vice President Dharmesh M. Mehta gave to the House Committee on Energy and Commerce in March, the company prevented 2.5 million suspected bad actor accounts from starting to sell in its online stores, blocked six billion suspected bad listings from appearing, and blocked and repressed 100 suspected fake reviews last year.¹²⁸ All of this benefits Amazon in preserving its good name, and it benefits consumers by protecting them from fraudulent items and information.

Market solutions are already working to protect consumers. A regulatory bill is not needed.

But worse than being repetitive, the INFORM Act may be harmful. The unintended consequences of the bill include security and privacy concerns with the gathering, storing, and sharing with customers of potentially sensitive information. The best intentions do not prevent the inherent tension between verification and privacy. There is also a chance that these compliance costs could act as a barrier to entry for the next, but still small, eBay or Amazon. The big platforms can afford to comply, but the new guy might find the regulatory hoop cost prohibitive.

Better to let market forces compete for consumers by catering to their preferences. It is already happening to combat fraud online. Let's hope Congress does not get in the way.

Conclusion

Market solutions, unlike legislation, better lend themselves to address the myriad problems that inevitably arise in a free, competitive economy. The Internet was not initially designed as the mass commercial and consumer medium it is today. If one were to design a commercial network today from the bottom up, it likely would incorporate better authentication. Now

*Market solutions
are already
working to
protect
consumers.*

that we are in midstream, we wonder if technology can fix its attendant problems, or if law must do it. Either free enterprise or Congress and legislators can set terms, but not both.

There is a role for law. Fraud, falsification, identity theft, hacking, and the like should be punished, but overly burdensome legislation will create legal and regulatory hassles for small businesses—a reason some large firms favor intervention—and the

development of newer technologies and services, which is one of the great hidden costs of regulation.

Bad legislation now lays the groundwork for worse legislation later. Embracing regulation and central planning entails embracing collective “solutions” that will be difficult or impossible to correct later. The legislation we actually need would be a bill to prevent many of these misguided proposals.

NOTES

- 1 Elizabeth Holmes and Amy Schatz, “McCain Tech Plan to Continue Hands-Off Approach to Regulation,” *Wall Street Journal*, August 14, 2008, <https://www.wsj.com/articles/SB121867827436739337>.
- 2 Clyde Wayne Crews, Jr., “Mapping Washington’s Lawlessness: An Inventory of ‘Regulatory Dark Matter’ 2017 Edition,” *Issue Analysis* 2017 No. 4, Competitive Enterprise Institute, <https://cei.org/content/mapping-washington%E2%80%99s-lawlessness-2017>. Clyde Wayne Crews, Jr., *Ten Thousand Commandments 2020: An Annual Snapshot of the Federal Regulatory State*, Competitive Enterprise Institute, May 27, 2020, <https://cei.org/10kc2020>.
- 3 The White House, “President Donald J. Trump’s Historic Deregulatory Actions are Benefiting American Families, Workers, and Businesses,” news release, June 28, 2019, <https://www.whitehouse.gov/briefings-statements/president-donald-j-trumps-historic-deregulatory-actions-are-benefiting-american-families-workers-and-businesses/>.
- 4 Clyde Wayne Crews, Jr. and Adam Thierer, “The Digital Dirty Dozen: The Most Destructive High-Tech Legislative Measures of the 107th Congress,” *Policy Analysis* No. 423, Cato Institute, February 4, 2002, <https://www.cato.org/publications/policy-analysis/digital-dirty-dozen-most-destructive-hightech-legislative-measures-107th-congress>.
- 5 Patrick Hedger, “Consumers to Benefit from Court Decisions to Uphold FCC Restoring Internet Order,” *OpenMarket* blog, Competitive Enterprise Institute, October 1, 2019, <https://cei.org/content/consumers-benefit-court-decision-uphold-fcc-restoring-internet-freedom-order>.
- 6 Clyde Wayne Crews Jr., “A CES Takeaway: Don’t Fear Robots and Artificial Intelligence, Fear Politicians,” *Forbes*, January 8, 2017, <https://www.forbes.com/sites/waynecrews/2017/01/08/a-ces-takeaway-dont-fear-robots-and-artificial-intelligence-fear-politicians/#357903107984>.
- 7 FAANG is but one acronym, and Netflix sometimes seems misplaced here. Other examples include GAFA (Google, Amazon, Facebook, Apple) and even MAGA (Microsoft, Amazon, Google, Apple).
- 8 Will Rinehart, “An Ongoing List of Tech Bills in 116th Congress (2019–2020),” *Medium*, March 15, 2019, <https://medium.com/@willrinehart/an-ongoing-list-of-tech-bills-in-116th-congress-2019-2020-f3822b2b3182>.
- 9 “No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.” Section 230 of the Communications Decency Act, characterized as such by Jeff Kosseff of the U.S. Naval Academy’s Cyber Science department in a book of the same name. Jeff Kosseff, *The Twenty-Six Words that Created the Internet* (Ithaca, NY: Cornell University Press, 2019).
- 10 On February 27, 2018, the Fight Online Sex Trafficking Act/Stop Ending Sex Traffickers Act (FOSTA-SESTA) package was passed in the House of Representatives by a 388-25 vote. On March 21, 2018, the FOSTA-SESTA package bill passed the Senate with a vote of 97-2, with only Sens. Ron Wyden (D-OR) and Rand Paul (R-KY) voting against it. Roll Call Vote on Passage of HR 1865 SESTA/FOSTA Last Vote of the Day, Senate Democrats, March 21, 2018, <https://www.democrats.senate.gov/2018/03/21/roll-call-vote-on-passage-of-hr-1865-last-vote-of-the-day>.
- 11 The Fight Online Sex Trafficking Act (FOSTA) was the House of Representatives bill and the Stop Enabling Sex Traffickers Act (SESTA) was its Senate companion bill. For more, see, Elizabeth Nolan Brown, “Section 230 Is the Internet’s First Amendment: Now Both Republicans and Democrats Want to Take it Away,” *Reason*, July 29, 2019, <https://reason.com/2019/07/29/section-230-is-the-internets-first-amendment-now-both-republicans-and-democrats-want-to-take-it-away/>.
- 12 1996 Communications Decency Act, Section 230, <https://www.law.cornell.edu/uscode/text/47/230>.
- 13 “Sites Using Facebook ‘Like’ Button Liable for Data, EU Court Rules,” Euractiv with AFP, July 30, 2019, <https://www.euractiv.com/section/digital/news/sites-using-facebook-like-button-liable-for-data-eu-court-rules>.
- 14 For more on EU Internet regulation, see Ryan Radia and Ryan Khurana, “European Union’s General Data Protection Regulation and Lessons for U.S. Privacy Policy,” *OnPoint* No. 245, Competitive Enterprise Institute, May 23, 2018, <https://cei.org/content/european-unions-general-data-protection-regulation-and-lessons-us-privacy-policy>.
- 15 Adam Thierer and Clyde Wayne Crews, Jr., eds, *Copy Fights: The Future of Intellectual Property in the Information Age* (Washington, DC: Cato Institute, 2002).
- 16 Telecommunications Act of 1996, Federal Communications Commission, <https://www.fcc.gov/general/telecommunications-act-1996>.
- 17 Charles B. Goldfarb, “Telecommunications Act: Competition, Innovation, and Reform,” Congressional Research Service, June 7, 2007. https://www.everycrsreport.com/files/20070607_RL33034_41a165fda09eb9fd0de96374f3425ae4f3276f53.pdf.
- 18 Digital Millennium Copyright Act, Harvard University. Accessed at: <https://dmca.harvard.edu/pages/overview>.
- 19 Mulligan, Stephen P., Wilson C. Freeman, and Chris D. Linebaugh, “Data Protection Law: An Overview,” Congressional Research Service, March 25, 2019. <https://fas.org/sgp/crs/misc/R45631.pdf>.

20 “What is the CAN-SPAM Act?” Legal Information Institute, Cornell Law School,
https://www.law.cornell.edu/wex/inbox/what_is_can-spam.

21 Goldman, Eric, “The Complicated Story of FOSTA and Section 230,” *First Amendment Law Review*, April 17, 2019.
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3362975.

22 Jeff Kossseff, *The Twenty-Six Words that Created the Internet* (Ithaca; N.Y.: Cornell University Press, 2019).
<https://www.vox.com/the-goods/2018/11/8/18076440/facebook-monopoly-curse-of-bigness-tim-wu-interview>.

23 Jemima Kiss, “An Online Magna Carta: Berners-Lee Calls for Bill of Rights for Web,” *Guardian*, March 12, 2014,
<https://www.theguardian.com/technology/2014/mar/12/online-magna-carta-berners-lee-web>.

24 “Web Pioneer Wants New ‘Contract’ for Internet,” *France24*, May 11, 2019,
<https://www.france24.com/en/20181105-web-pioneer-wants-new-contract-internet>. Jamey Keaten, “At Age 30, World Wide
 Web is ‘Not the Web We Wanted,’” *Associated Press*, March 12, 2019, <https://apnews.com/1a944fcf10c445f2a87fcd5c2d0320e5>.

26 Guy Faulconbridge and Paul Sandle, “Father of Web Says Tech Giants May Have to be Split Up,” *Reuters*,
 November 1, 2018,
<https://www.reuters.com/article/us-technology-www/father-of-web-says-tech-giants-may-have-to-be-split-up-idUSKCN1N63MV>.

27 Office of Congressman Ro Khanna, “Rep. Khanna Releases ‘Internet Bill of Rights’ Principles, Endorsed by Sir Tim
 Berners-Lee,” news release, October 4, 2018,
<https://khanna.house.gov/media/press-releases/release-rep-khanna-releases-internet-bill-rights-principles-endorsed-sir-tim>.
 Todd Shields, “Democrats Eye ‘Internet Bill of Rights’ If They Win the House Todd Shields,” *Bloomberg*, October 17, 2018,
<https://www.bloombergquint.com/business/democrats-eye-internet-bill-of-rights-if-they-win-u-s-house>.

28 “Notable and Quotable: Milton Friedman,” *Wall Street Journal*, October 6, 2015,
<https://www.wsj.com/articles/notable-quotable-milton-friedman-1444169267>.

29 Kari Paul, “Will Americans pay companies to keep their data private? Here’s their answer,” *MarketWatch*, January 19, 2019,
<https://www.marketwatch.com/story/will-americans-pay-companies-to-protect-their-personal-data-heres-their-answer-2019-01-17>.

30 Armando Roggio, “DuckDuckGo Attracts Privacy-conscious Shoppers,” *Practical Ecommerce*, January 24, 2020,
<https://www.practicalecommerce.com/duckduckgo-appeals-to-privacy-conscious-shoppers>.

31 DuckDuckGo traffic information, <https://duckduckgo.com/traffic>.

32 Jonathan Ponciano, “The Largest Technology Companies In 2019: Apple Reigns as Smartphones Slip and Cloud Services
 Thrive,” *Forbes*, May 15, 2019,
<https://www.forbes.com/sites/jonathanponciano/2019/05/15/worlds-largest-tech-companies-2019/#21e4b2bc734f>.

33 Sen. Josh Hawley (R-MO) remarked in September 2019: “It is time we held them accountable, stood up for the First
 Amendment, and it is time to stop censorship by these big companies and say that conservative speech is valuable speech
 and conservatives ought to be able to speak in our society openly, in public, and without reprisal.”
<https://twitter.com/yaf/status/1156615193385943040>.

34 For example, see Facebook’s Civil Rights Audit—Progress Report, June 30, 2019,
https://fbnewsroomus.files.wordpress.com/2019/06/civilrightaudit_final.pdf. Ina Fried and Rebecca Falconer, “Facebook
 Vows Misinformation Crackdown ahead of 2020 Election, Census,” *Axios*,
<https://www.axios.com/facebook-civil-rights-audit-2020-election-census-ed689151-f53b-49a5-b67a-0da99e095185.html>.

35 Josh Hawley, “Big Tech’s ‘Innovations’ that Aren’t,” *Wall Street Journal*, August 28, 2019,
<https://www.wsj.com/articles/big-techs-innovations-that-arent-11567033288>.

36 Office of Sen. Josh Hawley, “Senator Hawley Introduces Legislation to Amend Section 230 Immunity for Big Tech
 Companies,” news release, June 19, 2019,
<https://www.hawley.senate.gov/senator-hawley-introduces-legislation-amend-section-230-immunity-big-tech-companies>.
 “Ending Support for Internet Censorship Act,”
<https://www.hawley.senate.gov/sites/default/files/2019-06/Ending-Support-Internet-Censorship-Act-Bill-Text.pdf>.

37 Clyde Wayne Crews, Jr., “The Case Against Social Media Content Regulation; Reaffirming Congress’ Duty to Protect Online
 Bias, ‘Harmful Content,’ and Dissident Speech from the Administrative State,” *Issue Analysis* 2020 No. 4, Competitive
 Enterprise Institute, June 2, 2020, <https://cei.org/content/case-against-social-media-content-regulation>.

38 Office of Sen. Josh Hawley, “Senator Hawley Announces Bill Empowering Americans to Sue Big Tech Companies Acting in
 Bad Faith,” news release, June 17, 2020,
<https://www.hawley.senate.gov/senator-hawley-announces-bill-empowering-americans-sue-big-tech-companies-acting-bad-faith>.

39 47 U.S. Code § 230 (c).

40 Limiting Section 230 Immunity to Good Samaritans Act, S. 3983, 116th Congress, Second Session, 2020,
<https://www.hawley.senate.gov/sites/default/files/2020-06/Limiting-Section-230-Immunity-to-Good-Samaritans-Act.pdf>.

41 Dell Cameron, “Senator Hawley’s New ‘Section 230’ Bill Won’t Make Silicon Valley Sweat,” *Gizmodo*, June 17, 2020,
<https://gizmodo.com/senator-hawleys-new-section-230-bill-isnt-going-to-make-1844067513>.

- 42 Makena Kelly, “Big Tech’s Liability Shield Under Fire Yet Again from Republicans,” *The Verge*, July 28, 2019,
<https://www.theverge.com/2019/7/28/8933871/big-techs-liability-shield-under-fire-yet-again-from-republicans>.
- 43 Twitter post by @DrPaulGosar, September 18, 2019, 1:02 pm, <https://twitter.com/DrPaulGosar/status/1174368215738310657>.
- 44 James Pethokoukis, “Jeff Kosseff on the twenty-six words that created the internet: A long-read Q&A,” *AEIdeas*,
 American Enterprise Institute, July 3, 2019,
<https://www.aei.org/economics/jeff-kosseff-on-the-twenty-six-words-that-created-the-internet-a-long-read-qa/>.
- 45 H.R.492—Biased Algorithm Deterrence Act of 2019, 116th Congress, First Session,
<https://www.congress.gov/bill/116th-congress/house-bill/492/text?q=%7B%22search%22%3A%5B%22social+media+protection%22%5D%7D&r=2&s=4>.
- 46 Eric Rosenbaum, “Tech spending will near \$4 trillion this year. Here’s where all the money is going and why,”
CNBC, April 8, 2019,
<https://www.cnbc.com/2019/04/08/4-trillion-in-tech-spending-in-2019-heres-where-the-money-is-going.html>.
- 47 <https://cei.org/blog/cautiously-optimistic-about-facebooks-new-approach-speech>.
- 48 Matthew Ingram, “Leaked White Paper Proposes Congressional Regulation of Social Media,” *Columbia Journalism Review*,
https://www.cjr.org/the_new_gatekeepers/congress-white-paper-platforms.php. David McCabe, “Scoop: 20 Ways Democrats
 Could Crack Down on Big Tech,” *Axios*, July 30, 2018.
<https://www.axios.com/mark-warner-google-facebook-regulation-policy-paper-023d4a52-2b25-4e44-a87c-945e73c637fa.html>.
- 49 The *Axios* story features the full text of the white paper.
- 49 Warner White Paper, “Potential Policy Proposals for Regulation of Social Media and Technology Firms” p. 2.
- 50 Ibid.
- 51 Elizabeth Nolan Brown, “Senate Democrats Are Circulating Plans for Government Takeover of the Internet,” *Reason*, July 31,
 2018, <https://reason.com/2018/07/31/democrats-tech-policy-plans-leaked>.
- 52 For treatments by this author on the foundational importance of the right to anonymous speech, see Clyde Wayne Crews Jr.,
 “Cybersecurity and Authentication: The Marketplace Role in Rethinking Anonymity—Before Regulators Intervene,”
Issue Analysis 2004 No.2, November 8, 2004, <http://cei.org/pdf/4281.pdf>; also in *Knowledge and Policy*,
 Vol 20, No. 2 (June 2007),
https://www.researchgate.net/publication/225742893_Cybersecurity_and_Authentication_The_Marketplace_Role_in_Rethinking_Anonymity_-_Before_Regulators_Intervene. Clyde Wayne Crews, Jr., “Human Bar Code: Monitoring Biomet-
 ics Technologies In a Free Society,” *Policy Analysis* No. 452, Cato Institute, September 17, 2002,
<http://www.cato.org/pubs/pas/pa452.pdf>.
- 53 Ingram, “Leaked White Paper Proposes Congressional Regulation of Social Media.”
- 54 S.1629—A bill to regulate certain pay-to-win microtransactions and sales of loot boxes in interactive digital entertainment
 products, and for other purposes, 116th Congress, First Session,
<https://www.congress.gov/bill/116th-congress/senate-bill/1629/text>.
- 55 Makena Kelly, “Bill to Ban the Sale of Loot Boxes to Children Presses Forward with Bipartisan Support,” *The Verge*, May 23,
 2019, <https://www.theverge.com/2019/5/23/18636535/loot-boxes-josh-hawley-markey-blumenthal-privacy-video-games>.
- Kyle Orland, “Senator Hawley Announces Bill Banning Loot Boxes, Pay-to-Win Mechanics,” *Ars Technica*, May 8, 2019,
<https://arstechnica.com/gaming/2019/05/senator-hawley-announces-bill-banning-loot-boxes-pay-to-win-mechanics>.
- 56 Office of Senator Josh Hawley, “Senator Hawley to Introduce Legislation Banning Manipulative Video Game Features
 Aimed at Children,” news release, May 8, 2019,
<https://www.hawley.senate.gov/senator-hawley-introduce-legislation-banning-manipulative-video-game-features-aimed-children>.
- 57 Orland.
- 58 Jason Schreier, “U.S. Senator Introduces Bill To Ban Loot Boxes And Pay-To-Win Microtransactions,” *Kotaku*, May 8, 2019,
<https://kotaku.com/u-s-senator-introduces-bill-to-ban-loot-boxes-and-pay-1834612226>.
- 59 S. 1916—Protecting Children from Online Predators Act of 2019, 116th Congress, First Session,
<https://www.congress.gov/116/bills/s1916/BILLS-116s1916is.pdf>.
- 60 Elizabeth Nolan Brown, “6 Terrible New Tech Bills in Congress,” *Reason.com*, August 8, 2019,
<https://reason.com/2019/08/08/6-terrible-tech-plans-in-congress/>.
- 61 Federal Trade Commission, “FTC Seeks Comments on Children’s Online Privacy Protection Act Rule,” news release, July 25,
 2019, <https://www.ftc.gov/news-events/press-releases/2019/07/ftc-seeks-comments-childrens-online-privacy-protection-act-rule>.
- 62 Patrick Hedger, Comments of the Competitive Enterprise Institute to the Federal Trade Commission, July 25, 2019,
<https://beta.regulations.gov/document/FTC-2019-0054-117126>.
- 63 Susan Wojcicki, “An Update on Kids and Data Protection on YouTube,” YouTube Official Blog, September 4, 2019,
<https://youtube.googleblog.com/2019/09/an-update-on-kids.html>.

64 S. 2314—the Social Media Addiction Reduction Technology (SMART) Act, 116th Congress, First Session, <https://www.congress.gov/116/bills/s2314/BILLS-116s2314is.pdf>. Office of Sen. Josh Hawley, “Sen. Hawley Introduces Legislation to Curb Social Media Addiction,” news release, July 30, 2019, <https://www.hawley.senate.gov/sen-hawley-introduces-legislation-curb-social-media-addiction>. Emily Birnbaum, “GOP Senator Introduces Bill Banning ‘Addictive’ Social Media Features,” *The Hill*, July 30, 2019, <https://thehill.com/policy/technology/455235-gop-senator-introduces-bill-banning-addictive-social-media-features>.

65 Twitter post by @ismurray, July 30, 2019, 12:05 p.m., <https://twitter.com/ismurray/status/1156234350687600641>.

66 S. 2314.

67 John Eggerton, “Hill Briefing: DETOUR Act on the Right Track,” *Multichannel News*, June 25, 2019, <https://www.multichannel.com/news/hill-briefing-detour-act-on-right-road>.

68 Kayla Tausche and Mary Catherine Wellons, “A New Senate Bill Would Ban a ‘Deceptive’ Practice Used by Facebook to Get User Data, Such as Phone and Email Contacts,” *CNBC*, April 9, 2017, <https://www.cnn.com/2019/04/09/new-senate-bill-would-ban-a-deceptive-practice-used-by-facebook-to-get-users-contact-data.html>.

69 Twitter post by @MarkWarner, April 9, 2019, 1:00 p.m., <https://twitter.com/markwarner/status/1115660846955474945?lang=en>.

70 Hawley, “Big Tech’s ‘Innovations’ that Aren’t.”

71 “The Love-Hate Relationship Between 2020 Presidential Candidates and Tech Giants: A Delicate Dance of Money, Online Influence and Populist Anger,” *ABC News*, July 27, 2019, <https://abcnews.go.com/Politics/love-hate-relationship-2020-presidential-candidates-tech-giants/story?id=64490545>.

72 S. 1356—Honest Ads Act, 116th Congress, First Session, <https://www.congress.gov/116/bills/s1356/BILLS-116s1356is.pdf>.

73 <https://www.cnet.com/news/at-facebook-and-twitter-hearings-congress-needs-to-bring-its-a-game/>.

74 Sara Fischer and David McCabe, “Facebook Says it supports Honest Ads Act, Cracks Down on Issue Ads,” *Axios*, April 6, 2018, <https://www.axios.com/facebook-ad-changes-5da9d7f7-d297-488b-9f46-9729101201f8.html>.

75 As quoted in Makena Kelly, “Without New Laws, Facebook has No Reason to Fix its Broken Ad System,” *The Verge*, October 31, 2018, <https://www.theverge.com/2018/10/31/18048236/facebook-mark-warner-fec-congress-honest-ads-act>.

76 Casey Newton, “Russia Bought Political Ads from Facebook During the Election, Company Says,” *The Verge*, September 7, 2017, <https://www.theverge.com/2017/9/6/16263704/russia-election-hacking-facebook-ad-spending>; and see Colin Lecher, “Here are the Russia-Linked Facebook Ads Released by Congress,” *The Verge*, November 1, 2017, <https://www.theverge.com/2017/11/1/16593346/house-russia-facebook-ads>.

77 Lee E. Goodman, “‘Honest’ Political Ads: Watch Out, Drudge, You’re Next,” *The Hill*, September 4, 2019, <https://thehill.com/opinion/cybersecurity/459896-honest-political-ads-watch-out-drudge-youre-next>.

78 S. 2125—Bot Disclosure and Accountability Act, <https://www.congress.gov/116/bills/s2125/BILLS-116s2125is.pdf>.

79 Rachel Frazin, “Feinstein Introduces Bill to Prohibit Campaigns from Using Social Media Bots,” *The Hill*, July 7, 2019, <https://thehill.com/policy/cybersecurity/453336-dem-senator-introduces-bill-to-prohibit-campaigns-from-using-bots>.

80 Robb A. McDaniel, “Cato’s Letters,” *The First Amendment Encyclopedia*, Free Speech Center at Middle Tennessee State University, <https://mtsu.edu/first-amendment/article/857/cato-s-letters>.

81 S.1951—Designing Accounting Safeguards to Help Broaden Oversight and Regulations on Data, 116th Congress, First Session, <https://www.congress.gov/116/bills/s1951/BILLS-116s1951is.pdf>. David McCabe and Kaveh Waddell, “A New Bill Would Require Tech Platforms to Disclose the Value of Users’ Data,” *Axios*, March 9, 2019, <https://www.axios.com/warner-bill-disclose-value-of-user-data-0ed7cf90-1674-4dfb-9b95-be3bdcdfe73.html>.

82 Drew Clark, “Muris Reiterates Opposition to Privacy Legislation,” *National Journal’s Technology Daily*, November 7, 2001.

83 Alyna Selyukh, “Facebook CEO Mark Zuckerberg Readies to Testify on Capitol Hill,” Weekend Edition Sunday, National Public Radio, April 8, 2018, <https://www.npr.org/2018/04/08/600616534/facebook-ceo-mark-zuckerberg-readies-to-testify-on-capitol-hill>.

84 Mikael Thalen, “Facebook Lawyer Says Users ‘Have No Expectation of Privacy,’” *The Daily Dot*, May 31, 2019, <https://www.dailymail.com/debug/facebook-lawyer-no-expectation-of-privacy/>.

85 Mark Zuckerberg, “The Internet Needs New Rules. Let’s Start in these Four Areas,” *Washington Post*, March 30, 2019, https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html?noredirect=on&utm_term=.cd7a0187eaaf. Jeff Horwitz and Deepa Seetharaman, “Facebook’s Zuckerberg Backs Privacy Legislation,” *Wall Street Journal*, June 26, 2019, https://www.wsj.com/articles/facebooks-zuckerberg-backs-privacy-legislation-11561589798?mod=cx_picks&cx_navSource=cx_picks&cx_tag=video&cx_artPos=5#cxrecs_s.

86 John Eggerton, “Hawley: Big Tech is Exploiting Digital ‘Treadmill,’” *Multichannel News*, August 9, 2019, <https://www.multichannel.com/news/hawley-big-tech-is-exploiting-digital-treadmill>.

- 87 Clyde Wayne Crews, Jr., “Is Privacy Dead? Yes, If America’s Surveillance State Drones on,” *Forbes*, May 30, 2012,
<https://www.forbes.com/sites/waynecrews/2012/05/30/is-privacy-dead-yes-if-americas-surveillance-state-drones-on/#215ebbed662c>.
- 88 A bill to impose privacy requirements on providers of internet services similar to the requirements imposed on Federal agencies under the Privacy Act of 1974, 116th Congress, First Session.
https://www.rubio.senate.gov/public/_cache/files/3859c1d4-fd09-47c1-afa1-c1684e2f8df9/A9470F75C36C8115D756746340CC1E55.american-data-dissemination-act.pdf.
- 89 Will Rinehart, “Understanding the ADD Act,” *Insight*, American Action Forum, January 17, 2019,
<https://www.americanactionforum.org/insight/understanding-the-add-act/>.
- 90 S.189—Social Media Privacy Protection and Consumer Rights Act of 2019, 116th Congress, First Session,
<https://www.congress.gov/bill/116th-congress/senate-bill/189/text>.
- 91 Clyde Wayne Crews, Jr., “Policy Implications of Online Advertising” Committee on Commerce, U.S. Senate, July 9, 2009,
<https://www.commerce.senate.gov/services/files/CFDC9775-62AA-4A3E-9282-45B1C500A86C>.
- 92 S.806—Own Your Own Data Act, 116th Congress, First Session
<https://www.congress.gov/bill/116th-congress/senate-bill/806/text?q=%7B%22search%22%3A%5B%22social+media+protection%22%5D%7D&r=4&s=4>.
- 93 Will Rinehart, “The Law & Economics of ‘Owning Your Data,’” *Insight*, American Action Forum, April 10, 2018,
<https://www.americanactionforum.org/insight/law-economics-owning-data/>.
- 94 For more on the nature of privacy, see *The Future of Financial Privacy* (Washington, D.C.: Competitive Enterprise Institute, 2000).
- 95 A bill to prohibit the collection of data or information generated on the internet, 116th Congress, First Session,
<https://www.congress.gov/bill/116th-congress/house-bill/2013/text?q=%7B%22search%22%3A%5B%22technology++%5C%22consumer+protection%5C%22%22%5D%7D&r=10&s=7>.
- 96 H.R.2013—Information Transparency & Personal Data Control Act, 116th Congress, First Session,
<https://www.congress.gov/bill/116th-congress/house-bill/2013/text?q=%7B%22search%22%3A%5B%22DelBene%22%5D%7D>.
- 97 Chris Mills Rodrigo, “Moderate Democratic lawmakers back privacy bill favored by businesses,” *The Hill*, October 15, 2019,
<https://thehill.com/policy/technology/465951-moderate-democratic-lawmakers-back-privacy-bill-favored-by-businesses>.
- 98 <https://www.americanactionforum.org/insight/browser-act-explained/>.
- 99 Gregory Barber and Tom Simonite, “Some US Cities Are Moving Into Real-Time Facial Surveillance,” *Wired*, May 17, 2019,
<https://www.wired.com/story/some-us-cities-moving-real-time-facial-surveillance/>.
- 100 These may be on their smart phone or may be a separate home device. Amazon’s Alexa/Echo, Google Home, Apple’s Siri, and Microsoft’s Cortana all allow users to delete or opt out of collection and storing of user data to some degree. Clyde Wayne Crews, Jr., “Who Will Own the Infrastructure in the Smart City?” *Forbes*, January 11, 2018,
<https://www.forbes.com/sites/waynecrews/2018/01/11/who-will-own-the-infrastructure-in-the-smart-city/#3ced81d21ab4>.
- 101 Jennifer Jolly, “It’s not you, it’s them: Google, Alexa and Siri may answer even if you haven’t called,” *USA Today*, February 25, 2020,
<https://www.usatoday.com/story/tech/conferences/2020/02/25/google-alexa-siri-randomly-answer-even-without-wake-word-study-says/4833560002/>.
- 102 S.847—Commercial Facial Recognition Privacy Act of 2019, 116th Congress, First Session,
<https://www.congress.gov/bill/116th-congress/senate-bill/847/text?q=%7B%22search%22%3A%5B%22schatz%22%5D%7D>. For more on the threat to privacy being from government intrusion, not the private sector, see Clyde Wayne Crews, Jr.’s, “Human Bar Code.”
- 103 Ryan Young and Clyde Wayne Crews, Jr., “The Case Against Antitrust Law: Ten Areas Where Antitrust Policy Can Move On from the Smokestack Era,” *Issue Analysis* 2019, No. 1, Competitive Enterprise Institute, April 17, 2019,
<https://cei.org/content/the-case-against-antitrust-law>.
- 104 European Commission, “Antitrust: Commission fines Google €1.49 billion for abusive practices in online advertising, news release March 20, 2019, https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1770.
- 105 Young and Crews, “The Case against Antitrust Law.”
- 106 Ibid.
- 107 Patrick Hedger, “If Facebook and Apple are Feuding, How Are they Monopolies?” *OpenMarket*, Competitive Enterprise Institute, June 25, 2019, <https://cei.org/blog/if-facebook-and-apple-are-feuding-how-are-they-monopolies>.
- 108 H.R.1006—Open Internet Act of 2019, 116th Congress, First Session,
<https://www.congress.gov/bill/116th-congress/house-bill/1006?q=%7B%22search%22%3A%5B%22h.r.+1006%22%5D%7D&s=1&r=1>.
- 109 H.R.1096—Promoting Internet Freedom and Innovation Act of 2019 116th Congress, First Session,
<https://www.congress.gov/bill/116th-congress/house-bill/1096/text>.

109 H.R.1101—To amend the Communications Act of 1934 to ensure internet openness, to prohibit blocking lawful content and non-harmful devices, to prohibit throttling data, to prohibit paid prioritization, to require transparency of network management practices, to provide that broadband shall be considered to be an information service, and to prohibit the Commission or a State commission from relying on section 706 of the Telecommunications Act of 1996 as a grant of authority, 116th Congress, First Session, <https://www.congress.gov/bill/116th-congress/house-bill/1101/text>.

110 Daniel Lyons, “Analyzing the Republican net neutrality bills,” *AEIdeas*, American Enterprise Institute, April 18, 2019, <https://www.aei.org/technology-and-innovation/telecommunications/analyzing-the-republican-net-neutrality-bills/>.

111 Federal Communications Commission, “FCC Launches \$20 Billion Rural Digital Opportunity Fund,” news release, January 30, 2020, <https://www.fcc.gov/document/fcc-launches-20-billion-rural-digital-opportunity-fund>.

112 H.R.530—Accelerating Broadband Development by Empowering Local Communities Act of 2019, 116th Congress, First Session, <https://www.congress.gov/bill/116th-congress/house-bill/530?q=%7B%22search%22%3A%5B%22broadband%22%5D%7D&s=6&r=29>.

113 S. 454—Office of Rural Broadband Act, 116th Congress, First Session, <https://www.congress.gov/bill/116th-congress/senate-bill/454/text?q=%7B%22search%22%3A%5B%22S.+454%3A+Office+of+Rural+Broadband+Act%22%5D%7D&r=1&s=1>.

114 S.777—CHANCE in TECH Act, 116th Congress, First Session, <https://www.congress.gov/bill/116th-congress/senate-bill/777>.

115 Charlie Osborne, “In the line of fire: Will California’s AB5 labor law cause havoc for cybersecurity consultants?” *The Daily Swig*, January 30, 2020, <https://portswigger.net/daily-swig/in-the-line-of-fire-will-californias-ab5-labor-law-cause-havoc-for-cybersecurity-consultants>.

116 California Assembly Bill No. 5, Chapter 296, An act to amend Section 3351 of, and to add Section 2750.3 to, the Labor Code, and to amend Sections 606.5 and 621 of the Unemployment Insurance Code, relating to employment, and making an appropriation therefor, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB5.

117 A CEI study published before AB5 went into effect found that, if it is successful at forcing ridesharing companies to reclassify employees, the price of a typical ride in a California rideshare would increase substantially, perhaps by 30 to 50 percent. Ryan Radia, “California Ride Share Contracting Legislation Is a Solution in Search of a Problem,” *OnPoint* No. 261, Competitive Enterprise Institute, December 17, 2019, <https://cei.org/content/california-ride-share-contracting-legislation-solution-search-problem>.

118 John Berlau, “Cryptocurrency and the SEC’s Limitless Power Grab: Why Speculative Consumer Goods Are Not ‘Securities,’” *OnPoint* No. 253, Competitive Enterprise Institute, April 11, 2019, <https://cei.org/content/cryptocurrency-and-secs-limitless-power-grab>. For more on “regulatory dark matter, see Clyde Wayne Crews, Jr., “Mapping Washington’s Lawlessness: An Inventory of Regulatory Dark Matter 2017 Edition,” *Issue Analysis* 2017 No. 4, <https://cei.org/content/mapping-washington%E2%80%99s-lawlessness-2017>.

119 Hester Peirce, Dissent to Release No. 34-83723; File No. SR-BatsBZX-2016-30, July 26, 2018, Securities and Exchange Commission, <https://www.sec.gov/news/public-statement/peirce-dissent-34-83723>.

120 Securities and Exchange Commission, “Framework for ‘Investment Contracts’ Analysis of Digital Assets,” April 3, 2019, <https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets>.

121 Telephone Interview with Georgia Quinn, published in: Berlau, “Cryptocurrency and the SEC’s Limitless Power Grab.”

122 Ina Steiner, “eBay Lauded for Its Fight Against Fakes,” *eCommerce Bytes*, January 15, 2020, <https://www.ecommercebytes.com/2020/01/15/ebay-lauded-for-its-fight-against-fakes/>.

123 P.J. Bednarski, “USPS, Amazon, Google, PayPal Most Trusted Brands,” *Marketing Daily*, January 13, 2020, <https://www.mediapost.com/publications/article/345638/usps-amazon-google-paypal-most-trusted-brands.html#:~:text=That%20may%20be%20changing,the%20most%20trusted%20among%20millennials>.

124 Statement of Dharmesh M. Mehta Vice President, Worldwide Customer Trust and Partner Support, Amazon.com Services LLC before the United States House of Representatives Committee on Energy and Commerce, Subcommittee on Consumer Protection and Commerce, March 4, 2020, <https://docs.house.gov/meetings/IF/IF17/20200304/110634/HHRG-116-IF17-Wstate-MehtaD-20200304.pdf>.

125 Amazon Brand Registry Program, accessed September 3, 2020, <https://brandservices.amazon.com/>.

126 Amazon Transparency, accessed September 3, 2020, <https://brandservices.amazon.com/transparency>.

127 Annie Palmer, “Amazon says a new ‘Counterfeit Crimes Unit’ will work with law enforcement to take on fraudsters,” *CNBC*, June 24, 2020, <https://www.cnbc.com/2020/06/24/amazon-says-counterfeit-crimes-unit-to-work-with-law-enforcement.html>.

128 Statement of Dharmesh M. Mehta.

About the Authors

Jessica Melugin is Associate Director of the Center for Technology and Innovation at the Competitive Enterprise Institute. Her research focuses on technology issues including antitrust, online privacy, Internet taxation, telecommunications, social media content, and net neutrality regulation. Her writings have appeared in the *New York Times*, *USA Today*, *Forbes*, *Fortune*, *The Hill*, *Washington Examiner*, *Washington Times*, Fox News, CNBC, and various regional papers. She has been cited in *Politico* and *U.S. News and World Report*, among many other publications. Melugin has appeared on CSPAN's "Washington Journal," CNBC's "Power Lunch," and Fox Business Network's "Varney and Company." She has been featured on National Public Radio's Marketplace and the David Webb Show on SiriusXM, and is regularly interviewed on terrestrial radio programs.

Melugin graduated magna cum laude from Claremont McKenna College, with a degree in government and art history. Her honors thesis explored the development of American antitrust law as it pertains to the Microsoft trial. She lives in Virginia's horse country with her children.

Clyde Wayne Crews, Jr. is Vice President for Policy at the Competitive Enterprise Institute (CEI). He is widely published and a contributor to *Forbes*. A frequent speaker, he has appeared at venues including the DVD Awards Showcase in Hollywood, European Commission-sponsored conferences, the National Academies, the Spanish Ministry of Justice, and the Future of Music Policy Summit. He has testified before Congress on various policy issues. Crews has been cited in dozens of law reviews and journals. His work spans regulatory reform, antitrust and competition policy, safety and environmental issues, and various information-age policy concerns.

Alongside numerous studies and articles, Crews is co-editor of the books *Who Rules the Net? Internet Governance and Jurisdiction*, and *Copy Fights: The Future of Intellectual Property in the Information Age*. He is co-author of *What's Yours Is Mine: Open Access and the Rise of Infrastructure Socialism*, and a contributing author to other books. He has written in the *Wall Street Journal*, *Chicago Tribune*, *Communications Lawyer*, *International Herald Tribune*, and other publications. He has appeared on Fox News, CNN, ABC, CNBC, and the PBS News Hour. His policy proposals have been featured prominently in *The Washington Post*, *Forbes*, and *Investor's Business Daily*.

Before coming to CEI, Crews was a scholar at the Cato Institute. Earlier, Crews was a legislative aide in the U.S. Senate, an economist at Citizens for a Sound Economy and the Food and Drug Administration, and a fellow at the Center for the Study of Public Choice at George Mason University. He holds a Master of Business Administration from the College of William and Mary and a Bachelor of Science from Lander College in Greenwood, South Carolina. While at Lander, he was a candidate for the South Carolina state senate. A dad of five, he can still do a handstand on a skateboard and enjoys custom motorcycles.

Iain Murray is Vice President for Strategy and senior fellow at the Competitive Enterprise Institute. He also directs the Center for Economic Freedom at CEI. He is the author of the best-selling books *The Socialist Temptation*, *The Really Inconvenient Truths*, and *Stealing You Blind*. He has written extensively on free markets and the environment, labor policy, finance, the European Union, and trade.

His op-eds have appeared in *The Wall Street Journal*, CNBC, and *National Review*. He has appeared on Fox News, CNN Headline News, the BBC, and Al-Jazeera, among other broadcast networks.

Patrick Hedger is Vice President of Policy at the Taxpayers Protection Alliance. He is a former research fellow at the Competitive Enterprise Institute's Center for Technology and Innovation. With a focus on Internet and telecommunications policy, he provides everything from commentary to detailed research and analysis on how limited government-policies best facilitate innovation and competition in the marketplace.

Prior to joining CEI, Hedger served as director of policy at FreedomWorks Foundation, where he oversaw the organization's work on regulatory reform, including a successful campaign to support the Federal Communications Commission's Restoring Internet Freedom Order in 2017.

Hedger is a twice-graduate of George Mason University, with a Bachelor of Arts degree in government and international politics and a Master of Public Policy degree.

Ryan Young is a fellow at the Competitive Enterprise Institute. His research focuses on regulatory reform, trade policy, antitrust policy, and other issues. His work has been featured in publications like *USA Today*, *Politico*, and *Investor's Business Daily*. Previously, Young was CEI's Warren T. Brookes Journalism Fellow. Before joining CEI, he worked in the Cato Institute's Government Affairs Department.

He holds a Master in Economics from George Mason University and a Bachelor's in history from Lawrence University. Young's personal blog is Inertia Wins.

John Berlau is a senior fellow at the Competitive Enterprise Institute. His work focuses on how public policy affects access to capital, entrepreneurship, and opportunities for the public to build wealth through investing.

Berlau is a contributing writer for *Forbes*. His work has been published and cited in the *Wall Street Journal*, *New York Times*, *Washington Post*, *Financial Times*, Bloomberg News, *The Atlantic*, *Politico*, *Washington Examiner*, *Investor's Business Daily*, *National Journal*, *National Review*, *Reason*, and more. He is a frequent guest on radio and television programs, including CNBC's "The Call," "Power Lunch," and "Closing Bell," and Fox Business' "Cavuto."

Berlau has testified on the impact of financial regulation before the House Committee on Financial Services and the House Committee on Energy and Commerce. He has spoken at prominent conferences such as South by Southwest Interactive in Austin, Money 20/20 in Las Vegas, the FinTech Global Expo in San Diego, the CFGE Crowdfund Banking and Lending Summit in San Francisco, and the Crowdfund Intermediary Regulatory Advocates Summit in Washington, D.C. Before joining CEI, Berlau was an award-winning financial and political journalist. He served as Washington correspondent for *Investor's Business Daily* and as a staff writer for *Insight* magazine.

Berlau is also the author of the acclaimed biography *George Washington, Entrepreneur* (St. Martin's Press, 2020), which details Washington's innovative endeavors in his private business career and his struggle with overweening regulation that helped lead to the American Revolution.

He graduated from the University of Missouri-Columbia in 1994 with degrees in journalism and economics.

The authors are grateful to Gabriel Greenspan, Christopher Scott, and Sean Stewart for their valuable research assistance.



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